Московский государственный университет имени М.В.Ломоносова

На правах рукописи

Савченко Максим Алексеевич

# Влияние дополнительной информационной асимметрии на решения неантагонистических игр

1.2.3. Теоретическая информатика, кибернетика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук, профессор
Васин Александр Алексеевич

Москва — 2022

## Оглавление

Стр.

Стр.

# Введение

В теории игр конфликты с участием трёх и более преследующих собственные цели сторон по многим причинам считаются существенно более трудными для моделирования в сравнении с классическими парными противостояниями. Среди этих причин следует особо подчеркнуть влияние, оказываемое на их ход информационной асимметрией. В играх с двумя участниками её эффект, в целом, сводится к последствиям априорной неполноты их знаний о параметрах конфликта и обычно описывается при помощи байесовских моделей. Платёжная функция в таких случаях не является общим знанием игроков, каждый из них действует исходя из собственных, возможно, различающихся предположений, выраженных в форме распределения вероятностей на пространстве всевозможных платёжных функций с заданным множеством стратегий.

Ещё одним источником информационной асимметрии в парном конфликте может выступать присутствие в действиях оппонентов тайной составляющей в тех случаях, когда он проходит в несколько стадий. При этом действия, уже совершённые игроком на ранних стадиях, могут быть полностью или частично неизвестны его противнику, вынужденному основывать стратегию более поздних стадий на предположениях. Это естественным образом формализуется при помощи информационных разбиений дерева ходов в развёрнутой форме игры. По сути, двумя упомянутыми аспектами исчерпывается влияние информационной асимметрии на конфликты с двумя сторонами. Однако, увеличение количества участников ещё хотя бы на одного порождает новый феномен, замеченный ещё Робертом Ауманом в статье [1], где впервые было сформулировано коррелированное расширение игр в нормальной форме.

Выражается этот феномен в том, как для одних и тех же игр соотносятся множества равновесий по Нэшу в смешанных стратегиях и с использованием внешних механизмов корреляции. Для случая двух игроков все вектора математических ожиданий выплат в точках коррелированных равновесий принадлежат выпуклой оболочке множества смешанных равновесий, т. е. механизмы корреляции можно рассматривать просто как способ получения линейных комбинаций классических решений. С появлением третьего игрока картина меняется — в некоторых играх присутствие непубличного корреляционного механизма позволяет достичь точек равновесия по Нэшу с выплатами за пределами выпуклой оболоч-

ки решений в смешанных стратегиях. Фактически, это означает, что асимметрия знаний может оказывать существенное влияние на исход многостороннего конфликта даже в тех случаях, когда она не касается существенных для структуры выплат факторов. Назовём игры, подверженные этому эффекту, *чувствительными к дополнительной информационной асимметрии*.

Хотя описанный феномен известен уже давно, при построении моделей большинство исследователей обходили его стороной, рассматривая скорее как курьёзную особенность некоторых игр многих игроков. Важным исключением при этом выступает, пожалуй, наиболее значимая из активно использующих формализм коррелированного расширения игр в нормальной форме область теории игр — «дизайн механизмов» [2]Леонида Гурвича, Эрика Маскина и Роджера Майерсона. Их подход ставит своей целью создание экономических инструментов, стимулирующих эгоистичных рациональных агентов к поведению, оптимальному с точки зрения общих целевых функций, формализующих различные социальные блага. Будучи чрезвычайно плодотворной областью исследований, дизайн механизмов породил множество направлений и ответвлений, объединённых тем не менее рядом неотъемлемых общих черт, проистекающих из информационной структуры игр, для которых доказываются его основные положения. Типичная схема взаимодействий выглядит так: игроки-агенты, знающие свои предпочтения и возможности, но находящиеся в неведении относительно этих параметров у других участников, информируют о них центр, формирующий на основе этой информации набор коррелированных стратегий. Далее центр реализует его для конкретного случая в виде набора чистых стратегий и инструктирует каждого из агентов, которые в свою очередь и принимают окончательное решение о том или ином действии. При этом подразумевается, что агенты могут лгать на первом этапе и не подчиняться на последнем. Главной задачей дизайна механизмов в этой парадигме становится создание таких алгоритмов поведения центра, что стратегии правдивости и послушания образуют для агентов равновесие Нэша.

Не вдаваясь в детали, можно сказать, что дизайн механизмов базируется на частном случае информационной асимметрии — своего рода звёздчатой структуре связей, где выделенный центральный агент может в своих интересах распоряжаться общим механизмом корреляции, а подчинённые ему агенты находятся в полной изоляции как друг от друга, так и от остального мира. Название здесь действительно неплохо отражает свойственный для модели взгляд на конфликты — через её призму стороны рассматриваются как взаимозамени-

мые детали единого рукотворного механизма, не связанные ничем кроме участия в нём. Хотя моделирование в рамках подобного упрощения вполне может быть полезно при конструировании формализованных способов решения конфликтов, оно никак не может помочь в тех случаях, когда на них оказывает существенное влияние информационная асимметрия, складывающаяся не в результате сознательного дизайна, а естественным образом, по мере спонтанного взаимодействия агентов в неконтролируемой, внешней с точки зрения модели среде. К примеру, сложно переоценить значимость влияния коррупции на политические и экономические институты, а ведь она складывается именно из таких незапланированных информационных связей, внешних по отношению к самим институтам.

По описанной причине исследование влияния дополнительной информационной асимметрии на решения игр многих игроков никак нельзя сводить только к конструктивным моделям. Увы, но за пределами дизайна механизмов сложилась традиция игнорировать этот феномен. К примеру, в статье [3]Дрю Фуденберга и Эрика Маскина можно найти следующую сноску: «Actually, if $n \geqslant 3$, the other players may be able to keep player $j$'s payoff even lower by using a correlated strategy against $j$, where the outcome of the correlating device is not observed by $j$ (...). In keeping with the rest of the literature on repeated games, however, we shall rule out such correlated strategies.»[1] А ведь казалось бы, в контексте повторяющихся игр с дисконтированием проблематика использования секретности механизма корреляции для усиления стратегий наказания довольно любопытна — наверное в каждой области исследований, использующей народную теорему, от антропологии до международной политики, несложно отыскать примеры того, как группы агентов усиливали свою коллективную долгосрочную позицию при помощи необходимо тайного согласования действий. Увы, но приходится констатировать, что теории игр до сих пор почти нечего предложить другим наукам в качестве инструмента анализа описанного феномена.

**Целью** данной работы является создание новой модели многосторонних конфликтов, учитывающей влияние на их ход дополнительной информационной асимметрии.

[1]«В сущности, если $n \geqslant 3$, остальные игроки получают возможность опустить выплаты игрока $j$ ещё ниже, используя против него коррелированную стратегию, в которой игрок $j$ не может наблюдать сигнала механизма корреляции (...). Придерживаясь сложившейся в посвящённых повторяющимся играм публикациях традиции, мы, впрочем, не будем рассматривать такие коррелированные стратегии.»

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Исследовать формализм коррелированного обобщения игр в нормальной форме с точки зрения проблематики работы.
2. Разработать способ описания информационных структур, достаточно разнообразным образом связывающих участников произвольного конфликта.
3. Исследовать влияние дополнительной информационной асимметрии на соответствие равновесий критериям коллективной рациональности.
4. Разработать приемлемую концепцию решения с учётом связей между агентами для игр с дополнительной информационной асимметрией.

**Научная новизна:**

1. Выделены в качестве самостоятельного объекта исследования игры многих игроков, проявляющие чувствительность к дополнительной информационной асимметрии.
2. Предложен формализм пространства заговоров, специальным образом сужающий в целях моделирования дополнительной информационной асимметрии формализм пространства корреляции.
3. Сформулирована концепция структурно согласованного равновесия, позволяющая во многих случаях выделять среди решений игр в пространствах заговоров отвечающие принципу коллективной рациональности.
4. Показана возможность расширения множества совершенных подыгровых равновесий в повторяющихся играх, чувствительных к дополнительной информационной асимметрии, при помощи инструментов современной криптографии.

**Практическая значимость** работы проистекает из явной необходимости учитывать при моделировании многосторонних конфликтов тот факт, что состав их участников не является в большинстве случаев случайной выборкой никак не связанных друг с другом агентов. Классический формализм игр в нормальной форме опирается на неявное допущение, состоящее в том, что единственной значимой характеристикой каждого игрока является порядок его предпочтений относительно исхода розыгрыша, выражающийся в форме платёжной функции. Совершенно очевидно при этом, что реальных людей, вступающих в противостояние, зачастую связывают значимые для его исхода отношения, структура которых

не может быть выражена простым сочетанием платёжных функций. В качестве наглядной иллюстрации такой связи можно сравнить две воображаемые партии в бридж или преферанс с участием одинаково сильных игроков, различающиеся тем, что в одном случае за столом сидят незнакомцы, а в другом часть из них играют вместе уже много лет. Любой достаточно опытный картёжник скажет, что при равных навыках фактор «сыгранности» с партнёром надёжно обеспечивает решающее преимущество. Естественным образом этот феномен можно обобщить и на более значимые конфликты: политика, бизнес, дипломатия — везде, где исход противостояния существенно зависит от согласованности и непредсказуемости действий, взаимопонимание, не требующее коммуникации, зачастую может превратить поражение в победу. Таким образом, для более точного предсказания исходов многосторонних конфликтов насущно необходимы модели, позволяющие учитывать этот фактор.

**Методология и методы исследования.** В работе используются методы теории игр, теории вероятности, топологии и криптографии.

**Основные положения, выносимые на защиту:**

1. Доказательство теоремы об изоморфизме пространств корреляции, определяющей для них классы эквивалентности, в которые входят только неразличимые с теоретико-игровой точки зрения пространства.
2. Доказательство теоремы о пространствах заговоров одной структуры, благодаря которой структуру пространства можно считать его исчерпывающим описанием.
3. Доказательство чувствительности к дополнительной информационной асимметрии симметричной проблемы планирования заданий с немонотонной отдачей.
4. Решение трёхсторонней симметричной проблемы планирования с немонотонной функцией оплаты за срочность в ассиметричном пространстве заговоров, удовлетворяющее критерию структурной согласованности.
5. Модель повторяющихся игр с учётом стоимости вычислений, необходимых для выбора хода на очередной итерации.
6. Криптографические стратегии наказания для повторяющегося трёхстороннего чёт-нечета, пополняющие множество совершенных подыгровых равновесий точками, не достижимыми без принятия во внимание сложности алгоритмов.

**Апробация работы.** Основные результаты работы докладывались на: Ломоносовских чтениях (2017, 2021 гг.) [4; 5], IX Московской международной конференции по исследованию операций [6] и конференции молодых учёных по математической экономике и экономической теории (МЕЕТ-2021) [7].

**Личный вклад.** Результаты, представленные в диссертационной работе теоремами и другими выносимыми на защиту положениями, получены автором самостоятельно. Подготовка к публикации полученных результатов проводилась без соавторов.

**Публикации.** Основные результаты по теме диссертации изложены в 7 печатных работах, 3 из которых [8][9][10] изданы в периодическом научном журнале, рекомендованном ВАК и индексируемом Web of Science и Scopus. Центральная работа имеет перевод на английский язык[11]. 3 работы изданы в тезисах докладов.

**Объем и структура работы.** Диссертация состоит из введения, 3 глав, заключения и 4 приложений. Полный объём диссертации составляет 91 страницу, включая 2 рисунка и 5 таблиц. Список литературы содержит 28 наименований.

# Глава 1. Модель заговоров

## 1.1 Коррелированное расширение игры в нормальной форме[1]

Базовым формализмом для описания дополнительной информационной асимметрии в сложившейся научной традиции выступает коррелированное расширение нормальной формы игр, предложенное Робертом Ауманом в [1]. Для удобства его центральные элементы будут изложены здесь в нотации, адаптированной к русскоязычной среде. Рассмотрим игру в нормальной форме $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$. Конечное множество игроков здесь и далее везде обозначается как $A = \{1, \ldots, m\}$, а конечное множество наборов чистых стратегий — $S = S^1 \times \ldots \times S^m$. Помимо множества стратегий $S^a$, каждый игрок определяется платёжной функцией $u^a : S \to \mathbb{R}$.

Также рассмотрим вероятностное пространство[12] $\langle \Omega, \mathfrak{B}, \mathbb{P}\rangle$, в котором реализуется наблюдаемое игроками состояние природы. Здесь $\Omega$ — множество всевозможных таких состояний, $\mathfrak{B}$ — σ-алгебра подмножеств $\Omega$, а $\mathbb{P} : \mathfrak{B} \to \mathbb{R}_{\geqslant 0}$ — вероятностная мера. Каждому игроку $a \in A$ поставим в соответствие *собственное подпространство* $\langle \Omega, \mathfrak{I}^a, \mathbb{P}\rangle$ такое, что $\mathfrak{I}^a \subseteq \mathfrak{B}$. При этом набор σ-алгебр $\mathfrak{I} = (\mathfrak{I}^a, a \in A)$ отражает информированность игроков о состоянии природы. В описываемой ситуации это состояние не влияет на функции выигрышей непосредственно, выступая исключительно как способ синхронизации действий игроков. Это значит, что σ-алгебра $\mathfrak{B}$ сама по себе не является существенным параметром модели, и измеримость по ней для $\mathbb{P}$ можно заменить измеримостью по $\mathfrak{I}^a, \forall a \in A$.

Отдельно следует заметить, что в оригинале для собственных подпространств игроков Аумановский формализм предполагал индивидуальность не только σ-алгебр, но и соответствующих им мер, учитывая тем самым возможную субъективность оценок вероятности наступления тех или иных событий, что немаловажно в случаях, когда в качестве механизма корреляции выступают процессы, слишком сложные для объективного анализа (например спортивные соревнования). Однако, для целей данного исследования этот аспект не имеет

[1] Раздел уточняет и дополняет материалы статьи [8].

большого смысла, поскольку в модели заговоров подразумевается, что их участники могут произвольным образом выбирать механизм корреляции, а в такой ситуации разумно ожидать, что люди будут использовать простые источники случайности с известным распределением (рулетки, кости, жребий и т.д.). По этой причине здесь и далее модель коррелированных стратегий используется в её упрощённой форме, с общей для всех игроков объективной вероятностной мерой в пространстве состояний природы.

Таким образом, получается $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$ — набор параметров, характеризующих некоторое *пространство корреляции* для произвольной игры с множеством игроков $A$. Отметим, что в играх с одним множеством игроков, но различными множествами чистых стратегий и функциями выигрыша можно применять одно и то же пространство корреляции. Полностью же *коррелированное расширение игры* определяет пара $\Gamma|\Phi$. Опишем полученную новую игру в терминах нормальной формы[2]:

$$\Gamma|\Phi = \langle A, \mathbf{S}^a, u^a(\mathbf{s}), a \in A \rangle.$$

Здесь множество $\mathbf{S}^a$ доступных игроку $a$ коррелированных стратегий состоит из всех $\mathfrak{I}^a$-измеримых функций $\mathbf{s}^a : \Omega \to S^a$, отображающих множество возможных состояний природы на множество доступных ему чистых стратегий. Соответственно, функция выигрыша вычисляется по формуле математического ожидания случайной величины

$$u^a(\mathbf{s}) = \sum_{s \in S} \mathbb{P}(\mathbf{s}^{-1}(s)) u^a(s),\ \mathbf{s}^{-1}(s) = \{\omega \in \Omega \mid \mathbf{s}^a(\omega) = s^a, \forall a \in A\},$$

где $\mathbb{P}(\mathbf{s}^{-1}(s))$ выступают в роли коэффициентов распределения на матрице игры.

В своей статье Ауман демонстрирует силу вводимого формализма, показывая на примерах, как с его помощью в играх можно получать новые точки равновесия по Нэшу. Подбирая параметры пространств корреляции, можно конструировать не только решения с любыми выплатами из выпуклой оболочки векторов выплат в точках классического смешанного равновесия Нэша, но для некоторых игр даже решения, лежащие за пределами такой выпуклой оболочки. Это позволяет сформулировать ключевое для данной работы понятие:

**Определение 1.1.1.** Пусть $\Gamma$ — игра в нормальной форме с $m$ участниками, а $U \subseteq \mathbb{R}^m$ — множество всех векторов выплат, достижимых в её смешанных

[2]Следуя нотации, введённой в [1], наборы стратегий и множества исходов коррелированного расширения игры обозначаются жирным шрифтом ($\mathbf{s}$ и $\mathbf{S}$ там, где в базовой игре $s$ и $S$).

равновесиях по Нэшу. Игра Г называется *чувствительной к дополнительной информационной асимметрии*, когда существует пространство корреляции Ф такое, что в игре Г|Ф найдётся коррелированное равновесие по Нэшу с вектором выплат, не принадлежащим выпуклой оболочке множества $U$.

Кроме того, в этой же статье доказывается, что наличие в пространстве корреляции публичной вещественной рулетки, т.е. подпространства событий с равномерно распределённым вещественным исходом в диапазоне $[0, 1)$, влечёт выпуклость как множества достижимых выплат, так и множества равновесий Нэша в любой игре. Касательно коррелированного расширения игр в нормальной форме, вышеизложенного вполне достаточно для понимания идей данной работы, более подробно же современное состояние знаний на эту тему можно проследить по публикациям, упомянутым в Приложении A.

## 1.2 Изоморфизм пространств корреляции[3]

Следует отметить, что модель пространств корреляции в некотором смысле существенно избыточна, поскольку как таковые события из состояния природы значения не имеют и используются лишь в качестве сигналов для синхронизации стратегий игроков. Чтобы осмысленным образом рассуждать о влиянии, оказываемом дополнительной информационной асимметрией на исходы конфликтов, неизбежно требуется умение абстрагироваться от конкретных её источников, фокусируя внимание на структурных различиях в осведомлённости оппонентов. Если формально различные пространства корреляции оказываются полностью взаимозаменимы с теоретико-игровой точки зрения, то они должны быть отнесены к общему классу эквивалентности, чьё описание и является в действительности существенным параметром модели. Сразу заметим, что это касается не только тривиальных замен множества состояний природы на другое множество той же мощности с соответствующей биекцией остальных параметров пространства, но и более сложных случаев. Например, если в контексте некоторой игры группа игроков наблюдает общий сигнал в виде колеса вещественной рулетки, будет ли

[3] Раздел уточняет и дополняет материалы статьи [8].

иметь значение наблюдение ими ещё и броска монетки? Здравый смысл подсказывает, что любую общую стратегию с использованием рулетки и монетки можно легко превратить в эквивалентную для одной только рулетки, для чего достаточно поделить колесо пополам и отобразить отдельные варианты для орла и решки на полученные два сектора. Опишем этот феномен в виде изоморфизма:

**Определение 1.2.1.** *Разбиением* пространства корреляции $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$ *в произвольное конечное множество исходов (кодомен)* $X = X^1 \times ... \times X^m$ называется отображение $f : \Omega \to X$, состоящее из набора функций $(f^1, ..., f^m)$, где каждая $f^a : \Omega \to X^a$ измерима в $\mathfrak{I}^a$. Далее разбиение $f$ пространства корреляции $\Phi$ будем сокращённо обозначать $f \models \Phi$.

В контексте коррелированного расширения множествам исходов $X^a$ соответствуют множества чистых стратегий $S^a$, а элементам разбиения $f^a$ — коррелированные стратегии $\mathrm{s}^a$. Далее также будут использоваться отображения $f^{-1} : X \to 2^\Omega$, обратные к разбиениям пространств корреляции:

$$f^{-1}(x) = \bigcap_{a \in A} (f^a)^{-1}(x^a).$$

**Определение 1.2.2.** Пространство $\Phi_1$ с мерой $\mathbb{P}_1$ называется *отобразимым на* $\Phi_2$ *с мерой* $\mathbb{P}_2$ (далее $\Phi_1 \precsim \Phi_2$), если их множества игроков совпадают и для любого разбиения $f_1 \models \Phi_1$ существует разбиение $f_2 \models \Phi_2$ с тем же кодоменом такое, что $\mathbb{P}_1 \circ f_1^{-1} = \mathbb{P}_2 \circ f_2^{-1}$. Взаимно отобразимые друг на друга пространства корреляции называются *изоморфными* (далее $\Phi_1 \sim \Phi_2$).

Это определение легко проиллюстрировать упомянутым выше примером — для любого разбиения $f_1 : [0, 1) \times \{0, 1\} \to X$ пространства, состоящего из вещественной рулетки и симметричной монетки, можно построить соответствующий образ $f_2 : [0, 1) \to X$ в пространстве из одной только рулетки:

$$f_2(\alpha) = \begin{cases} f_1(2\alpha, 0), & 0 \leqslant \alpha < \frac{1}{2} \\ f_1(2\alpha - 1, 1), & \frac{1}{2} \leqslant \alpha < 1 \end{cases}.$$

Рефлексивность, симметричность и транзитивность вводимого при помощи данного определения изоморфизма очевидны, а значит это действительно отношение эквивалентности на множестве пространств корреляции. При этом, хотя определение изоморфизма дано в отрыве от коррелированного расширения игр, можно сформулировать следующую теорему:

**Определение 1.2.3.** Для игры $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ множеством достижимых выплат по отклонениям группы игроков $A_*$ от профиля стратегий $s$ будем называть

$$U_\Gamma^{A_*}(s) = \{\bar{u} \mid \exists s_* \in S : u(s_*) = \bar{u}, \forall a \in A \setminus A_*, s^a = s_*^a\}.$$

**Теорема 1.2.1** (Об изоморфных пространствах)**.** *Пусть* $\Phi_1 \sim \Phi_2$*. Тогда для любой игры в нормальной форме* $\Gamma$ *с конечными множествами стратегий игроков её коррелированные расширения* $\Gamma|\Phi_1$ *и* $\Gamma|\Phi_2$ *обладают следующим свойством. Пусть* $\mathbf{s}_1$ *— некоторый профиль стратегий игры* $\Gamma|\Phi_1$*. Тогда существует* $\mathbf{s}_2$ *— профиль стратегий игры* $\Gamma|\Phi_2$ *такой, что* $U_{\Gamma|\Phi_1}^{A_*}(\mathbf{s}_1) = U_{\Gamma|\Phi_2}^{A_*}(\mathbf{s}_2)$ *для любой группы игроков* $A_*$*.*

Эта теорема позволяет считать изоморфные пространства корреляции неразличимыми в контексте поиска равновесий, устойчивых к как индивидуальным, так и групповым отклонениям. Доказательство, представляющее собой упражнение в топологии без тесной связи с центральными идеями работы, вынесено в Приложение Б.

## 1.3 Пространства заговоров[4]

Получив осмысленный изоморфизм для пространств корреляции, можно выделить из всевозможных классов эквивалентности те, что представляют интерес с точки зрения моделирования дополнительной информационной асимметрии. Как показал Ауманн, выход за пределы выпуклой оболочки множества решений в смешанных стратегиях возможен, если часть игроков (не менее двух) использует коррелированную стратегию, зависящую от события, о котором не проинформирован хотя бы один из остальных игроков. Подобную форму взаимовыгодного тайного согласования действий естественно называть *заговором*, а используемый для синхронизации сигнал — *тайной*. Пусть в пространстве корреляции $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A\rangle$ имеется тайна, т.е. вероятностное подпространство $\langle \Omega, \mathfrak{S}, \mathbb{P}\rangle$. Искомая асимметрия информированности предполагает, что некоторые игроки наблюдают события из $\mathfrak{S}$ (или другие, коррелирующие с ними), а некоторые — нет. Хотя теоретически можно представить заговор, степень вовлеченности

[4] Раздел уточняет и дополняет материалы статьи [8].

в который варьируется от игрока к игроку (кто-то может наблюдать события из $\mathfrak{S}$ частично или опосредованно, через наблюдение других коррелирующих с ними событий), имеет смысл в первую очередь рассмотреть простейший случай — деление всех игроков на «заговорщиков» $A_{\mathfrak{S}} \subseteq A$, наблюдающих $\mathfrak{S}$ целиком, и «аутсайдеров» $A \setminus A_{\mathfrak{S}}$, в чьём поле зрения только события, не коррелирующие с элементами $\mathfrak{S}$.

Следующий логичный вопрос — о структуре самой тайны. Вполне можно представить, как заговорщики используют в её роли самые разные источники случайности: броски игральных костей, тасование карточных колод, лотерейные розыгрыши и т.д., так что на первый взгляд неочевидно, можно ли ограничиться рассмотрением какого-то одного, естественного в контексте происходящего механизма. Положительный ответ можно получить, используя введённые выше отображения пространств корреляции. Если мы будем сравнивать всевозможные пространства, различающиеся только тайнами группы заговорщиков $A_* \subseteq A$, отношение $\precsim$ вводит на их множестве частичный порядок. Нижней гранью этого порядка будет вырожденное пространство корреляции, в котором тайна заговора состоит из единственного атомарного события с вероятностью $1$ — такое пространство отобразимо на любое другое и, очевидно, вообще не может быть использовано для корреляции стратегий. Верхняя грань интереснее — в её типичном представителе тайна заговора представляет собой произвольное безатомическое [13, с. 81] пространство. Проще всего представить такой механизм корреляции в виде вещественной рулетки, вращение которой генерирует равномерно распределённую случайную величину в единичном полуинтервале $[0, 1)$. Наблюдающие рулетку заговорщики могут, разделяя её на сектора необходимых размеров, согласовать любой набор коррелированных стратегий в играх с конечным множеством исходов. В первую очередь такой универсальный источник случайности и имеет смысл рассматривать как предоставляющий максимум свободы выбора.

Наконец, следует подумать о пространствах корреляции с множественными тайнами. По сути, ничего не мешает игрокам наблюдать сразу несколько рулеток, выбирая в зависимости от ситуации, с кем из оппонентов коррелировать свою стратегию. Более того, стратегия игрока может одновременно существенно зависеть от более чем одной тайны. Таким образом, естественным предметом рассмотрения можно считать пространства корреляции, состоящие из наборов независимых вещественных рулеток, каждая из которых характеризуется подмножеством игроков, имеющих возможность её наблюдать. Остаётся заметить, что

при наличии в одном пространстве корреляции двух и более вещественных рулеток, принадлежащих одному и тому же кругу заговорщиков, все кроме одной можно без ущерба для модели выкинуть, так как в играх с конечными множествами исходов такое дублирование, очевидно, бесполезно. Перейдём теперь к более формальному определению предложенной концепции. Для этого рассмотрим произвольное пространство корреляции $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$. В этом пространстве для каждой непустой группы игроков $A_* \subseteq A$ определим следующее семейство событий[5]:

$$\mathfrak{S}_\Phi^{A_*} = \{U \in \bigcap_{a \in A_*} \mathfrak{I}^a \mid \mathbb{P}(U \cap V) = \mathbb{P}(U)\mathbb{P}(V), \forall V \in \sigma(\bigcup_{a \in A \setminus A_*} \mathfrak{I}^a)\}.$$

Таким образом, $\mathfrak{S}_\Phi^{A_*}$ — множество всех таких событий, что о них осведомлены все члены $A_*$, и каждое событие попарно независимо со всеми событиями, известными не членам $A_*$ даже при объединении их знаний. Поскольку пересечение σ-алгебр образует σ-алгебру, и так как подмножество независимых с некоторым событием событий σ-алгебры также образует σ-алгебру, то $\mathfrak{S}_\Phi^{A_*}$ — σ-алгебра. Это позволяет говорить о вероятностном подпространстве $\langle \Omega, \mathfrak{S}_\Phi^{A_*}, \mathbb{P} \rangle$, которое и называется тайной группы $A_*$. Выделим два случая: тайны с безатомическими мерами мы будем называть *полными*, а тайны с тривиальными атомическими мерами с единственным атомом $\Omega$ — *пустыми*. Это даёт возможность сформулировать следующее:

**Определение 1.3.1.** Пространство корреляции $\langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$ назовём пространством заговоров структуры $\mathfrak{A} = \{A_1, ..., A_n\} \subseteq 2^A$, когда

- $\{\{a\} \mid a \in A\} \subseteq \mathfrak{A}$;
- $\forall A_* \in \mathfrak{A}$ тайна $A_*$ полна;
- $\forall A_* \notin \mathfrak{A}$ тайна $A_*$ пуста;
- $\mathfrak{I}^a = \sigma(\bigcup_{a \in A_* \in \mathfrak{A}} \mathfrak{S}_\Phi^{A_*})$, т.е. $\mathfrak{I}^a$ — наименьшая σ-алгебра, включающая все σ-алгебры тайн групп, в которые входит каждый игрок $a$.

Проще говоря, пространствами заговоров называются такие пространства корреляции, в которых а) тайна любой группы игроков либо полна, либо пуста; б) каждый игрок в отдельности является группой с полной тайной и в) у игроков нет никаких знаний о состоянии природы, которые не порождались бы тайнами

[5] Здесь и далее под $\sigma(\mathfrak{X})$ понимается пополнение семейства множеств $\mathfrak{X}$ до σ-алгебры

групп, которым они принадлежат. Построим для иллюстрации простейший пример такого пространства:

– $A = \{1, 2, 3\}$,
– $\Omega = [0, 1)^2$,
– $\mathfrak{I}^1 = \sigma(\{[0, p_1) \times [0, 1) \mid 0 < p_1 \leqslant 1\})$,
– $\mathfrak{I}^2 = \sigma(\{[0, 1) \times [0, p_2) \mid 0 < p_2 \leqslant 1\})$,
– $\mathfrak{I}^3 = \sigma(\{[0, p_1) \times [0, p_2) \mid 0 < p_1 \leqslant 1, 0 < p_2 \leqslant 1\})$,
– $\mathbb{P}$ — мера Лебега.

В этом примере пространство корреляции состоит из двух независимых вещественных рулеток, первый и второй игроки наблюдают по одной из них, а третий наблюдает обе. При этом выходит, что $\mathfrak{S}_\Phi^{\{1,3\}}$ совпадает с $\mathfrak{I}^1$, $\mathfrak{S}_\Phi^{\{2,3\}}$ совпадает с $\mathfrak{I}^2$, а для остальных групп $A_* \subseteq A$ соответствующая $\mathfrak{S}_\Phi^{A_*}$ тривиальна. Структурой пространства (или *семейством заговоров*) называется множество всех групп игроков с полными тайнами. В вышеприведённом примере структура пространства $\mathfrak{A} = \{\{1,3\},\{2,3\}\}$. С точки зрения допустимых профилей стратегий это означает, что любая группа игроков, входящая в семейство заговоров, может использовать общую тайну для формирования коррелированной стратегии, причём игроки, не входящие в эту группу, не могут присоединиться к согласованному таким образом выбору стратегий. Напротив, группы игроков, не входящие в семейство заговоров, вышеописанной возможностью не располагают. Структуру пространства можно считать его исчерпывающим конечным описанием в силу истинности следующего утверждения:

**Теорема 1.3.1.** *Все пространства заговоров одной структуры изоморфны.*

Доказательство этой теоремы снова представляет собой упражнение в топологии без тесной связи с основными идеями работы и вынесено в приложение B. Теперь, когда установлено, что множество всех пространств заговоров разбивается на классы эквивалентности, нетрудно предложить способ конструирования стандартного представителя каждого класса по соответствующему семейству заговоров:

**Определение 1.3.2.** Стандартным пространством структуры $\mathfrak{A} = \{A_1, A_2, ..., A_n\}$ называется пространство корреляции $\Phi_\mathfrak{A} = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A\rangle$ со следующими параметрами:

– $A = \bigcup\limits_{i=1}^{n} A_i$,

– $\Omega = [0,1)^n$,
– $\mathfrak{I}^a = \sigma(\{\prod_{i=1}^{n} [0,p_i) \mid \textbf{if } a \in A_i \textbf{ then } 0 < p_i \leqslant 1 \textbf{ else } p_i = 1\})$,
– $\mathbb{P}$ — мера Лебега.

Множество состояний природы представляет собой $n$-мерный (по числу заговоров, входящих в семейство) единичный куб, а вероятностная мера соответствует непрерывному равномерному распределению. При этом σ-алгебра каждого игрока борелева в проекциях на оси, соответствующие заговорам в которые он входит, и тривиальна в проекциях на остальные оси. Выделение стандартного представителя для любых семейств заговоров позволяет использовать нотацию $\Gamma|\mathfrak{A}$, под которой в дальнейшем будет пониматься $\Gamma|\Phi_{\mathfrak{A}}$. Эта нотация подчёркивает тот факт, что выбор конкретного пространства корреляции среди всех пространств заговоров необходимой структуры для нас значения не имеет, а стандартное пространство выступает в роли простейшего представителя, пригодного для практических вычислений.

## 1.4 Трёхсторонний чёт-нечет

В качестве элементарного примера конфликта, чувствительного к дополнительной информационной асимметрии, может выступать «трёхсторонний чёт-нечет». В этой игре каждый из трёх участников тайно выбирает «орла» или «решку» на своей монете и прижимает её к столу соответствующей стороной вверх, после чего все одновременно поднимают ладони и в зависимости от сложившейся комбинации делят фиксированный банк. Когда все три монеты лежат одной и той же стороной, раунд считается сыгранным вничью и игроки делят банк поровну. Если же совпали только две из них, то оказавшийся в меньшинстве игрок считается проигравшим и не получает доли при дележе банка. В матричной форме это можно описать так:

Таблица 1 — Трёхсторонний чёт-нечет

| | |
|---|---|
| $4,4,4$ | $6,0,6$ |
| $0,6,6$ | $6,6,0$ |

| | |
|---|---|
| $6,6,0$ | $0,6,6$ |
| $6,0,6$ | $4,4,4$ |

В таблице 1 первый игрок выбирает строку, второй — столбец, а третий — матрицу. Решением этой игры в чистых стратегиях являются два равновесия Нэша, соответствующие синхронным выборам одинаковых сторон всеми игроками. В смешанных стратегиях добавляется ещё одно вырожденное решение, когда каждый игрок делает случайный выбор между орлом и решкой с равными вероятностями. Все эти решения, очевидно, дают математическое ожидание платежей равное $(4,4,4)$. В рамках классической теории игр этим анализ конфликта и исчерпывается, однако добавление фактора информационной асимметрии делает ситуацию интереснее. Рассмотрим эту же игру в пространстве заговоров структуры $\{\{1,2\}\}$, т.е. в ситуации, когда игроки 1 и 2 имеют возможность использовать согласованные втайне от игрока 3 коррелированные стратегии. Пусть $\alpha \in [0,1)$ — значение соответствующей секретной рулетки. Заговорщики могут использовать стратегии вида $\mathbf{s}^1, \mathbf{s}^2 : [0,1) \to P_{\{\mathbf{head},\mathbf{tail}\}}$, где под $P_{\{\mathbf{head},\mathbf{tail}\}}$ понимаются всевозможные вероятностные меры на множестве $\{\mathbf{head}, \mathbf{tail}\}$, т.е. множество классических смешанных стратегий рассматриваемой игры. Аутсайдер же вынужден довольствоваться стратегиями $\mathbf{s}^3 \in P_{\{\mathbf{head},\mathbf{tail}\}}$, поскольку не имеет доступа к рулетке заговора. Для того, чтобы оказаться в более выгодной по сравнению с равным дележом точке равновесия, игроки 1 и 2 могут выбрать любые стратегии, обеспечивающие им равновероятный синхронный выбор стороны монетки:

$$\mathbf{s}^1(\alpha) = \mathbf{s}^2(\alpha) = \begin{cases} (1,0), & \alpha < \frac{1}{2}, \\ (0,1), & \alpha \geqslant \frac{1}{2}. \end{cases}$$

При этом любая смешанная стратегия игрока 3 в силу независимости с рулеткой заговора обеспечивает ему совпадение с остальными ровно в половине случаев. Выплаты в сложившейся ситуации равны $(5,5,2)$, причём ни для одного из игроков нет выгодного индивидуального отклонения.

## 1.5 Необходимая сложность модели заговоров

Классический формализм матричной игры в нормальной форме отождествляет профиль чистых стратегий и исход розыгрыша — они являются буквально одним и тем же математическим объектом. Почти то же самое можно сказать и о

его смешанном расширении — пространство профилей смешанных стратегий изоморфно пространству исходов, состоящему из вероятностных распределений на матрице игры, соблюдающих условие независимости выбора строк и столбцов. Увы, коррелированное расширение в формулировке Роберта Аумана ломает эту идиллическую картину. Пространство исходов розыгрышей в нём даже проще, чем в смешанном случае — распределение вероятностей на множестве элементов игровой матрицы может быть любым, без дополнительных условий. Но вот со стратегическими профилями всё резко становиться сложнее — стратегия каждого игрока представляет собой функцию, отображающую множество состояний природы в множество его чистых стратегий, причём с соблюдением измеримости по σ-алгебре его информированности. Очевидно, что более ни о каком взаимно однозначном соответствии между профилями и исходами не может идти и речи — в зависимости от параметров пространства корреляции некоторые исходы могут оказаться вообще не достижимы, а равновероятные события можно без влияния на исход менять местами в домене стратегий. Вдобавок, работая с коррелированными стратегиями в формулировке Аумана, можно столкнуться с многомерными пространствами событий, борелевскими σ-алгебрами и другими нетривиальными феноменами колмогоровской теории вероятностей, что, вероятно, тоже вносит свой вклад в то, сколь неохотно специалисты теории игр прибегают к этому инструменту в более прикладных исследованиях.

Предложенная здесь модель заговоров сужает коррелированное расширение, выделяя из континуума всевозможных пространств корреляции конечный (для любого конечного числа игроков) набор, по одному на каждую структуру заговоров. На первый взгляд такое радикальное упрощение пространства параметров даёт надежду на то, что и при практическом использовании модели удастся обойтись без «эзотерических» аспектов теории меры. В идеале хотелось бы, чтобы в играх с заговорами можно было тем или иным способом отождествить пространство стратегических профилей и множество исходов, так же, как это происходит в классических формализмах. Если бы мы могли, глядя только на распределение вероятностей реализации отдельных исходов в игровой матрице, определить, какой профиль стратегий (или любой представитель семейства неразличимых профилей) был сыгран игроками, то это означало бы, что мы можем без погружения в детали аумановской модели корреляции найти также и все распределения, достижимые в тех или иных отклонениях от сыгранного профиля стратегий, проверяя тем самым ситуацию на равновесность.

Увы, в общем случае это вряд ли возможно — наглядно показать потерю важной информации при переходе от наборов стратегий к результату корреляции можно при помощи того же самого трёхстороннего чёт-нечета, описанного в предыдущем разделе. Представим себе, что игра ведётся в пространстве заговоров $\{\{1,2\},\{1,2,3\}\}$, то есть, игроки 1 и 2 могут коррелировать свои действия как втайне от игрока 3, так и вместе с ним. Пространство корреляции при этом оказывается состоящим из двух рулеток $\alpha^{1,2}$ и $\alpha^{1,2,3}$, наблюдаемых игроками, указанными в верхних индексах их обозначения. Рассмотрим два набора стратегий: первый —

$$\mathbf{s}^1(\alpha^{1,2},\alpha^{1,2,3}) = \mathbf{s}^2(\alpha^{1,2},\alpha^{1,2,3}) = \begin{cases}(1,0), & \alpha^{1,2,3} < \frac{1}{2},\\ (0,1), & \alpha^{1,2,3} \geqslant \frac{1}{2},\end{cases} \mathbf{s}^3(\alpha^{1,2,3}) = (\frac{1}{2},\frac{1}{2}),$$

и второй —

$$\mathbf{s}^1(\alpha^{1,2},\alpha^{1,2,3}) = \mathbf{s}^2(\alpha^{1,2},\alpha^{1,2,3}) = \begin{cases}(1,0), & \alpha^{1,2} < \frac{1}{2},\\ (0,1), & \alpha^{1,2} \geqslant \frac{1}{2},\end{cases} \mathbf{s}^3(\alpha^{1,2,3}) = (\frac{1}{2},\frac{1}{2}).$$

В обоих случаях все игроки делают равновероятный выбор между орлом и решкой, причём первые два игрока делают его синхронно, а третий — независимо от них. Если записать распределение вероятностей отдельных исходов в матрице $2\times2\times2$, соответствующей игровой из таблицы 1, то для обоих наборов это будет выглядеть так: $\begin{array}{|c|c|}\hline \frac{1}{4} & 0\\ \hline 0 & \frac{1}{4}\\ \hline\end{array}$ $\begin{array}{|c|c|}\hline \frac{1}{4} & 0\\ \hline 0 & \frac{1}{4}\\ \hline\end{array}$. Понятное дело, платежи здесь также равны и составляют $(5,5,2)$. Тем не менее, если присмотреться, можно обнаружить, что в первом случае игроки 1 и 2 используют для синхронизации общую с игроком 3 рулетку $\alpha^{1,2,3}$, что позволяет ему, изменив свою стратегию на

$$\mathbf{s}^3(\alpha^{1,2,3}) = \begin{cases}(1,0), & \alpha^{1,2,3} < \frac{1}{2},\\ (0,1), & \alpha^{1,2,3} \geqslant \frac{1}{2},\end{cases}$$

присоединиться к ним и перейти в исход с распределением вероятностей $\begin{array}{|c|c|}\hline \frac{1}{2} & 0\\ \hline 0 & 0\\ \hline\end{array}$ $\begin{array}{|c|c|}\hline 0 & 0\\ \hline 0 & \frac{1}{2}\\ \hline\end{array}$, где выплаты составляют $(4,4,4)$. Таким образом, первая точка не является равновесием Нэша. Во втором же случае игроки 1 и 2 используют для синхронизации приватную рулетку $\alpha^{1,2}$, исход которой игрок 3 наблюдать не может. Какую бы стратегию он ни выбрал, совпадёт со стратегиями заговорщиков она ровно в половине случаев, а значит выплаты не изменятся. Так как

у остальных игроков выгодных отклонений тоже нет, эта ситуация уже будет равновесием Нэша.

Таким образом, мы построили пример, в котором одному и тому же распределению вероятностей исходов в матрице игры соответствуют как минимум два настолько различных набора стратегий, что один из них является равновесием Нэша, а второй — нет. Очевидно, что никаким разумным способом объединить эти наборы в одном классе эквивалентности нельзя, а значит отождествление игровых ситуаций и исходов розыгрыша в общем случае невозможно, как бы мы ни старались. Следует, впрочем, заметить, что в более простых случаях, когда каждый игрок может входить не более чем в один заговор, построить такой наглядный и тривиальный контрпример уже не получится — если корреляция, проявляющаяся в распределении вероятностей на матрице игры, могла бы быть получена только одним способом, то при решении практических задач ничего не мешает оперировать именно распределениями вероятностей, а не функциями, отображающими сигналы в исходы. Однако, если рассматривать теорию заговоров как способ моделирования информационных асимметрий, складывающихся в ходе реальных процессов взаимодействия независимых агентов в неконтролируемой среде, то подобное самоограничение, увы, загнало бы нас в рамки, не имеющие естественного обоснования.

# Глава 2. Коллективная рациональность в играх с заговорами

## 2.1 Проблема планирования заданий[1]

Концепция равновесия по Нэшу, будучи фундаментом классических моделей теории игр, сама по себе зачастую оказывается недостаточно сильным формализмом. При анализе многосторонних конфликтов нередко возникают ситуации, когда множество равновесий по Нэшу слишком велико, чтобы считать его полноценным решением игры. В этом случае на помощь исследователям приходят критерии коллективной рациональности — выбирая среди равновесных точек оптимальные по Парето или Слейтеру, иногда можно значительно сузить пространство решений за счёт вполне естественного исключения заведомо невыгодных для всех участников. Присутствие дополнительной информационной асимметрии при этом создаёт дополнительные затруднения, поскольку предлагаемая модель подразумевает неизбежный элемент антагонизма интересов — в новых точках равновесия увеличение выигрышей участвующих в корреляции происходит за счёт сокращения выплат тех, кто не может к ней присоединиться, тем самым делая непродуктивными обычные критерии коллективной рациональности. Для демонстрации этого эффекта рассмотрим тривиальное обобщение классической проблемы планирования заданий [14], занимающей важное место в концептуальном ландшафте теории игр. При помощи этого конфликта хорошо иллюстрируются понятия *цены анархии* и *цены стабильности*, давая вероятно самый выразительный пример того, насколько равновесия Нэша в одной и той же игре могут различаться в смысле их глобальной оптимальности. Нам, однако, необходимо взглянуть на эту игру под другим углом, при котором понятие цен анархии и стабильности теряет смысл, уступая место чувствительности к дополнительной информационной асимметрии.

Начнём с классической модели планирования заданий. В вычислительном центре работают $m$ сотрудников, каждому из которых поручено произвести некое вычисление. В их распоряжении находятся $n$ компьютеров, на каждом из которых может быть запущена одна или несколько программ, производящих вычисления сотрудников. Машины отличаются архитектурными особенностями, что задаёт-

[1] Раздел уточняет и дополняет материалы статьи [10].

ся матрицей констант $t_i^a \geqslant 0$, обозначающих время выполнения программы сотрудника $a = \overline{1,\ldots,m}$ на компьютере $i = \overline{1,\ldots,n}$. Каждое вычисление может производиться только одним устройством. Несколько программ на одном компьютере выполняются последовательно, но результаты их работы выводятся одновременно после остановки последней из них. Таким образом, выгода сотрудника заключается в выборе такого компьютера для своего вычисления, что для него оказывается минимальным суммарное время выполнения всех запущенных программ. Опишем происходящее в терминах игры нормальной формы

$$\Gamma = \langle A, S^a, u^a(s), a \in A \rangle \tag{2.1}$$

с параметрами:

- $A = \{1,\ldots,m\}$;
- $S^1 = \ldots = S^m = \{1,\ldots,n\}$;
- $u^a(s) = -t_{s^a}(s)$, где $t_i(s) = \sum\limits_{a \in A, s^a = i} t_i^a$.

Здесь следует заострить внимание на определении функции выплат. Выбрав $u^a(s) = -t_{s^a}(s)$, мы моделируем ситуацию, когда все вычисления должны были быть готовы ещё вчера, и сотрудники напрямую штрафуются за каждую лишнюю секунду, пока их результаты не лягут на стол начальству. Однако, можно смоделировать и менее напряжённый рабочий момент, взяв, например, ступенчатую функцию выплат:

$$u^a(s) = \begin{cases} u^a_{GOOD}, & t_{s^a}(s) < t^a_{DEADLINE}; \\ u^a_{LATE}, & t_{s^a}(s) \geqslant t^a_{DEADLINE}. \end{cases}$$

При этом получается, что для каждого игрока $a$ назначен срок успешного выполнения задания $t^a_{DEADLINE}$, уложившись в который, он получает фиксированную выплату $u^a_{GOOD}$ (с учётом премии), а не уложившись — $u^a_{LATE}$ (обычную ставку). Можно придумать и более сложные схемы поощрения сотрудников, так что сформулируем сразу в общем виде:

$$u^a(s) = v^a(t_{s^a}(s)), \tag{2.2}$$

где $v^a(t)$ — монотонно невозрастающая функция оплаты за срочность по заданию сотрудника $a$. Любая игра в нормальной форме, построенная по схеме 2.1 с платёжной функцией вида 2.2, в сущности является проблемой планирования задач. При этом условие монотонного невозрастания $v^a(t)$ необходимо, поскольку

на него в явном виде опирается доказательство считающегося важным свойства этой игры — равенство 1 цены стабильности [15]. Напомним, в оптимизационных задачах с эгоистичными агентами цена стабильности представляет собой соотношение $\frac{t_{NASH}}{t_{BEST}}$, где $t_{NASH}$ — значение наилучшего из равновесий Нэша, а $t_{BEST}$ — значение глобально оптимального решения. Это означает, что в проблеме планирования задач среди всех ситуаций, минимизирующих время до остановки последнего компьютера, обязательно найдутся равновесия по Нэшу. Однако, в данной работе предлагается на время забыть о минимизации общей продолжительности вычислений и вместо этого проанализировать, какие новые свойства модели могут проявиться в отсутствие такого ограничения на монотонность.

## 2.2 Штраф за индивидуализм[2]

Представим вычислительный центр с компьютерами, требующими сложного техобслуживания после смены, если на них запускали хотя бы одну задачу. Если поощрять укладывающихся в дедлайны сотрудников невзирая на это, несложно представить ситуацию, когда они, в стремлении любой ценой гарантировать себе премию, будут раскидывать задачи по неразумно большому количеству компьютеров. Перед лицом такой перспективы у руководства может возникнуть соблазн стимулировать своих сотрудников избегать систематической недозагрузки машин при помощи штрафов. Это может быть смоделировано ступенчатой функцией оплаты за срочность следующего вида:

$$v^a(t) = \begin{cases} u^a_{HAST}, & t < t^a_{BREAKAWAY}; \\ u^a_{GOOD}, & t^a_{BREAKAWAY} \leqslant t < t^a_{DEADLINE} \quad ; \\ u^a_{LATE}, & t^a_{DEADLINE} \quad \leqslant t \qquad\qquad . \end{cases}$$

Здесь для каждого сотрудника $a$ зафиксирован не только дедлайн $t^a_{DEADLINE}$, к которому требуется успеть, чтобы получить премию, но и минимальная загруженность используемого компьютера $t^a_{BREAKAWAY}$, которой нужно достигнуть, чтобы не нарваться на штраф за нерациональное расходование вычислительных ресурсов (причём $u^a_{HAST} < u^a_{LATE} < u^a_{GOOD}$). Размер минимальной загруженности может устанавливаться, например, в зависимости

[2] Раздел уточняет и дополняет материалы статьи [10].

от важности соответствующей задачи — если срочное получение результата окупает использование дополнительных машин, то его можно сделать пониже или вовсе приравнять к нулю. Если же наоборот задача не так уж и важна, то большая минимальная загруженность заставит соответствующего сотрудника вспомнить об интересах фирмы и скооперироваться с коллегами.

Как видно, сотрудникам в данном случае приходится руководствоваться немонотонной функцией оплаты за срочность, что создаёт некоторые эффекты, несвойственные для классической формулировки проблемы планирования заданий. Во-первых, при такой постановке ожидаемо не во всякой игре цена стабильности обязана равняться 1. Достаточно рассмотреть игру с 2 сотрудниками и 2 одинаковыми компьютерами:

- $t_1^1 = t_2^1 = 8$,
  $t_1^2 = t_2^2 = 2$;
- $t_{DEADLINE}^1 = t_{DEADLINE}^2 = 9$,
  $t_{BREAKAWAY}^1 = t_{BREAKAWAY}^2 = 3$;
- $u_{HAST}^1 < u_{LATE}^1 < u_{GOOD}^1$,
  $u_{HAST}^2 < u_{LATE}^2 < u_{GOOD}^2$.

Поскольку первый игрок, заведомо не имеющий проблем с недозагрузкой, укладывается в дедлайн только если компьютер будет в его безраздельном пользовании, то очевидно, что сочетания стратегий, в которых оба игрока выбирают одну машину, равновесиями Нэша быть не могут. Похожим образом, поскольку второму игроку выгоднее опоздать с расчётами нежели быть наказанным за использование отдельного компьютера для недостаточно большой задачи ($u_{HAST}^a < u_{LATE}^a$), равновесиями Нэша не могут быть и те ситуации, где каждый из сотрудников использует свою машину. По структуре выплат игра оказывается неотличима от игры в чёт-нечет, вовсе не имеющей решений в чистых стратегиях и с единственным равновесием Нэша в точке независимого равновероятного выбора между альтернативами обоими игроками. При этом максимально загруженная машина с вероятностью $\frac{1}{2}$ проработает либо 10 часов при совпадении их выбора, либо 8 при несовпадении, что даёт математическое ожидание цены стабильности, равное $\frac{9}{8}$. По сути, при отказе от монотонности функции оплаты за срочность вряд ли имеет смысл вообще рассуждать о ценах стабильности и анархии, поскольку класс игр теперь начинает включать и такие, которые явно не имеют отношения к поискам минимума продолжительности вычислений.

## 2.3 Смешанные равновесия игры $\Gamma_n^3$[3]

Планирование заданий с немонотонной отдачей представляет собой довольно обширный класс конфликтов, анализ которого в общем виде выходит за рамки данной работы. Для наглядной демонстрации необходимого эффекта вполне достаточно будет специально сконструированного примера. Рассмотрим игру $\Gamma_n^3$ той же общей схемы, что в предыдущем разделе, но чуть боле сложную, с $3$ однотипными заданиями и $n \geqslant 2$ одинаковыми компьютерами:

- $t_i^1 = t_i^2 = t_i^3 = 2, i = \overline{1,n}$;
- $t_{DEADLINE}^1 = t_{DEADLINE}^2 = t_{DEADLINE}^3 = 5$,
  $t_{BREAKAWAY}^1 = t_{BREAKAWAY}^2 = t_{BREAKAWAY}^3 = 3$;
- $u_{HAST}^1 = u_{HAST}^2 = u_{HAST}^3 = 0$,
  $u_{GOOD}^1 = u_{GOOD}^2 = u_{GOOD}^3 = 3$,
  $u_{LATE}^1 = u_{LATE}^2 = u_{LATE}^3 = 2$

Проще говоря, в игре $\Gamma_n^3$ выгоднее всего использовать компьютер вдвоём — $4$ часа суммарной продолжительности работы оказываются как раз в оптимальном промежутке между границей недогруза и дедлайном. Следующий по выгоде вариант — использование одной машины втроём, что приводит к штрафу за опоздание. Наименее привлекателен выбор компьютера, на котором задача оказывается одна — за такое расходование общественного ресурса игрок не получает вообще ничего. На первый взгляд эта игра не выглядит слишком необычно. В ней без особого труда находятся равновесия Нэша в чистых стратегиях — все наборы $(i,i,i), i = \overline{1,n}$, причём очевидно и то, что других решений в чистых стратегиях быть не может. Со смешанными стратегиями дело становится чуть интереснее.

**Лемма 2.3.1.** *Пусть $S_* \subseteq \{1,\ldots,n\}$ — произвольное непустое подмножество компьютеров. Тогда в игре $\Gamma_n^3$ набор одинаковых смешанных стратегий $s^1 = s^2 = s^3 = \left(\frac{[1\in S_*]}{|S_*|},\ldots,\frac{[n\in S_*]}{|S_*|}\right)$, где каждый игрок независимо и равновероятно выбирает одну из машин множества $S_*$, является равновесием по Нэшу.*[4]

*Доказательство.* Воспользуемся тем, что достаточно проверить отклонения только в пользу чистых стратегий. Обозначим символом $s|_i^a$ отклонение от набо-

[3] Раздел уточняет и дополняет материалы статьи [10].

[4] Здесь и далее для упрощения и сокращения записи используется нотация «скобка Айверсона»: $[\text{TRUE}] = 1, [\text{FALSE}] = 0$.

ра $s$ игроком $a$ в пользу стратегии $i$ и заметим, что

$$u^a(s|_i^a) = [i \in S_*]\left(\frac{(|S_*|-1)^2}{|S_*|^2}u^a_{HAST} + 2\frac{|S_*|-1}{|S_*|^2}u^a_{GOOD} + \frac{1}{|S_*|^2}u^a_{LATE}\right)$$
$$= [i \in S_*]\frac{6\,|S_*|-4}{|S_*|^2}.$$

Таким образом, для каждого игрока максимум ожидаемого выигрыша достигается при отклонении в пользу любого из компьютеров, входящих в $S_*$. □

Соответственно без отклонений математическое ожидание выигрышей предстаёт в виде $u^a(s) = \frac{6|S_*|-4}{|S_*|^2}, a = \overline{1,3}$. Для доказательства того, что других равновесий по Нэшу в смешанных стратегиях нет, нам понадобятся ещё пара лемм:

**Лемма 2.3.2.** *В игре $\Gamma_n^3$ набор смешанных стратегий $s = (s^1, s^2, s^3)$ может быть равновесием по Нэшу только в том случае, когда $s^1 = s^2 = s^3$.*

*Доказательство.* Пусть $s^a = (p_1^a, \ldots, p_n^a), a = \overline{1,3}$. Если стратегии игроков не совпадают, то найдётся компьютер $i$, для которого (без потери общности) вероятности выбора первым и вторым игроком $p_i^1 > p_i^2$. В силу элементарных свойств вероятностей, найдётся также и компьютер $j$, где $p_j^1 < p_j^2$. Выпишем математическое ожидание выигрышей тех же игроков при выборе ими $i$-го компьютера (для $j$-го всё совпадает с точностью до индекса, очевидно):

$$u^1(s|_i^1) = (1-p_i^2)(1-p_i^3)u^1_{HAST} + (p_i^2 + p_i^3 - 2p_i^2p_i^3)u^1_{GOOD} + p_i^2p_i^3u^1_{LATE}$$
$$= 3p_i^2 + 3p_i^3 - 4p_i^2p_i^3;$$
$$u^2(s|_i^2) = 3p_i^1 + 3p_i^3 - 4p_i^1p_i^3;$$
$$u^3(s|_i^3) = 3p_i^1 + 3p_i^2 - 4p_i^1p_i^2.$$

Про функцию $f(x,y) = 3x + 3y - 4xy$ на области определения $0 \leqslant x \leqslant 1, 0 \leqslant y \leqslant 1$ можно заметить следующее — если $f(x_0, y_0) < 2$, то для любых $x_1 > x_0, y_1 \geqslant y_0$ или $x_1 \geqslant x_0, y_1 > y_0$ выполняется $f(x_0, y_0) < f(x_1, y_1)$. Предположим, что $p_i^3 \leqslant p_j^3$ (если $p_i^3 \geqslant p_j^3$, рассуждения аналогичны с точностью до индексов). Рассмотрим следующие случаи:

– $p_i^2 < p_j^2$. В силу элементарных свойств вероятностей мы можем быть уверены, что $p_i^2 < \frac{1}{2}$ и $p_i^3 \leqslant \frac{1}{2}$, откуда $u^1(s|_i^1) < 2$, а значит $u^1(s|_i^1) < u^1(s|_j^1)$. Поскольку $p_i^1 > p_i^2 \geqslant 0$, первый игрок выбирает неоптимальную стратегию с ненулевой вероятностью. ⊥

– $p_i^2 \geqslant p_j^2$, из чего следует $p_i^1 > p_j^1$, а значит аналогично предыдущему пункту $u^3(s|_j^3) < u^3(s|_i^3)$. Если $p_j^3 > 0$, то третий игрок выбирает неоптимальную стратегию с ненулевой вероятностью. $\perp$
– $p_i^2 \geqslant p_j^2$, как и в предыдущем случае, но теперь $p_i^3 = p_j^3 = 0$. Из $p_j^1 < p_i^1$ аналогичным образом следует $u^2(s|_j^2) < u^2(s|_i^2)$, и поэтому $p_j^2 > p_j^1 \geqslant 0$ влечёт выбор неоптимальной стратегии с ненулевой вероятностью уже вторым игроком. $\perp$

Таким образом, предположение о существовании компьютера, для которого вероятность выбора его одним игроком отличается от вероятности выбора другим, в любом случае противоречит необходимому условию равновесия Нэша. □

**Лемма 2.3.3.** *В игре $\Gamma_n^3$ набор одинаковых смешанных стратегий может быть равновесием по Нэшу только в том случае, когда все компьютеры, выбираемые с ненулевой вероятностью, выбираются с равными вероятностями.*

*Доказательство.* Возьмём любой набор, состоящий из одинаковых стратегий $(p_1, \ldots, p_n)$, где $0 < p_i < p_j$. Пользуясь формулой выплат из предыдущей леммы, $u^a(s|_i^a) = 2p_i(3 - 2p_i)$. Опять же, из $p_i < \frac{1}{2}$ следует $u^a(s|_i^a) < u^a(s|_j^a)$, а значит все игроки выбрали неоптимальную стратегию с ненулевой вероятностью, что противоречит необходимому условию равновесия по Нэшу. □

Доказав, что предложенные точки равновесия исчерпывают пространство решений в смешанных стратегиях, мы можем сконструировать выпуклую оболочку множества достижимых векторов выплат. Поскольку множество целиком лежит на прямой $(u, u, u)$, достаточно найти минимум и максимум ожидаемых выигрышей:

$$\min_{\varnothing \subset S_* \subseteq \{1,\ldots,n\}} \frac{6\,|S_*| - 4}{|S_*|^2} = \frac{6n-4}{n^2};$$
$$\max_{\varnothing \subset S_* \subseteq \{1,\ldots,n\}} \frac{6\,|S_*| - 4}{|S_*|^2} = 2.$$

Таким образом искомая выпуклая оболочка представляет собой отрезок, соединяющий точки $(2, 2, 2)$ и $(\frac{6n-4}{n^2}, \frac{6n-4}{n^2}, \frac{6n-4}{n^2})$. Если бы рассматриваемая игра не была чувствительна к дополнительной информационной асимметрии, на этом её анализ можно было бы закончить — все игроки находятся в равном положении и,

действуя оптимально, могут ожидать равных выигрышей из указанного промежутка. Однако, взгляд на этот конфликт через призму модели заговоров делает картину происходящего куда интереснее.

## 2.4 Коррелированные равновесия игры $\Gamma_n^3$ в пространстве заговоров[5]

Проанализируем этот же конфликт с позиций теории заговоров, перейдя к игре $\Gamma_n^3|\{\{1,2\}\}$. При этом игра $\Gamma_n^3$ дополняется одной вещественной рулеткой, результат вращения которой перед выбором стратегии узнают игроки 1 и 2, но не 3. Для получения равновесного набора коррелированных стратегий, выводящего платежи за выпуклую оболочку множества решений в смешанных стратегиях, заговорщикам достаточно взять любую из классических точек равновесия по Нэшу с $|S_*| \geqslant 2$, но вместо того, чтобы выбирать между элементами $S_* \subseteq \{1,\ldots,n\}$ независимо, они должны разделить тайную рулетку на $|S_*|$ равных секторов и делать свой выбор синхронно, в зависимости от выпавшего сектора. Опишем это более формально, используя пространство корреляции

$$\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$$

В данном случае множество состояний природы $\Omega = [0,1)$, σ-алгебры информированности игроков $\mathfrak{I}^1 = \mathfrak{I}^2$ — борелевские, $\mathfrak{I}^3 = \{\varnothing, \Omega\}$ и мера $\mathbb{P}(X) = |X|$. Вышеописанные стратегии в игре $\Gamma_n^3|\Phi$ можно представить в виде функций, отображающих множество состояний природы в пространство смешанных стратегий:

$$\mathbf{s}^1(\omega) = \mathbf{s}^2(\omega) = ([\zeta(\omega) = 1], \ldots, [\zeta(\omega) = n]);$$
$$\mathbf{s}^3(\omega) = \left( \frac{[1 \in S_*]}{|S_*|}, \ldots, \frac{[n \in S_*]}{|S_*|} \right),$$

где общая для игроков 1 и 2 функция $\zeta : \Omega \to S_*$ определяет разбиение рулетки на $|S_*|$ равных секторов.

[5] Раздел уточняет и дополняет материалы статьи [10].

Выплаты в этом наборе уже не симметричны:

$$u^1(\mathbf{s}) = u^2(\mathbf{s}) = \frac{|S_*|-1}{|S_*|}u^a_{GOOD} + \frac{1}{|S_*|}u^a_{LATE} = \frac{3\,|S_*|-1}{|S_*|};$$
$$u^3(\mathbf{s}) = \frac{|S_*|-1}{|S_*|}u^a_{HAST} + \frac{1}{|S_*|}u^a_{LATE} = \frac{2}{|S_*|}.$$

При этом ситуация действительно является равновесием по Нэшу, поскольку первый и второй игроки могут в качестве стратегий использовать любые функции, отображающие $\Omega$ в пространство вероятностных мер на $\{1,\ldots,n\}$, а вот третий игрок вынужден довольствоваться только константными в виду того, что механизм корреляции не информирует его о состоянии природы. Заметив, что $\frac{3|S_*|-1}{|S_*|} > 2$ при $|S_*| \geqslant 2$, мы подтверждаем чувствительность игры $\Gamma^3_n$ к дополнительной информационной асимметрии — в новых решениях игроки, наблюдающие не связанный напрямую с выплатами случайный эксперимент, увеличивают свой выигрыш по сравнению с наилучшим результатом, достижимым в классическом смешанном случае.

## 2.5 Коллективная рациональность решений[6]

При рассмотрении множества решений игры $\Gamma^3_n$ в обычных смешанных стратегиях следует обратить внимание на то, что при $|S_*| > 2$ получающиеся точки равновесия по Нэшу лишены оптимальности не только в смысле Парето, но и по Слейтеру. В самом деле, выплаты всем игрокам в точках, где $|S_*| = 1$ или $|S_*| = 2$, равны 2, а вот при больших размерах множества $\frac{6|S_*|-4}{|S_*|^2} < 2$. Такие обстоятельствах наделяют решения с использованием одного или двух компьютеров особым статусом — можно ожидать, что агенты, знакомые с принципом коллективной рациональности, всё же сумеют договориться о том, чтобы не оказаться в ситуации, которую другое решение доминирует по всем платежам. Естественно сразу задаться вопросом, а нельзя ли и решения с учётом дополнительной информационной асимметрии отфильтровать похожим образом, выделив из них удовлетворяющие принципам коллективной рациональности хоть в каком-то смысле?

[6] Раздел уточняет и дополняет материалы статьи [10].

При добавлении в игру пространства заговоров, состоящего из группы $\{1, 2\}$, сразу бросается в глаза то, что классические принципы коллективной рациональности становится бесполезны. В новых точках равновесия выигрыши первых двух игроков теперь $u^1(\mathrm{s}) = u^2(\mathrm{s}) > 2$ и растут с ростом $k$, а третьего — $u^3(\mathrm{s}) < 2$ и падают, что говорит о прямом антагонизме интересов. Это делает невозможным коллективно рациональный выбор в обычном смысле между смешанным равновесием с $|S_*|$ равным 1 или 2 и коррелированными решениями с различными $k$. Тем не менее, можно попытаться применить более тонкий критерий оптимальности, опирающийся на слегка расширенную интерпретацию происходящего в игре — назовём этот формализм *структурно согласованным равновесием по Нэшу*.

Идея структурной согласованности равновесий в играх с заговорами довольно проста — если допустить, что входящие в семейство заговоров группы игроков объединяет не только общий механизм корреляции, но и в целом большие возможности для согласования действий, то среди обычных равновесий по Нэшу в коррелированных стратегиях можно особо выделить обладающие устойчивостью не только к индивидуальным отклонениям, но и к групповым, имея в виду исключительно входящие в семейство заговоров группы. Для игры $\Gamma_n^3|\{\{1{,}2\}\}$, например, это могло бы означать, что структурно несогласованными окажутся те равновесия, для которых найдётся отклонение, в котором участвуют первый и второй игроки, обоюдно увеличивая при этом свои выигрыши. В наиболее общих терминах это можно выразить так:

**Определение 2.5.1.** В игре с заговорами $\Gamma|\mathfrak{A}$ равновесие по Нэшу $\mathrm{s}$ называется структурно согласованным, если для всех заговоров $A_* \in \mathfrak{A}$ отсутствуют приемлемые отклонения от ситуации $\mathrm{s}$.

Остаётся сформулировать, что в рамках данной модели можно считать отклонением, приемлемым для того или иного заговора. Если взглянуть на этот вопрос как на проблему многокритериальной оптимизации, где критериями являются выигрыши отдельных участников, то напрашиваются два варианта:

1. Отклонение приемлемо, если оно увеличивает выигрыш всех участников заговора; (по Слейтеру)
2. Отклонение приемлемо, если оно увеличивает выигрыш хотя бы одного участника заговора, при этом не уменьшая выигрыша остальных. (по Парето)

Увы, оба варианта нельзя назвать подходящими для наших целей. Разумно было бы ожидать, что добавление в любой заговор «болвана», т.е. игрока с единственной чистой стратегией и константным выигрышем, не должно ничего менять в решении игры. Однако, заговор с подобным «болваном» в составе вообще не может иметь приемлемых отклонений в смысле Слейтера, а значит его участники теряют возможность использовать коллективную рациональность. Это делает первый из предложенных вариантов, очевидно, слишком слабым. С другой же стороны, рассмотрение игры в трёхсторонний чёт-нечет (см. 1.4) с двумя заговорами порождает неприятную проблему и для второго варианта. Если 1-й игрок находится в заговоре со 2-м, а 2-й с 3-м, то можно ожидать исходов с платежами, образованными любым смешением $(5,5,2)$ и $(2,5,5)$, причём выбор пропорции происходит по воле 2-го игрока. Загвоздка в том, что приемлемость в смысле Парето побуждает 2-го игрока в ситуации $(5,5,2)$ отклоняться в рамках заговора с 3-м для улучшения чужого выигрыша. Аналогично, в ситуации $(2,5,5)$ 2-му игроку приходится спасать 1-го. В промежуточных же ситуациях 2-й игрок может помочь обоим, а значит подобный альтруизм вообще исключает существование структурно согласованного равновесия в задаче, делая второй вариант определения приемлемости слишком сильным. Для обхода обоих проблем следует предложить промежуточное определение отклонения, которое будет сильнее чем по Слейтеру, но слабее чем по Парето:

**Определение 2.5.2.** В игре с заговорами $\Gamma|\mathfrak{A}$ ситуацию $\mathbf{s}_* \neq \mathbf{s}$ назовём отклонением от $\mathbf{s}$, приемлемым для заговора $A_* \in \mathfrak{A}$, если

– $\forall a \notin A_* \quad \mathbf{s}^a = \mathbf{s}^a_*$;
– $\forall a \in A_* \quad u^a(\mathbf{s}_*) \geqslant u^a(\mathbf{s})$;
– $\forall a : \mathbf{s}^a \neq \mathbf{s}^a_* \quad u^a(\mathbf{s}_*) > u^a(\mathbf{s})$.

Несложно заметить, что предлагаемый критерий оптимальности родственен концепции сильного равновесия по Нэшу [16], подразумевающей устойчивость к всевозможным групповым отклонениям, приносящим выгоду всем своим участникам. По сути, структурно согласованное равновесие можно считать модификацией сильного, отличающейся в двух аспектах, один из которых его заметно ослабляет, а другой немного усиливает. Ослабление проистекает из того, что коллективные отклонения разрешены не всевозможным группам игроков, а только входящим в структуру заговоров. К усилению же приводит то, что критерием успеха для отклонения считается получение прибыли не всеми членами группы,

а только теми, кто в отклонении активно участвует, меняя свою стратегию, тогда как пассивные наблюдатели из той же группы могут довольствоваться отсутствием убытков.

Если бы мы говорили только о равновесиях Нэша в чистых и смешанных стратегиях, даже такой критерий оптимальности оказался бы слишком сильным — действительно, одновременный выбор первым и вторым игроками компьютера $i$, выбираемого третьим с вероятностью $p_i^3 < 1$, даёт обоим выигрыш $(1 - p_i^3)u^a_{GOOD} + p_i^3 u^a_{LATE} = 3 - p_i^3 > 2$, что отсеивает вообще все решения в игре $\Gamma_n^3$. Для игры с заговорами же можно сформулировать следующее:

**Теорема 2.5.1.** *В игре с заговорами $\Gamma_n^3|\mathfrak{A}$ структурно согласованное равновесие Нэша существует при любых $n$ и $\mathfrak{A}$. При невырожденном $\mathfrak{A}$, каждому заговору из двух участников соответствует единственное такое равновесие.*

*Доказательство.* Возможны три случая в зависимости от $\mathfrak{A}$:

1. $\mathfrak{A} = \varnothing$. При пустом семействе заговоров групповые отклонения невозможны, так что любое равновесие по Нэшу в чистых или смешанных стратегиях будет структурно согласованным.
2. $\mathfrak{A} = \{\{1, 2, 3\}\}$. При вырожденном семействе заговоров с одним публичным механизмом корреляции множество решений представляет собой выпуклую оболочку векторов платежей смешанных равновесий, что, как было показано в разделе 2.3, даёт отрезок, соединяющий $(2, 2, 2)$ и $(\frac{6n-4}{n^2}, \frac{6n-4}{n^2}, \frac{6n-4}{n^2})$. При этом критерий структурной согласованности, очевидно, отсеивает всё, кроме точки $(2, 2, 2)$, соответствующей чистым равновесиям с выбором одной любой общей стратегии на всех и смешанным равновесиям с независимым равновероятным выбором из двух любых одних и тех же стратегий каждым игроком.
3. $\mathfrak{A}$ содержит $\{1, 2\}$, $\{1, 3\}$ или $\{2, 3\}$. Как было показано в разделе 2.4, использование тайных механизмов корреляции даёт новые точки равновесия с выплатами $\frac{3k-1}{k}$ участникам заговора и $\frac{2}{k}$ аутсайдеру, где $k$ — количество задействованных в наборе стратегий машин. Поскольку при $k \geqslant 2$ выигрыш каждого из заговорщиков превосходит наилучший классический результат, никакие точки смешанного равновесия структурно согласованными уже не будут. Поскольку с ростом $k$ растут и выигрыши заговорщиков, отсеиваются также и все коррелированные равновесия, кроме максимизирующих доход любой из пар заговорщиков при $k = n$.

Таким образом, каждой группе, входящей в структуру заговоров, соответствует одна (с точностью до пермутаций рулеток) точка структурно согласованного равновесия, в которой игроки выбирают равновероятно из всего доступного парка машин, причём выбор членов группы всегда совпадает между собой и независим с выбором оставшегося игрока.

□

Для новых структурно согласованных равновесий несложно подобрать вполне естественную интерпретацию. Если представить, что два сотрудника могут координировать свои действия втайне от третьего, то нет ничего неожиданного в их стремлении выбрать один компьютер на двоих, чтобы избежать штрафа за недозагруз, минимизируя при этом шанс для третьего игрока наткнуться на них по воле случая, лишив их премии за срочность. Достигается это логичным образом тогда, когда наибольшая вероятность выбора каждой из машин минимальна, т.е. при равновероятном выборе из всех. Аналогичным образом, для третьего игрока целью становится максимизация наименьшей вероятности выбора каждого из компьютеров, поскольку он понимает, что заговорщики действуют заодно и пытаются избежать встречи с ним, и это тоже достигается в ситуации равновероятного выбора из всего парка машин.

Таким образом именно объединение в заговорах способности к групповому отклонению с наличием тайного механизма корреляции позволяет получать в игре $\Gamma_n^3|\mathfrak{A}$ решения, отвечающие критериям одновременно коллективной и индивидуальной рациональности. Заметим, что в отсутствие дополнительной информационной асимметрии игра $\Gamma_n^3$ не имеет таких решений даже при использовании более тонкого и сложного по сравнению с сильными равновесиями формализма коалиционно-устойчивого равновесия по Нэшу [17]. Это делает критерий структурной согласованности мощным инструментом для исследования конфликтов, провоцирующих своих участников на тайное согласование действий. Важно, впрочем, понимать, что структурно согласованное равновесие найдётся не во всякой игре с заговорами — очевидным примером может служить классическая дилемма заключённого, где коллективная и индивидуальная рациональности находятся в непримиримом противоречии, которое, конечно же, не снимается добавлением механизма корреляции.

## 2.6 Сохранение тайн заговоров в процессе выработки консенсуса

Как известно, в матричных играх нередко наличествуют несколько точек равновесия по Нэшу (например, координационные игры), причём наборы, состоящие из стратегий, принадлежащих к разным точкам, сами равновесиями не являются. При интерпретации таких точек равновесия в качестве решений игры приходится оговаривать, что выбор игроками равновесных стратегий в сущности не является независимым — предпочтение одной точки равновесия другой должно носить характер консенсуса среди игроков. В классических играх с полной информацией это не создаёт больших проблем, поскольку процедура, приводящая к консенсусу, вполне может быть гласной. Однако, когда речь заходит о моделировании конфликтов с заговорами, данный вопрос начинает требовать гораздо более осторожного подхода. При появлении в игре информационной асимметрии, существенно влияющей на её исход, игрокам может становиться выгодно изменять картину этой асимметрии (оповещая, к примеру, о значении тайного сигнала игроков, которые не должны его знать в соответствии со структурой пространства корреляции), для чего при неправильном дизайне могут использоваться те самые механизмы выработки консенсуса. Для того чтобы понять, что может пойти не так, имеет смысл начать с классического случая. Если представить произвольную матричную игру в виде реального процесса с живыми игроками под управлением беспристрастного ведущего, следящего за соблюдением протокола игры, то для получения равновесия по Нэшу можно применить что-то вроде следующей процедуры:

1. Ведущий объявляет матрицу выплат;
2. Игроки гласно обсуждают выбор стратегий;
3. Игроки втайне друг от друга извещают ведущего о своих ходах;
4. Ведущий оглашает собранный набор стратегий;
5. Ведущий может с ненулевой вероятностью выбрать любого из игроков и предложить ему переходить;
6. Ведущий вычисляет и объявляет выигрыши.

Этой процедуры вполне достаточно, если мы говорим о классических равновесиях Нэша в чистых и смешанных стратегиях. Во втором случае следует только уточнить, что реализация конкретного исхода, определяемого набором смешанных стратегий, либо не происходит вообще (ведущий объявляет матема-

тические ожидания выигрышей), либо происходит только на последнем этапе. Однако, при добавлении к модели пространств корреляции ситуация несколько усложняется. Поскольку коррелированными стратегиями могут быть любые функции, отображающие получаемые игроками сигналы в смешанные стратегии, кажется естественным представлять себе, как игроки сами вычисляют избранные ими же функции, получив все релевантные сигналы:

1. Ведущий объявляет матрицу выплат;
2. Игроки гласно обсуждают выбор коррелированных стратегий;
3. Ведущий генерирует состояние природы и извещает игроков о соответствующих событиях из их σ-алгебр информированности;
4. Игроки втайне друг от друга вычисляют смешанные стратегии и извещают ведущего о своих ходах;
5. Ведущий оглашает собранный набор смешанных стратегий;
6. Ведущий может с ненулевой вероятностью выбрать любого из игроков и предложить ему переходить;
7. Ведущий вычисляет и объявляет выигрыши.

К сожалению, такой наивный подход обладает существенным недостатком — он работает ожидаемым образом только в симметричных пространствах корреляции, где σ-алгебры информированности всех игроков совпадают. Если же мы говорим о пространствах заговоров, то возникают сразу две проблемы. Во-первых, между этапами 3 и 4 у кого-то из игроков может возникнуть искушение разгласить значение приватного сигнала, если это может сподвигнуть неосведомлённых о нём игроков на выбор более выгодной для разглашающего стратегии. Этот вопрос ещё можно было бы закрыть, добавив в алгоритм запрет на коммуникацию между игроками, начинающийся после этапа 2, но, увы, это только одна из проблем.

Во-вторых, что поправить несколько сложнее, при наличии информационной асимметрии возможность одного из игроков изменить выбранную стратегию на этапе 6 перестаёт соответствовать концепции равновесия по Нэшу. В симметричном случае между первоначальным выбором смешанной стратегии на этапе 4 и возможным отклонением от неё на этапе 6 игрок не получает никакой дополнительной информации, поскольку публичность сигнала и так позволяет вычислить избранные другими игроками смешанные стратегии — оглашая их, ведущий, фактически, только фиксирует результат публичной договорённости, достигнутой на этапе 2. Асимметричные пространства корреляции же содержат события, о кото-

рых на этапе 3 оповещается только часть игроков. При этом каждый игрок может достоверно вычислить свою смешанную стратегию, но не стратегии оппонентов, завязанные на скрытые от него сигналы. В этой ситуации оглашение ведущим собранных смешанных стратегий на этапе 5 увеличивает знание игроков перед принятием кем-то из них решения об отклонении, что противоречит идее равновесия по Нэшу. Для приведения вышеописанной процедуры в соответствие с моделируемым формализмом её необходимо изменить несколько противоречащим интуиции образом:

1. Ведущий объявляет матрицу выплат;
2. Игроки гласно обсуждают выбор коррелированных стратегий;
3. Игроки втайне друг от друга извещают ведущего о выбранных коррелированных стратегиях;
4. Ведущий оглашает собранный набор коррелированных стратегий;
5. Ведущий генерирует состояние природы и вычисляет смешанные стратегии игроков;
6. Ведущий может с ненулевой вероятностью выбрать любого из игроков, известить его обо всех реализовавшихся событиях из его σ-алгебры информированности и предложить ему изменить вычисленную ведущим смешанную стратегию;
7. Ведущий вычисляет и объявляет выигрыши.

Таким образом, в отличие от симметричного случая модель заговоров не позволяет смотреть на коррелированные стратегии как на «чёрные ящики» в головах игроков, просто подсказывающие им синхронную реакцию на раздражители. Здесь наборы коррелированных стратегий приходится интерпретировать как проговариваемые и формально фиксируемые соглашения, поскольку концепция равновесия по Нэшу подразумевает возможность отклонения именно в тот момент, когда общим знанием являются только намерения игроков реагировать тем или иным образом на тайные сигналы, но ещё не конкретные их реакции.

Интересно то, что при попытке обобщить эту процедуру для получения структурно согласованных равновесий в пространствах заговоров мы снова сталкиваемся с похожей проблемой. На первый взгляд достаточно было бы уточнить только этап 6, чтобы ведущий мог предлагать отклониться от выбранных стратегий как отдельным игрокам, так и целым группам заговорщиков. Однако, это срабатывает ожидаемым образом только для наиболее простых семейств с непересекающимися заговорами. В том же случае, когда у двух заговоров могут

быть общие участники, уже групповые отклонения перестают соответствовать формализму — ведь если перед их обсуждением ведущий оповестит каждого заговорщика о рулетках всех заговоров, в которые тот входит, то кто-то из них тогда мог бы разгласить тайну другого заговора, тем самым неправомерно увеличив знания не входящих в него игроков до принятия решения об отклонении. Проще всего поправить это с помощью выноса групповых отклонений в отдельный этап, предшествующий генерации состояния природы:

1. Ведущий объявляет матрицу выплат;
2. Игроки гласно обсуждают выбор коррелированных стратегий;
3. Игроки втайне друг от друга извещают ведущего о выбранных коррелированных стратегиях;
4. Ведущий оглашает собранный набор коррелированных стратегий;
5. Ведущий может с ненулевой вероятностью выбрать любую из групп заговорщиков и предложить им изменить выбранные коррелированные стратегии;
6. Ведущий генерирует состояние природы и вычисляет смешанные стратегии игроков;
7. Ведущий может с ненулевой вероятностью выбрать любого из игроков, известить его обо всех реализовавшихся событиях из его σ-алгебры информированности и предложить ему изменить вычисленную ведущим смешанную стратегию;
8. Ведущий вычисляет и объявляет выигрыши.

Заметим, что этап 5 (обсуждение и утверждение заговорщиками группового отклонения) — сам по себе многостадийный процесс, в котором те, кто хочет увеличить свой выигрыш сменой стратегии, предлагают проект отклонения, а остальные участники заговора имеют индивидуальное право вето, если этот проект приносит им убыток. Таким образом, структурная согласованность равновесия подразумевает, что группы заговорщиков могут отклоняться на стадии планирования, перед получением игроками информации о состоянии природы, а индивидуальные отклонения возможны уже после срабатывания механизмов корреляции, но до оглашения конкретный смешанных стратегий, сыгранных противниками.

## 2.7 Немонотонная отдача в других конфликтах планирования

При помощи игры $\Gamma_n^3$ мы продемонстрировали, во-первых, что планирование заданий с немонотонной функцией оплаты за срочность может быть чувствительно к дополнительной информационной асимметрии, и, во-вторых, что в играх с заговорами, несмотря на присущий им частичный антагонизм интересов, возможны решения, отвечающие принципу коллективной рациональности. Подчеркнём полезность этих результатов, заметив, что проблема планирования заданий гораздо шире рассмотренного нами примера, причём как в смысле возможных значений параметров (матрицы коэффициентов $(t_i^a) \in \mathbb{R}_{\geqslant 0}^{m\times n}$ и функций отдачи $v^a : \mathbb{R}_{\geqslant 0} \to \mathbb{R}, a = \overline{1,m}$), так и в смысле разнообразия практических приложений модели. В контексте этой работы нет смысла заниматься слишком подробным разбором более сложных случаев, но для того, чтобы показать возможную связь модели с реальным миром за пределами вычислительных центров со странными схемами поощрений сотрудников, попробуем построить пару примеров с более солидной предметной областью.

Начнём с экономики, представив себе, как $m$ компаний готовятся выйти на рынок с предложениями высокотехнологичного товара, и перед ними встаёт выбор между $n$ различными открытыми стандартами на один и тот же его важный аспект. К примеру, это могут быть разнообразные промышленные роботы и стандарты их интеграции в «умный» цех. Когда компания $a \in \{1,\dots,m\}$ выходит на рынок стандарта $i \in \{1,\dots,n\}$, она тем самым осуществляет вклад в его развитие, характеризующийся векторной константой $t_i^a \in \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0}$, компоненты которой соответствуют отдельным независимым аспектам (например, функциям, для исполнения которых приобретаются роботы). Если в ситуации $s$ одним стандартом $i$ пользуются несколько компаний, то простым суммированием их вкладов можно посчитать общий индекс развития $t_i(s) = [s^1 = i]t_i^1 + \ldots + [s^m = i]t_i^m$. На ожидаемый доход от инвестиций в каждый из стандартов существенным образом влияют два дисконтирующих фактора: сетевой эффект и насыщение рынка.

Под сетевым эффектом мы понимаем зависимость покупательского энтузиазма от общего индекса развития стандарта — функция $0 \leqslant \alpha^a(t) \leqslant 1$ характеризует долю покупателей, готовых приобретать роботов компании $a$, выполненных по стандарту с общим индексом развития $t$. Более развитый стандарт всегда привлекает больше потребителей, так что функции $\alpha^a(t)$ монотонно неубы-

вающие, т.е. $\alpha^a(t) \leqslant \alpha^a(t+\Delta), \forall t, \Delta \succeq (0,\ldots,0)$. Насыщение рынка, с другой стороны, подразумевает ограниченность спроса — при избытке инвестиций в любой из стандартов, платёжеспособности покупателей перестаёт хватать на всех, цены приходится снижать, а с ними падают и доходы. Соответственно, ещё одна функция $0 \leqslant \beta^a(t) \leqslant 1$ характеризует, какой долей прибыли придётся ограничиться компании $a$ для сохранения конкурентоспособности своих роботов на рынке стандарта с общим индексом развития $t$. Эта функция, по понятным причинам, монотонно невозрастающая, т.е. $\beta^a(t) \geqslant \beta^a(t+\Delta), \forall t, \Delta \succeq (0,\ldots,0)$. Целью компании $a$ при выборе стратегии $s^a$ является максимизация комбинации дисконтирующих факторов $u^a(s) = \alpha^a(t_{s^a}(s))\beta^a(t_{s^a}(s))$.

Можно представить и политическую интерпретацию этой же игры. Пусть в некий коллегиальный выборный орган пытаются избираться $n$ кандидатов (самостоятельно, без партийных списков), а $m$ эффективных менеджеров выбирают, за кого из них развернуть агитацию в подведомственных учреждениях. Когда олигарх $a$ принимает решение о поддержке кандидата $i$, тем самым он вносит вклад в его популярность, характеризующийся векторной константой $t_i^a \in \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0}$, компоненты которой соответствуют электорально значимым демографическим группам. Если в ситуации $s$ кандидата $i$ поддерживают несколько олигархов, то простым суммированием их вкладов можно получить общий индекс популярности кандидата $t_i(s) = [s^1 = i]t_i^1 + \ldots + [s^m = i]t_i^m$. На ожидаемую выгоду от поддержки того или иного кандидата влияют два дисконтирующих фактора: политическое влияние и готовность к сотрудничеству.

Политическое влияние кандидата в вопросах, интересующих поддержавшего его олигарха, очевидно, растёт вместе с общим индексом его популярности, что выражается функцией $0 \leqslant \alpha^a(t) \leqslant \alpha^a(t+\Delta) \leqslant 1, \forall t, \Delta \succeq (0,\ldots,0)$. Готовность же кандидата к сотрудничеству с каждым из своих сторонников, наоборот, падает с ростом его суммарной популярности, что выражается функцией $1 \geqslant \beta^a(t) \geqslant \beta^a(t+\Delta) \geqslant 0, \forall t, \Delta \succeq (0,\ldots,0)$. Целью олигарха $a$ при выборе стратегии $s^a$ является максимизация комбинации дисконтирующих факторов $u^a(s) = \alpha^a(t_{s^a}(s))\beta^a(t_{s^a}(s))$.

Сведём описание обоих конфликтов к матричной игре в нормальной форме:

$$\Gamma = \langle A, S^a, u^a(s), a \in A\rangle;$$

$$A = \{1,\ldots,m\}, S^1 = \ldots = S^m = \{1,\ldots,n\};$$

$$u^a(s) = \alpha^a(t_{s^a}(s))\beta^a(t_{s^a}(s)), a = \overline{1,m};$$

$$\alpha^a, \beta^a : \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0} \to [0,1];$$

$$0 \leqslant \alpha^a(t) \leqslant \alpha^a(t+\Delta) \leqslant 1, \forall t, \Delta \succeq (0,\ldots,0);$$

$$1 \geqslant \beta^a(t) \geqslant \beta^a(t+\Delta) \geqslant 0, \forall t, \Delta \succeq (0,\ldots,0);$$

$$t_i(s) = [s^1 = i]t_i^1 + \ldots + [s^m = i]t_i^m, i = \overline{1,n}.$$

Несложно заметить сходство этой игры с проблемой планирования заданий, что мы здесь постарались подчеркнуть использованием тех же символов для переменных и констант. Фактически, единственным значимым отличием оказывается то, что в планировании заданий время $t$ было скаляром, а не вектором. Функциям оплаты за срочность в новых формулировках соответствуют $v^a(t) = \alpha^a(t)\beta^a(t)$, форма которых и определяет наши ожидания от исхода конфликта. Ранее мы уже говорили, что анализ проблемы планирования заданий в общем виде, для произвольных $(t_i^a)$ и $(v^a)$ представляет собой чрезвычайно сложную задачу, и, конечно же, переход от скаляров к векторам в домене функций отдачи дело нисколько не упрощает. Лучшее, что тут можно сделать — дать качественный прогноз для некоторых неформально описанных подклассов конфликта с опорой на здравый смысл, интуицию и аналогию с разобранным выше частным случаем $\Gamma_n^3$.

Во избежание переусложнения ограничимся случаем квазивогнутых функций отдачи $v^a(t) = \alpha^a(t)\beta^a(t)$, естественным образом обобщив это понятие на многомерные области определения. Для начала обозначим символом $T^a_{\nearrow}$ множество всех таких $t$, что $t_* \prec t \Rightarrow v^a(t_*) \leqslant v^a(t) \wedge t_* \in T^a_{\nearrow}$. Аналогично, символом $T^a_{\searrow}$ обозначим множество всех таких $t$, что $t_* \succ t \Rightarrow v^a(t_*) \leqslant v^a(t) \wedge t_* \in T^a_{\searrow}$. Это будут области непрерывного неубывания и невозрастания $v^a(t)$ соответственно. Если эти два множества покрывают всю область определения, т.е. $T^a_{\nearrow} \cup T^a_{\searrow} = \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0}$, то функция $v^a(t)$ квазивогнута. Для подобных функций также можно обозначить «гребень» $T^a_{\sim} = T^a_{\nearrow} \cap T^a_{\searrow}$, в одномерном случае соответствующий максимуму.

Попробуем представить логику конфликта для простейшего случая с двухэлементным семейством заговоров $\mathfrak{A} = \{A_p, A_q\}, A_p \cap A_q = \varnothing, A_p \cup A_q = A$. Сократим запись с помощью следующих обозначений:

$$t_i^{A_*} = \sum_{a \in A_*} t_i^a, \forall A_* \subseteq A;$$

$$\check{u}^a = \min_{1 \leqslant i \leqslant n} v^a(t_i^A), \hat{u}^a = \max_{1 \leqslant i \leqslant n} v^a(t_i^A), \forall a \in A.$$

Здесь $t_i^{A_*}$ соответствует суммарному индексу развития стандарта (популярности кандидата) $i$ при его выборе группой игроков $A_* \subseteq A$. Так же, для каждого игрока $a$ базовым платёжным интервалом называется промежуток от $\check{u}^a$ до $\hat{u}^a$, т.е. от наименьшего до наибольшего возможных выигрышей при единогласном выборе общей стратегии всеми участниками конфликта. Рассмотрим игры, ограниченные следующими условиями:

- $\forall a \in A, i = \overline{1,n}, v^a(t_i^{A_p \cup \{a\}}) < \check{u}^a$, т.е. ни один игрок не может достигнуть нижней границы своего базового платёжного интервала, если ту же стратегию выбирает только группа $A_p$;
- $\forall a \in A, i = \overline{1,n}, v^a(t_i^{A_q \cup \{a\}}) > \check{u}^a$, т.е. каждый игрок преодолевает нижнюю границу своего базового платёжного интервала при выборе любой стратегии совместно с группой $A_q$;
- $\forall a \in A_q, i = \overline{1,n}, t_i^{A_q} \in T^a_{\searrow}$, т.е. для всех членов группы $A_q$ выбор общей стратегии выводит суммарный индекс в область невозрастания функции отдачи.

Таким образом мы очертили круг ситуаций, в которых участники конфликта поделены на две непересекающиеся группы заговорщиков. Если рассматривать происходящее с точки зрения каждого заговора в предположении, что аутсайдеры вообще не участвует в игре, несложно заметить, что любой стратегический набор, в котором заговорщики выбирают одну стратегию на всех, будет хорошим кандидатом в равновесия по Нэшу. Это не означает, что других равновесий не может быть, но мы в целях наглядности сознательно ограничимся анализом наборов, характеризующихся двумя независимыми распределениями вероятностей $p = (p_1, \ldots, p_n)$ и $q = (q_1, \ldots, q_n)$, где участники заговоров $A_p$ и $A_q$ синхронно внутри групп но независимо между группами выбирают стратегии $i = \overline{1,n}$ с вероятностями $p_i$ и $q_i$ соответственно, используя соответствующий приватный механизм корреляции. Выплаты при этом считаются по формуле

$$u^a(p,q) = \sum_{i=1}^{n} p_i((1-q_i)v^a(t_i^{A_p}) + q_i v^a(t_i^A)), \forall a \in A_p,$$

$$u^a(p,q) = \sum_{i=1}^{n} q_i((1-p_i)v^a(t_i^{A_q}) + p_i v^a(t_i^A)), \forall a \in A_q,$$

В соответствии с условиями, заговор $A_p$ недостаточно велик для максимизации прибылей своих участников, так что каждый из них предпочёл бы присоединиться к стратегии, избранной заговором $A_q$. Однако, поскольку тайна

чужого заговора игрокам не доступна, от стратегии предписанной механизмом корреляции они могут отклониться только в пользу другой чистой стратегии. Таким образом, для получения прибыли в результате индивидуального отклонения от пары распределений $(p, q)$, заговорщику $a \in A_p$ необходимо и достаточно найти такие индексы $i \neq j \in \{1, \ldots, n\}$, что при $p_i > 0$ выполняется неравенство

$$(1 - q_i)v^a(t_i^{A_p}) + q_i v^a(t_i^A) < (1 - q_j)v^a(t_j^a) + q_j v^a(t_j^{A_q \cup \{a\}}).$$

Несложно заметить, что с ростом любого $q_j$ постепенно увеличивается и кол-во индексов $i$, для которых выполняется это неравенство, а при приближении $q_j$ к 1 оно рано или поздно начинает выполняться для всех $i \neq j$. Зафиксировав произвольное распределение $q$, можно для каждого заговорщика $a \in A_p$ вычислить множество $S_q^a \subseteq \{1, \ldots, n\}$, состоящее из стратегий, допускающих подобные продуктивные отклонения. При этом, поскольку участники заговора $A_q$, отклонившись от предписанной стратегии, неизбежно терпят убытки, для них проверять ничего не нужно. В результате, произвольная пара распределений $(p, q)$ описывает равновесие по Нэшу тогда и только тогда, когда

$$\forall i \in \bigcup_{a \in A_p} S_q^a, p_i = 0.$$

Таким образом, если мы говорим о равновесиях только в классическом Нэшевском смысле без учёта коллективной рациональности, то в описанном противостоянии участникам большого заговора вообще не приходится думать о возможном предательстве со стороны соратников, тогда как малый заговор должен внимательно выбирать общую стратегию так, чтобы у его участников не было искушения попытаться угадать стратегию, избранную большим. Стремление же удостовериться в структурной согласованности обозначенных решений дают чуть более интересную картину.

Сразу оговоримся, что в установленных ограничениях сложно точно убедиться в структурной согласованности даже для узкого множества рассматриваемых $(p, q)$-наборов, поскольку вполне возможны, например, коллективные отклонения, разделяющие заговор $A_q$ на две группы, выбирающие разные стратегии. Одна при этом получает прибыль в результате избавления от лишних участников (см. ограничение $t_i^{A_q} \in T_{\searrow}^a$, т.е. принадлежность точек единогласного выбора к области невозрастания функции отдачи). Вторая же потенциально увеличивает доход, присоединившись к стратегии, избранной заговором $A_p$, если

существует достаточно большое $p_i$. Можно, конечно, попытаться наложить на параметры конфликта дополнительные ограничения, предупреждающие подобные и даже более экзотические отклонения, однако это сильно усложнит постановку, не слишком добавляя иллюстративности.

Вместо этого мы ограничимся поиском только тех $(p, q)$-наборов, от которых не существует успешных коллективных отклонений в пользу других $(p, q)$-наборов. Найденные точки равновесия всё ещё можно будет подозревать в отсутствии структурной согласованности, однако мы хотя бы исключим большой класс заведомо несогласованных. Итак, для прибыльности коллективного отклонения малого заговора достаточно найти такие индексы $i \neq j \in \{1, \dots, n\}$, что при $p_i > 0$ для каждого $a \in A_p$ выполняется неравенство

$$(1 - q_i)v^a(t_i^{A_p}) + q_i v^a(t_i^A) < (1 - q_j)v^a(t_j^{A_p}) + q_j v^a(t_j^A).$$

Аналогично, для большого заговора отклонение успешно, если есть такие индексы $i \neq j \in \{1, \dots, n\}$, что при $q_i > 0$ для каждого $a \in A_q$ выполняется неравенство

$$(1 - p_i)v^a(t_i^{A_q}) + p_i v^a(t_i^A) < (1 - p_j)v^a(t_j^{A_q}) + p_j v^a(t_j^A).$$

Рассматривая эти неравенства в свете ограничений, наложенных нами на параметры конфликта, несложно заметить, что коллективная рациональность стимулирует обе группы игроков к минимизации наибольших вероятностей выбора отдельных стратегий, однако по противоположным причинам. Участникам малого заговора выгодно как по отдельности, так и сообща присоединяться к стратегии, выбранной большим заговором, выплаты членам которого такое совпадение стратегий заведомо уменьшает. Переводя на язык условленных ранее интерпретаций, члены слабого картеля с удовольствием воспользовались бы развитостью стандарта (или влиятельностью кандидата) избираемого крупным картелем, однако крупному картелю, напротив, совершенно не улыбается делить ограниченный спрос на и без того насыщенном рынке (или соревноваться за внимание и без того уверенного в избрании политика) с лишними конкурентами.

На уровне коллективно рациональных решений игра, таким образом, превращается в разновидность двухсторонних пряток, где одна группа ищет встречи с другой, пытающейся этого столкновения избежать, а заговоры служат для получения преимущества от объединения усилий при минимизации вероятности присоединения к дележу прибылей нежелательных попутчиков. По сути, формализм структурно согласованного равновесия в играх с заговорами является не

какой-то сложной экономической концепцией, а всего лишь воплощением интуитивного принципа, применявшегося, вероятно, ещё в дописьменную эпоху. Вполне возможно, что накой-нибудь охотник, заметив раненного мамонта при обходе племенных угодий, прикинул: «В одиночку я его, пожалуй, не завалю, но и племя всё звать смысла нет. Шепну-ка я лучше на ушко паре друзей — это ж сколько почёта и славы будет, втроём столько мяса добыть.» С похожего рассуждения и могла начаться мировая история заговоров.

# Глава 3. Вычислительная сложность стратегий в повторяющихся играх с дисконтированием

## 3.1 «Народная» теорема в пространствах заговоров

Для того, чтобы понять, как многократное повторение влияет на конфликты, чувствительные к дополнительной информационной асимметрии, необходимо сперва проанализировать то, как «народная» теорема может быть обобщена на игры в пространствах заговоров. Ранее эту теорему уже доказывали в различных формах для коррелированного расширения игр [3], сознательно ограничиваясь случаем публичных механизмов корреляции. Нам же необходимо сделать ещё один шаг, отказавшись от этого ограничения. По сути, главным изменением оказывается то, что использование приватных механизмов корреляции зачастую позволяет дополнительно уменьшить резервные выигрыши игроков, не имеющих к ним доступа. Напомним, что резервным выигрышем игрока $a$ называется

$$u_*^a = \min_{s \in \overline{S}_a} u^a(s), \overline{S}_a = \{\overline{s} \in S \mid \overline{s}^a \in \arg\max_{s^a \in S^a} u^a(\overline{s}|s^a)\},$$

то есть наименьший его выигрыш среди всевозможных исходов, в которых он использует стратегию наилучшего ответа. По сути, резервный выигрыш обозначает границу полезности, ниже которой для соответствующего игрока невозможно опустить ожидаемый выигрыш, даже если все остальные игроки объединятся для достижения этой цели, невзирая на ущерб себе. Набор стратегий, приводящий к такому исходу, называется минимаксным для игрока $a$. Вектор $u_* = (u_*^1, \ldots, u_*^m)$, составленный из резервных выигрышей каждого игрока, называется точкой минимакса игры. Аналогичным образом можно определить резервный равновесный выигрыш игрока $a$:

$$\tilde{u}_*^a = \min_{s \in \tilde{S}} u^a(s), \text{где } \tilde{S} \text{ — множество равновесных по Нэшу наборов},$$

из которых составляется вектор $\tilde{u}_* = (\tilde{u}_*^1, \ldots, \tilde{u}_*^m)$, называемый точкой равновесного минимакса игры. Очевидно при этом, что $\tilde{u}_* \succeq u_*$.

Центральной идеей, стоящей за доказательством большинства «народных» теорем, является использование минимаксных наборов стратегий для наказания игроков, отклоняющихся от запланированной цепочки действий, ожидаемых от

них соперниками. Любая последовательность розыгрышей $(s_i)$ с выплатами, сходящимися (в смысле среднего или с дисконтированием, в зависимости от версии теоремы) к вектору $u_0 = (u_0^1, \ldots, u_0^m)$, строго доминирующему точку минимакса игры (т.е. $u_0^a > u_*^a, a = \overline{1,m}$), может быть равновесным исходом (в смысле обычного Нэша или совершенного по подыграм, в зависимости от версии теоремы) повторяющейся игры. Если на итерации $i$ игрок $a$ отклоняется от ожидаемой стратегии $s_i^a$, то начиная со следующей итерации остальные игроки переходят к применению стратегии из минимаксного для этого игрока набора, продолжая делать это достаточно долго (в некоторых версиях доказательств бесконечно) для того, чтобы нанесённый ими игроку $a$ ущерб превзошёл его прибыль от отклонения.

Коррелированные стратегии в контексте повторяющихся игр понимаются обычно в ограниченном смысле — рассматриваются только публичные сигналы, что с точки зрения нашей модели соответствует пространствам заговоров структуры $\{A\}$, то есть состоящим из одного заговора, охватывающего всех игроков. Множество платёжных векторов, достижимых в игре $\Gamma|\{A\}$, представляет собой выпуклую оболочку множества векторов, входящих в матрицу выплат игры $\Gamma$. Множество коррелированных равновесий по Нэшу игры $\Gamma|\{A\}$ представляет собой выпуклую оболочку множества смешанных равновесий игры $\Gamma$. При этом, как было показано в предыдущих главах, добавление к пространству заговоров групп, в которые входят не все игроки, может пополнять множество коррелированных равновесий по Нэшу точками, лежащими за пределами выпуклой оболочки множества смешанных равновесий. Кроме того, благодаря использованию тайных сигналов могут быть снижены резервные выигрыши игроков, не имеющих возможности их наблюдать.

Для доказательств большинства версий «народной» теоремы переход к более сложным пространствам заговоров, вероятно, не представляет большой проблемы — логика рассуждений остаётся прежней, достаточно при необходимости учитывать новые значения минимаксов и коррелированные равновесия за пределами выпуклой оболочки множества смешанных. К счастью, в контексте данной работы у нас даже нет необходимости в современных её формулировках — вполне достаточно классического, относительно слабого утверждения:

**Теорема 3.1.1.** *Пусть* $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ *— игра в нормальной форме с конечным множеством исходов,* $V$ *— выпуклая оболочка множества платёжных*

*векторов её матрицы, а* $\mathfrak{A} \subseteq 2^A$ *— произвольное пространство заговоров. Если вектор выплат* $v \in V$ *строго доминирует точку минимакса игры* $\Gamma|\mathfrak{A}$*, то найдётся такой коэффициент дисконтирования* $0 < \delta < 1$*, что в бесконечно повторяющейся игре* $\Gamma|\mathfrak{A}$ *будет существовать равновесие Нэша с выплатами, сходящимися к* $v$*. Если же вектор* $v$ *доминирует ещё и точку равновесного минимакса той же игры, то в бесконечно повторяющейся игре с достаточно большим коэффициентом дисконтирования будет существовать совершенное подыгровое равновесие с выплатами, сходящимися к* $v$*.*

*Доказательство.* Если $A \in \mathfrak{A}$, то последовательность наборов с выплатами, сходящимися к $v$, строится из коррелированных стратегий, опирающихся на публичный сигнал и напрямую смешивающих наборы чистых стратегий в пропорциях, обеспечивающих необходимый вектор платежей. Если же $A \notin \mathfrak{A}$, то можно использовать последовательность наборов чистых стратегий, сходящуюся в пределе к той же точке. При отклонении любого игрока от предписанной стратегий остальные переключаются на его наказание соответствующими минимаксными наборами стратегий. Прибыль игрока $a$, отклоняющегося на $i$-й итерации в пользу стратегии $\hat{s}_i^a$, конечна и составляет $u^a(s_i|\hat{s}_i^a) - u^a(s_i)$, так что при достаточно большом $\delta$ ущерб от вечной кары минимаксом на все последующие итерации будет очевидно больше. Наказание, использующее обычный минимакс, может включать стратегии неоптимальные с точки зрения карающих игроков, так что получающиеся при этом точки равновесия в общем случае не являются совершенными по подыграм. Наказание с использованием равновесного минимакса лишено этого недостатка, а значит равновесия на его основе уже будут совершенными по подыграм. □

Для наших целей этого хватает, поскольку рассматривать мы будем повторение игры, у которой точки обычного и равновесного минимакса совпадают во всех пространствах заговоров. Тем не менее, если возникнет такая необходимость, ничего не мешает подобному обобщению и более современных, усиленных формулировок [18]. Чтобы не перегружать работу более громоздкими рассуждениями, которые по факту были бы почти дословным цитированием доказательств за авторством Васина А.А., ограничимся кратким пересказом их центральной идеи. Сделать участие в наказании обычным минимаксом первого отклонившегося от предписанной стратегии игрока оптимальной стратегией для наказывающих можно при помощи чуть более сложного формата угрозы.

Игрокам достаточно договориться о том, что наказание первого отклонившегося будет не вечным, а прерывающимся в тот момент, когда кто-либо отказывается принимать в нём участие. Как только один из наказывающих отклоняется от предписываемой минимаксным набором стратегии, предыдущий отклонившийся прощается и все переходят к такому же условно вечному наказанию последнего «уклониста», в котором участвуют все, включая только что прощённого игрока. Таким образом процесс превращается в что-то наподобие «салочек», создавая эффективную угрозу оказаться последним наказанным, что расширяет множество совершенных по подыграм равновесий до всех точек, доминирующих обычный минимакс. Добавление пространства заговоров здесь, опять же, не создаёт особых проблем — рассуждение продолжает работать даже при использовании в наказаниях синхронизации тайными сигналами.

## 3.2 Повторяющийся трёхсторонний чёт-нечет

Продемонстрировать применение обобщения «народной» теоремы на игры с заговорами можно на примере всё того же трёхстороннего чёт-нечета (см. таблицу 1). Здесь $V$ представляет собой треугольник с вершинами $(6, 6, 0)$, $(6, 0, 6)$ и $(0, 6, 6)$. У игры две точки равновесия по Нэшу в чистых стратегиях (синхронный выбор орла или решки всеми игроками) и одна дополнительная в смешанных (равновероятный независимый выбор между орлом и решкой всеми игроками), влекущие один и тот же вектор платежей $(4, 4, 4)$, являющийся, к тому же, ещё и точкой минимакса игры. Действительно, пусть первый игрок избрал стратегию $(p, 1 - p)$, а второй — $(q, 1 - q)$. Тогда выигрыши третьего при выборе чистых стратегий составляют:

$$u^3(p, q, 1) = 6(p + q) - 8pq;$$
$$u^3(p, q, 0) = 2(p + q) - 8pq + 4.$$

Несложно заметить, что

$$\begin{aligned}
p \geqslant q \geqslant \frac{1}{2} &\Rightarrow u^3(p,q,1) \geqslant 4;\\
p \geqslant 1-q \geqslant \frac{1}{2} &\Rightarrow u^3(p,q,1) \geqslant 4;\\
q \geqslant p \geqslant \frac{1}{2} &\Rightarrow u^3(p,q,1) \geqslant 4;\\
q \geqslant 1-p \geqslant \frac{1}{2} &\Rightarrow u^3(p,q,1) \geqslant 4;\\
p \leqslant q \leqslant \frac{1}{2} &\Rightarrow u^3(p,q,0) \geqslant 4;\\
p \leqslant 1-q \leqslant \frac{1}{2} &\Rightarrow u^3(p,q,0) \geqslant 4;\\
q \leqslant p \leqslant \frac{1}{2} &\Rightarrow u^3(p,q,0) \geqslant 4;\\
q \leqslant 1-p \leqslant \frac{1}{2} &\Rightarrow u^3(p,q,0) \geqslant 4.
\end{aligned}$$

Эти варианты исчерпывают всё пространство возможных ситуаций, так что никакое сочетание смешанных стратегий двух игроков не может быть эффективным наказанием для третьего. Таким образом в отсутствие приватных механизмов корреляции народная теорема никак не расширяет множество решений повторяющегося чёт-нечета. Однако, добавление в пространство заговоров, например, пары $\{1,2\}$ меняет картину — в игре появляются коррелированные равновесия с выплатами $(5,5,2)$ в ситуации, когда все игроки снова делают равновероятный выбор между орлом и решкой, но при этом благодаря секретному механизму корреляции выбор игроков 1 и 2 всегда синхронен. Это уменьшает резервные (в обычном и равновесном смыслах) выигрыши игрока 3, давая нам новую точку минимакса — $(4,4,2)$. В соответствии с сформулированной выше версией «народной» теоремы, в пространстве заговоров $\{\{1,2\}\}$ у повторяющегося трёхстороннего чёт-нечета появляются новые совершенные по подыграм равновесия в треугольнике с вершинами $(6,4,2)$, $(4,6,2)$ и $(4,4,4)$.

Аналогичным образом, в пространстве заговоров $\{\{1,2\},\{2,3\}\}$ точка минимакса игры перемещается в $(2,4,2)$, что расширяет множество решений до плоской трапеции с вершинами $(4,6,2)$, $(2,6,4)$, $(2,4,6)$ и $(6,4,2)$. Наконец, пространство $\{\{1,2\},\{2,3\},\{1,3\}\}$, включающее все парные заговоры, даёт точку минимакса $(2,2,2)$, превращая множество выплат, достижимых в совершенных подыгровых равновесиях, в плоский шестиугольник с вершинами $(6,4,2)$,

$(6,2,4)$, $(4,2,6)$, $(2,4,6)$, $(2,6,4)$ и $(4,6,2)$. Эта иллюстрация неплохо согласуется с интуитивным представлением о том, что группы агентов, имеющие возможность координировать свои действия втайне от остальных, могут использовать это как угрозу в адрес аутсайдеров, принуждая тех соглашаться на исходы конфликтов, которые в отсутствие тайных сговоров были бы отвергнуты как невыгодные. Однако, этим влияние чувствительности к дополнительной информационной асимметрии на повторяющиеся игры не исчерпывается. Далее будет показано, что даже при отсутствии априорной информационной асимметрии (т.е. внешних по отношению к конфликту событий, о которых его участники осведомлены по-разному) игроки, ограниченные в сложности производимых ими для выбора стратегий вычислений, могут использовать угрозу искусственного создания информационной асимметрии при помощи специальным образом организованных совместных публичных действий.

## 3.3 Модель повторяющихся игр с учётом стоимости вычислений

Построение искомой модели подразумевает конкретизацию способа, при помощи которого рациональные агенты вычисляют стратегию поведения. Для этой цели подойдёт любой формализм, позволяющий алгоритмически полные вычисления с вероятностным ветвлением. Кроме того, необходимы возможность сохранения произвольного внутреннего состояния в памяти для использования на последующих итерациях и, очевидно, метод численной оценки сложности произведённого на каждой итерации вычисления.

Диаграмма на рисунке 3.1 изображает общую схему взаимодействия агентов и среды для двух игроков (естественным образом обобщающуюся на любое конечное их число). В узлах, помеченных буквой $\Gamma$, происходят последовательные розыгрыши произвольной игры $\Gamma = \langle A, S^a, u^a(s), a \in A \rangle$. В $i$-м розыгрыше игрок $a$ выбирает свою стратегию $s_i^a$, применяя вероятностный алгоритм $M^a$, находящийся в состоянии $\psi_i^a$, к результату предыдущего розыгрыша $s_{i-1}$ (если таковой был) и запоминая необходимые для будущих итераций результаты вычислений в новом состоянии $\psi_{i+1}^a$. Узлы $\Sigma^a$ изображают последовательное суммирование разностей выигрыша $u^a(s_i)$ и затрат на произведённое вычисление $\mathfrak{w}_i^a$, с учётом экспоненциально уменьшающегося коэффициента дисконтирования $\delta^i$.

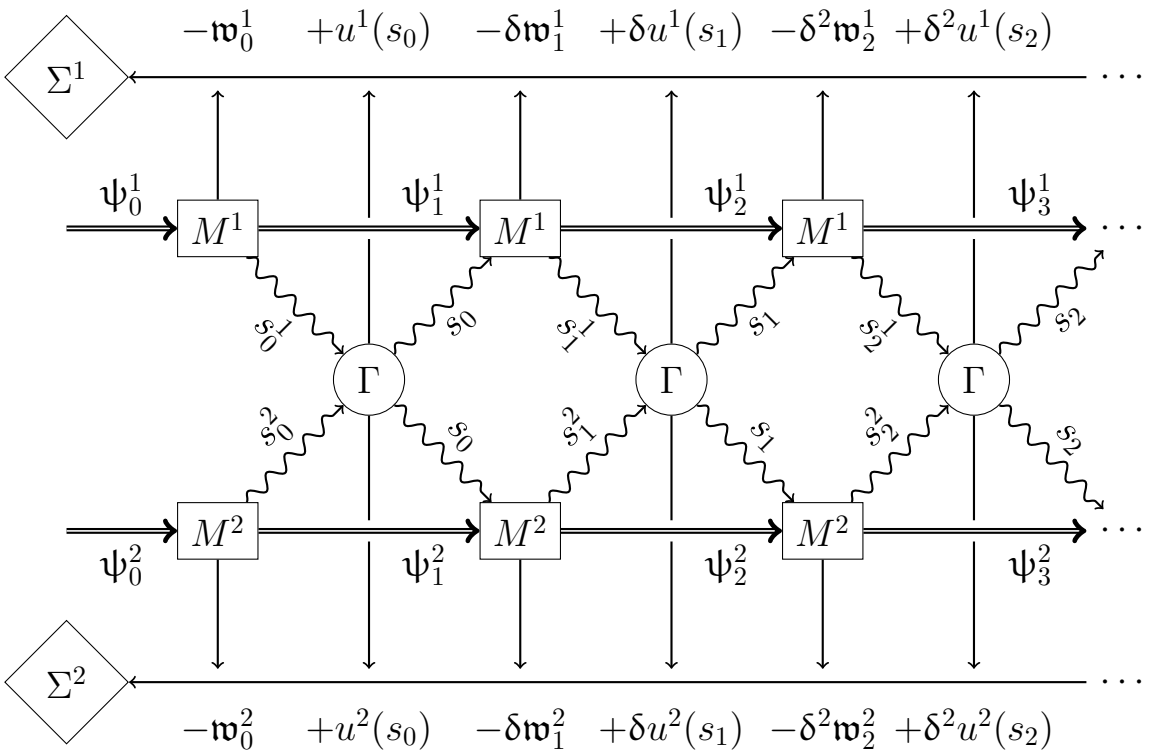


Рисунок 3.1 — Повторяющаяся игра с учётом стоимости вычислений

Поскольку мы говорим о конфликтах рациональных агентов, имеет смысл рассматривать только универсальные алгоритмы $M^a$, позволяющие закодировать любой набор вычислимых стратегий повторяющейся игры в начальных состояниях памяти $\psi_0^a$. Нотация $M^a[g]$ будет обозначать среднюю стоимость вычисления произвольной функции $g$ при её оптимальной реализации посредством $M^a$. Кроме того, если обозначить символом $\mathfrak{s}$ набор стратегий повторяющейся игры с дисконтированием, то нотация $M^a[\mathfrak{s}]$ подходит для обозначения стоимости полного объёма вычислений, необходимых игроку $a$ для выбора каждого хода с учётом того же коэффициента $\delta$. Таким образом, в повторяющейся игре с учётом стоимости вычислений каждый игрок $a$ оптимизирует не просто $u^a(\mathfrak{s})$, но

$$\hat{u}^a(\mathfrak{s}) = u^a(\mathfrak{s}) - M^a[\mathfrak{s}].$$

## 3.4 Криптографическое согласование стратегий

Хотя, как было показано ранее, в отсутствие дополнительной информационной асимметрии трёхсторонний чёт-нечет не даёт возможности двум игрокам

наказывать третьего, используя только лишь смешанные стратегии, даже в том случае, когда игроки не могут использовать тайные механизмы корреляции, учёт стоимости вычислений позволяет в повторяющихся играх применять стратегии наказания, опирающиеся на достижения современной криптографии. Для демонстрации этого нам понадобятся два распространённых криптографических примитива.

Во-первых, необходим *протокол совместной выработки ключа* [19]. В криптографии этим термином называют механизм, при помощи которого Алиса и Боб могут создать общую секретную последовательность битов, априорно обладая лишь публичным знанием об устройстве и параметрах самого механизма, и обмениваясь сообщениями через незащищённый от прослушивания канал связи. При этом Кэрол, обладая тем же априорным знанием и имея возможность читать их сообщения, не может вычислить искомую секретную последовательность битов, поскольку это требует решения алгоритмически трудной задачи (такой, для которой необходимо количество операций, зависящее от длинны ключа экспоненциально). В качестве такого механизма может выступать, например, семейство протоколов Диффи-Хеллмана (далее DH) на основе задач факторизации целых чисел или дискретного логарифмирования (в конечной мультипликативной группе или на эллиптической кривой). Опишем общую схему произвольного протокола DH, не вдаваясь в технические детали.

Пусть имеется семейство биекций $f_n : \mathbb{N}_{<2^n} \leftrightarrow \mathbb{N}_{<2^n}, n \in \mathbb{N}$, обладающих свойством односторонности, т.е. для любого универсального вычислителя $M^*$ одновременно выполняется $M^*[f_n] \in o(2^n)$ (стоимость вычисления самой функции растёт с ростом $n$ полиномиально) и $M^*[f_n^{-1}] \in \Theta(2^n)$ (стоимость вычисления обратной функции растёт с ростом $n$ экспоненциально). Кроме этого, пусть имеется семейство двухместных функций $h_n : \mathbb{N}_{<2^n} \times \mathbb{N}_{<2^n} \to \mathbb{N}_{<2^n}$ таких, что

- $\forall x, y \in \mathbb{N}_{<2^n}, h_n(f_n(x), y) = h_n(x, f_n(y))$;
- $\forall x, y, z \in \mathbb{N}_{<2^n}, h_n(h_n(x, y), z) = h_n(x, h_n(y, z))$;
- $h_n(x_1, y_1) = h_n(x_2, y_2) \Rightarrow x_1 = x_2 \cap y_1 = y_2 \cup x_1 \neq x_2 \cap y_1 \neq y_2$.;
- $M^*[h_n] \in o(2^n)$.

Алиса выбирает случайное натуральное число $0 \leqslant x < 2^n$, выполняющее роль её закрытого ключа, и вычисляет $X = f_n(x)$, выполняющее роль её открытого ключа. На другом конце Боб аналогичным образом генерирует пару ключей $y$ и $Y = f_n(y)$. Алиса и Боб обмениваются открытыми ключами через прослушиваемый Кэрол канал связи. Теперь Алиса, зная свой закрытый ключ

$x$ и открытый ключ Боба $Y$, может вычислить $h_n(x, Y)$, а Боб, соответственно, $h_n(X, y)$. В силу свойств функции $h_n$, вычисленные ими значения можно считать искомым общим секретным ключом $K = h_n(x, Y) = h_n(X, y)$. При этом для Кэрол, знающей только открытые ключи $X$ и $Y$, вычисление общего секретного ключа требует вычисления либо $f_n^{-1}(X)$, либо $f_n^{-1}(Y)$. Благодаря разнице между асимптотической сложностью прямой и обратной функции всегда можно подобрать такое $n$, что стоимости вычисления $f_n$ и $h_n$ оказываются приемлемы, тогда как вычисление $f_n^{-1}$ — непозволительно дорогой процесс. Также заметим, что вследствие ассоциативности функции $h_n$ можно считать многоместными, и члены группы агентов любого размера могут комбинировать с их помощью общие секретные ключи, если каждый опубликовал свой открытый ключ — например, $K = h_n(x, Y, Z) = h_n(X, y, Z) = h_n(X, Y, z)$ для трёх сторон.

Вторым криптографическим примитивом, необходимым для стратегии наказания, является *криптографически стойкий генератор псевдослучайных чисел* [20], далее называемый CSPRNG. Его можно представить в виде семейства функций $G_n : \mathbb{N}_{<2^n} \times \mathbb{N} \to \{0, 1\}$, первый аргумент которых называется зерном (или seed), а второй — позицией. Программа, вычисляющая для заданного $K \in \mathbb{N}_{<2^n}$ последовательные значения $G_n(K, i), i = 1, 2, \ldots$, должна совершать каждый шаг за полиномиальное от $n$ число операций. При этом генератор обязан проходить тест на следующий бит, т.е. не должно существовать полиномиально сложного от $n$ алгоритма, способного без знания $K$ по первым $i$ битам генерируемой последовательности угадать $G_n(K, i + 1)$ с вероятностью, отличной от $\frac{1}{2}$.

Теперь, используя вышеописанные примитивы, можно сконструировать три новых типа стратегий для повторяющегося трёхстороннего чёт-нечета. Представим, что игроки сидят за круглым столом так, что игрок 1 сидит справа от игрока 2, игрок 2 — справа от игрока 3, а игрок 3 — справа от игрока 1. Назовём первую из новых стратегией $\mathfrak{s}_n^L$ «рукопожатие влево»:

1. Выбрать случайное число $x \in \mathbb{N}_{<2^n}$.
2. Вычислить $X = f_n(x)$ и представить в виде битовой последовательности $(X_i) \in \{0, 1\}^n$.
3. Для каждого $i = 1 \ldots n$ совершить один ход игры, выбирая решку при $X_i = 1$ и орла в противном случае. Выбранную сидящим слева игроком стратегию (с тем же сопоставлением) запомнить в качестве очередного элемента битовой последовательности $(Y_i) \in \{0, 1\}^n$, соответствующей числу $Y \in \mathbb{N}_{<2^n}$.

4. Вычислить $K = h_n(x, Y)$.
5. Все последующие ходы совершать, выбирая стратегию в соответствии с последовательно генерируемыми CSPRNG значениями $G_n(K, i), i = 1, 2, \ldots$.

Стратегию $\mathfrak{s}_n^R$ «рукопожатие вправо» строим аналогичным образом, заменяя «слева» на «справа» и меняя местами $x$ с $y$, $X$ с $Y$ и $h_n(x, Y)$ с $h_n(X, y)$. Такие парные стратегии с равной длиной ключа позволяют любым двум игрокам превратить первые $n$ ходов игры в своеобразный «танец синхронизации», вырабатывая общее секретное зерно для генератора псевдослучайных битов, чей вывод на последующих ходах используется в качестве механизма корреляции. Третьему игроку, при этом, для присоединения к согласованному выбору приходится применять стратегию $\mathfrak{s}_n^*$ «взлом»:

1. Первые $n$ ходов играть смешанную стратегию равновероятного выбора и запоминать ходы оппонентов для получения их открытых ключей $X$ и $Y$.
2. Вычислить $K = h_n(f_n^{-1}(X), Y)$ или $K = h_n(X, f_n^{-1}(Y))$.
3. Все последующие ходы совершать, выбирая стратегию в соответствии с последовательно генерируемыми CSPRNG значениями $G_n(K, i), i = 1, 2, \ldots$.

Обозначим также стратегию $\mathfrak{s}^\varnothing$ «пас», при использовании которой игрок на каждой итерации просто выбирает между орлом и решкой случайно и равновероятно. Несложно заметить, что если мы ограничимся рассмотрением только четырёх вышеперечисленных классов стратегий, то почти все комбинации любых из них по выплатам неотличимы от классической точки равновесия в смешанных стратегиях $u(\mathfrak{s}^\varnothing, \mathfrak{s}^\varnothing, \mathfrak{s}^\varnothing) = (4, 4, 4)$. Единственным исключением оказываются ситуации, в которой любые два игрока применяют друг на друга соответствующие «рукопожатия» с одним и тем же $n$, а третий игрок не применяет «взлома» с той же длиной ключа — например, $u(\mathfrak{s}_n^L, \mathfrak{s}_n^R, \mathfrak{s}^\varnothing) = (4 + \delta^n, 4 + \delta^n, 4 - 2\delta^n)$. Здесь первые два игрока первые $n$ ходов тратят на обмен ключами, что с точки зрения выплат неотличимо от случайного выбора, а после этого пользуются общим CSPRNG в качестве механизма корреляции, забирая у третьего половину его выигрыша. Если бы третий не мог ответить им стратегией «взлома», то, применяя народную теорему, наборы с двумя «рукопожатиями» можно было бы использовать для его равновесного наказания. Поскольку взаимное рукопожатие возможно в любой паре игроков, запрет взломов обеспечил бы этой игре точку равновесно-

го минимакса $(4-2\delta^n, 4-2\delta^n, 4-2\delta^n)$, что при $\delta^n > \frac{1}{2}$ позволяло бы, например, конструировать совершенные подыгровые равновесия с вектором выплат $(6,3,3)$, недостижимым ни в одном равновесии по Нэшу однократного трёхстороннего чёт-нечета.

Покажем теперь, как учёт стоимости вычислений позволяет правильным подбором длины ключа $n$ достичь необходимого запрета на стратегию «взлома». Выпишем для каждой из предложенных стратегий дисконтированные затраты на выбор ходов:

- $M^a[\mathfrak{s}^\varnothing] = 0$, поскольку для любого разумно устроенного вычислительного устройства обычные смешанные стратегии, очевидно, можно считать бесплатными или почти бесплатными;
- $M^a[\mathfrak{s}_n^L] = M^a[\mathfrak{s}_n^R] = (1-\delta)M^a[f_n] + \delta^n((1-\delta)M^a[h_n] + M_a[G_n])$, поскольку для стратегий рукопожатия необходимо один раз перед первым ходом создать пару ключей, по прошествии $n$ ходов вычислить общий секретный ключ, а потом каждый ход генерировать по одному биту CSPRNG;
- $M^a[\mathfrak{s}_n^*] = \delta^n((1-\delta)(M^a[f_n^{-1}] + M^a[h_n]) + M_a[G_n])$, поскольку для стратегии взлома необходимо один раз по прошествии $n$ ходов, имея только пару публичных ключей, вычислить секретный ключ, а потом каждый ход генерировать по одному биту CSPRNG.

Проверим теперь ситуацию $(\mathfrak{s}_n^L, \mathfrak{s}_n^R, \mathfrak{s}^\varnothing)$ на равновесие по Нэшу с учётом расходов на вычисления. Для первых двух игроков требуется, чтобы затраты на криптографическую синхронизацию не превысили доход от хвоста розыгрыша, т.е. $\frac{1-\delta}{\delta^n} M^a[f_n] + (1-\delta)M^a[h_n] + M^a[G_n] \leqslant 1$. Несложно заметить, что до тех пор, пока $M^a[G_n] < 1$, всегда можно подобрать $\delta$ достаточно большое для нивелирования разовых подготовительных расходов. Для третьего же игрока наоборот, приходится подбирать достаточно большую битовую длину ключа, чтобы процедура его взлома оказалась дороже, чем потенциальный доход в хвосте розыгрыша, т.е. $(1-\delta)(M^a[f_n^{-1}] + M^a[h_n]) + M_a[G_n] \geqslant 2$. Здесь уже в качестве главного компонента выступает экспоненциально растущая стоимость обращения односторонней функции — при $M^a[f_n^{-1}] \geqslant \frac{2}{1-\delta}$ присоединение к коррелированной стратегии полностью теряет смысл. Таким образом, чтобы рассматриваемая точка

была равновесием по Нэшу, достаточно выполнения следующего набора условий:

$$\begin{cases} (1-\delta)(\delta^{-n}M^1[f_n] + M^1[h_n]) + M^1[G_n] < 1; \\ (1-\delta)(\delta^{-n}M^2[f_n] + M^2[h_n]) + M^2[G_n] < 1; \\ (1-\delta)M^3[f_n^{-1}] \geqslant 2. \end{cases}$$

Поскольку речь идёт о сравнении производительности абстрактных вычислительных устройств с безразмерными величинами, характеризующими предпочтения рациональных агентов, попытки доказательства каких-либо формальных утверждений относительно совместимости этой системы неравенств представляются малопродуктивными. Тем не менее, мы вполне можем попробовать отобразить выделенную неравенствами область допустимых величин $n$ и $\delta$ на соответствующие объекты реального мира. На практике криптосистемы, использующие дискретное логарифмирование на эллиптических кривых, считаются надёжными уже при 256-битных ключах (Curve25519 [21], например), т.е. стоимость их взлома заведомо превосходит возможности, доступные человеческой цивилизации на текущем этапе технологического развития. Одновременно с этим существуют и широко используются генераторы псевдослучайных чисел с 256-битным зерном, считающиеся криптографически стойкими (CTR-DRBG [22], например). Это задаёт для дисконтирующего коэффициента диапазон приемлемости $0 < \varepsilon \leqslant 1 - \delta \leqslant \frac{1}{370}$, причём, поскольку вычисление $f_{256}^{-1}$ на данный момент считается невозможным, $\varepsilon$ можно считать бесконечно малым. Таким образом, если игроки, в распоряжении которых находятся современные вычислительные устройства, будут играть с реальными ставками в повторяющийся трёхсторонний чёт-нечет, то протяжённости серий от нескольких сотен розыгрышей окажется достаточно, чтобы применение криптографического согласования стратегий стало реальным способом получить преимущество.

### 3.5 Народная теорема для игр с учётом стоимости вычислений

При помощи уточнённого варианта «народной» теоремы продемонстрированный в предыдущем разделе фокус можно обобщить для пополнения множества совершенных подыгровых равновесий любой повторяющейся игры, отдельные итерации которой чувствительны к дополнительной информационной

асимметрии. С этой целью в качестве наказаний для игрока, отклоняющегося от предписанной стратегии, могут использоваться наборы, коррелированные в пространстве заговоров, состоящем из единственной группы, включающей всех игроков кроме самого наказываемого. Поскольку при этом стратегии зависят не более чем от одного корреляционного механизма, можно упростить рассуждения, перейдя к вероятностным распределениям на платёжной матрице. Рассматривая игру $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ с множествами участников $A = \{1, \ldots, m\}$ и исходов $S = S^1 \times \ldots \times S^m$ соответственно, введём обозначения:

$$\mathbf{P}_S = \{\mu : S \to [0,1] \mid \sum_{s\in S} \mu(s) = 1\};$$
$$\mathbf{P}_S^{\setminus a} = \{\mu \in \mathbf{P}_S \mid \forall s_1, s_2 \in S, s^a \in S^a, \mu(s_1)\mu(s_2|s^a) = \mu(s_2)\mu(s_1|s^a)\}.$$

Здесь $\mathbf{P}_S$ представляет собой всевозможные вероятностные меры на множестве исходов $S$, а $\mathbf{P}_S^{\setminus a}$ — все вероятностные меры, гарантирующие попарную независимость выбора стратегии игроком $a$ с действиями всех остальных. Очевидно, выплаты при этом вычисляются по формуле математического ожидания:

$$u^a(\mu) = \sum_{s\in S} \mu(s)u^a(s).$$

Кроме того, для удобства обозначим девиацию игрока $a$ в пользу чистой стратегии $s_0^a$ аналогичным классической нотации образом:

$$\mu|s_0^a(s) = \begin{cases} \sum_{s_*^a \in S^a} \mu(s|s_*^a), & s^a = s_0^a; \\ 0, & s^a \neq s_0^a. \end{cases}$$

Теперь можно наконец ввести уточнённое для рассматриваемой модели понятие о резервном выигрыше:

**Определение 3.5.1.** Слепым резервным выигрышем игрока $a$ в игре $\Gamma$ называется его резервный выигрыш $u^a(\check{\mu}^a)$ в игре $\Gamma|\{A\setminus\{a\}\}$, т.е. с заговором, объединяющим всех игроков кроме него:

$$\check{\mu}^a \in \arg\min_{\mu\in\check{\mathbf{P}}} u^a(\mu),$$

где $\check{\mathbf{P}} = \{\mu \in \mathbf{P}_S^{\setminus a} \mid u^a(\mu) \geqslant u^a(\mu|s^a), \forall s^a \in S^a\}$.

Для классической народной теоремы резервные выигрыши напрямую определяют соответствующую точку минимакса, однако в нашем случае всё немного

сложнее. Поскольку для синхронизации как предписанных стратегий, так и наказаний используются CSPRNG, необходимо учитывать стоимость вычисления необходимой для выбора стратегического набора последовательности псевдослучайных битов. Обозначим символом $\mathfrak{b}(\mu) \in \mathbb{R}_{\geqslant 0}$ среднее количество бит, необходимое для выбора коррелированного набора стратегий по следующей процедуре. Занумеруем все исходы $\{s_1, \ldots, s_k\} \subseteq S$, участвующие в $\mu$ с ненулевой вероятностью, и построим в единичном интервале $[0, 1)$ сетку неубывающих чисел $\rho = (\rho_0 = 0, \rho_1, \ldots, \rho_{k-1}, \rho_k = 1)$ разбивающую его таким образом, что $\rho_j - \rho_{j-1} = \mu(s_j), j = \overline{1,k}$.

1. Положим $\mathcal{X}_{min} = 0$ и $\mathcal{X}_{max} = 1$.
2. Проверим, нет ли такого $j$, что $\rho_{j-1} \leqslant \mathcal{X}_{min} < \mathcal{X}_{max} \leqslant \rho_j$. Если есть, остановим алгоритм, приняв решение о выборе стратегического набора $s_j$.
3. Сгенерируем очередной бит псевдослучайной последовательности. Значение $\frac{\mathcal{X}_{min}+\mathcal{X}_{max}}{2}$ в случае $0$ присвоим переменной $\mathcal{X}_{max}$, а в случае $1$ — $\mathcal{X}_{min}$.
4. Перейдём к шагу 2.

Если все игроки используют CSPRNG с одним и тем же зерном, очевидно, что они выберут один и тот же набор стратегий, использовав при этом одно и то же количество псевдослучайных битов, в среднем зависящее только от распределения вероятностей $\mu$. Следовательно, ожидаемый доход игрока $a$ с учётом стоимости вычислений можно представить как $u^a_{M,n}(\mu) = u^a(\mu) - \mathfrak{b}(\mu)M^a[G_n]$, где $M^a[G_n]$ — стоимость генерации одного псевдослучайного бита. Заметим, что полученное значение зависит ещё и от $n$, т.е. битовой длины используемого зерна CSPRNG, что приводит к необходимости заменять понятие о точке минимакса более сложным определением:

**Определение 3.5.2.** Распределение вероятностей $\mu$ на множестве исходов игры в нормальной форме $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ называется $M,n$-приемлемым, если $u^a_{M,n}(\mu) > u^a(\check{\mu}^a)$ для каждого игрока $a \in A$.

Заметим, что мы пока говорили о том, как игроки используют для синхронизации действий CSPRNG с общим зерном, не уточняя, как именно это общее зерно вырабатывается. Аналогично примеру из предыдущего раздела в этом качестве будем использовать общие секретные ключи, вычисляемые по протоколу DH. Опишем процедуру для генерации и публикации ключей. Сперва каждый игрок $a$

выбирает случайное вещественное число $\chi^a$, равномерно распределённое в диапазоне $[0, 2^n)$. Округление этого числа $x^a = \lfloor \chi^a \rfloor \in \mathbb{N}_{<2^n}$ используется им далее в качестве закрытого ключа. При помощи односторонней функции игрок вычисляет открытый ключ $X^a = f(x^a) \in \mathbb{N}_{<2^n}$. Для обмена значениями $X^a$ игроки могут использовать любой условленный *тотально смешанный* набор стратегий:

**Определение 3.5.3.** Набор смешанных стратегий назовём тотально смешанным, когда в его составе нет ни одной чистой стратегии.

Поскольку $f$ — биекция, случайная величина $\mathcal{X}^a = \chi^a - x^a + X^a$ также равномерно распределена в диапазоне $[0, 2^n)$. Для того, чтобы раскрыть другим игрокам своё значение $X^a$, каждый игрок использует метод «фрактального» кодирования числа $\mathcal{X}^a$ в последовательности совершаемых им ходов, неотличимых по вероятностному распределению от смешанной стратегии $s_0^a = (p_1^a, \ldots, p_{|S^a|}^a)$ из условленного тотально смешанного набора $s_0$. Построим в единичном интервале $[0, 1)$ сетку неубывающих чисел $\rho^a = (\rho_0^a = 0, \rho_1^a, \ldots, \rho_{|S^a|-1}^a, \rho_{|S^a|}^a = 1)$ разбивающую его таким образом, что $\rho_j^a - \rho_{j-1}^a = p_j^a, j = \overline{1,|S^a|}$. Это позволяет применить следующий алгоритм кодирования:

1. До совершения первого хода другие игроки знают, что $\mathcal{X}^a$ равномерно распределено в интервале $[0, 2^n)$. Положим $\mathcal{X}_{min}^a = 0$ и $\mathcal{X}_{max}^a = 2^n$.
2. Отмасштабируем $\rho^a$ на интервал $[\mathcal{X}_{min}^a, \mathcal{X}_{max}^a)$, получив вложенную в него сетку $\mathcal{P}^a = (\mathcal{X}_{min}^a(1 - \rho_j^a) + \mathcal{X}_{max}^a \rho_j^a, j = \overline{0, |S^a|})$.
3. Выберем на очередной итерации $s_j^a$ такое, что $\mathcal{P}_{j-1}^a \leqslant \mathcal{X}^a < \mathcal{P}_j^a$.
4. Теперь другие игроки знают, что $\mathcal{X}^a$ равномерно распределено в интервале $\left[\mathcal{P}_{j-1}^a, \mathcal{P}_j^a\right)$. Вернёмся к шагу 2, положив $\mathcal{X}_{min}^a = \mathcal{P}_{j-1}^a$ и $\mathcal{X}_{max}^a = \mathcal{P}_j^a$.

Этот алгоритм может выполняться бесконечно, постепенно уменьшая меру незнания других игроков относительно величины $\mathcal{X}^a$. При этом на каждой отдельной итерации распределение вероятностей исходов неотличимо от набора смешанных стратегий $s_0$. В тот момент когда начинает выполняться неравенство $X^a \leqslant \mathcal{X}_{min}^a < \mathcal{X}_{max}^a \leqslant X^a + 1$, другие игроки получают уверенность относительно значения $X^a$, и открытый ключ игрока $a$ можно считать опубликованным. Если все игроки начинают публикацию ключей одновременно, то ожидаемое количество итераций до завершения публикации последнего из них зависит только от используемого стратегического набора $s_0$ и величины $n$, так что его можно обозначить символом $\mathfrak{t}(s_0, n) \in \mathbb{N}$.

Прежде чем переходить к аналогу народной теоремы для повторяющихся игр с учётом стоимости вычислений, необходимо ввести ещё одно обозначение. Вектор $\Delta u = (\Delta u^a, a \in A) \in \mathbb{R}^m_{\geqslant 0}$, где

$$\Delta u^a = \max_{s \in S, s^a_* \in S^a} (u^a(s|s^a_*) - u^a(s)),$$

состоит из максимальных доходов, которые может получить каждый игрок, отклоняясь от стратегии из произвольного предписанного набора.

**Теорема 3.5.1.** *Пусть $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ — произвольная матричная игра $m$ участников, имеющая хотя бы одно тотально смешанное равновесие $s_0$. Пусть $M = (M^1, \ldots, M^m)$ — набор универсальных вычислительных устройств, которые соответствующие игроки могут использовать для выбора очередного шага стратегии в повторяющейся игре. Пусть $(\Gamma)^\delta_M$ — бесконечно повторяющаяся игра с итерацией $\Gamma$, дисконтирующим коэффициентом $\delta$ и учётом стоимости эксплуатации вычислительных устройств $M$. Любому $M,n$-приемлемому распределению вероятностей $\mu$ на множестве исходов игры $\Gamma$ можно поставить в соответствие набор стратегий игры $(\Gamma)^\delta_M$ с выплатами каждого игрока $a$, равными*

$$(1 - \delta^{\mathfrak{t}(s_0,n)})u^a(s_0) + \delta^{\mathfrak{t}(s_0,n)} u^a_{M,n}(\mu) - (1-\delta)(M^a[f_n] + \delta^{\mathfrak{t}(s_0,n)}(m-1)M^a[h_n]).$$

*При этом для того, чтобы этот набор оказался равновесием по Нэшу, достаточно выполнения следующих условий для каждого $a \in A$:*

1. $(1-\delta)(M^a[f_n] + \delta^{\mathfrak{t}(s_0,n)}(m-1)M^a[h_n]) < \delta^{\mathfrak{t}(s_0,n)}(u^a_{M,n}(\mu) - u^a(\check{\mu}^a))$;
2. $(1-\delta)\Delta u^a < \delta(u^a_{M,n}(\mu) - u^a(\check{\mu}^a))$;
3. $(1-\delta)M^a[f_n^{-1}] > \delta\Delta u^a$.

*Доказательство.* Равновесие, соответствующее $M,n$-приемлемому распределению вероятностей $\mu$ строится как трёхэтапный процесс:

– *Синхронизация.* Сперва каждый игрок $a$ создаёт пару ключей длины $n$, терпя при этом убыток равный $(1-\delta)M^a[f_n]$. Затем, используя вышеописанный алгоритм фрактального кодирования в тотально смешанном равновесии $s_0$, публикует свой открытый ключ. Эта фаза продолжается до тех пор, пока не будут опубликованы все ключи, что в среднем займёт $\mathfrak{t}(s_0, n)$ ходов, давая суммарный выигрыш $(1-\delta^{\mathfrak{t}(s_0,n)})u^a(s_0)$. Завершается стадия вычислением общего секретного ключа, для чего каждому игроку

необходимо $m-1$ раз вычислить функцию $h_n$, что соответствует убытку размером $(1-\delta)\delta^{\mathrm{t}(s_0,n)}(m-1)M^a[h_n]$.

– *Розыгрыш.* Используя CSPRNG, инициируемое общим секретным ключом, игроки на каждой итерации псевдослучайно выбирают в соответствии с распределением $\mu$ новый набор чистых стратегий, так что каждый игрок $a$ получает при бесконечном повторении ожидаемый суммарный выигрыш $\delta^{\mathrm{t}(s_0,n)}u^a_{M,n}(\mu)$. Если ни один из игроков не отклонился от предписанного поведения ни на предыдущей стадии, ни на этой, то итоговые выплаты в пределе соответствуют предсказанным в формулировке теоремы.

– *Наказание.* Если любой из игроков на стадии розыгрыша выбирает чистую стратегию, не соответствующую предписанной CSPRNG, остальные игроки переключаются в режим его наказания. То же самое происходит сразу после стадии синхронизации, если на ней кто-то из игроков игнорирует процедуру создания ключей. Для этого они вычисляют новый общий секретный ключ, на этот раз исключая публичный ключ наказываемого игрока $a$. Инициировав CSPRNG этим новым ключом, они на каждой итерации псевдослучайно выбирают новый набор чистых стратегий в соответствии с распределением $\breve{\mu}^a$.

От этой схемы предписанных действий возможны несколько видов индивидуальных отклонений. Во-первых, на стадии синхронизации любой игрок $a$ может попытаться сэкономить путём отказа от создания пары ключей и вычисления общего секретного ключа. Поскольку набор $s_0$ равновесен по Нэшу, улучшить выигрыш по сравнению с $(1-\delta^{\mathrm{t}(s_0,n)})u^a(s_0)$ не получится, но можно используя простую смешанную стратегию избежать расходов на криптографию в размере $(1-\delta)(M^a[f_n]+\delta^{\mathrm{t}(s_0,n)}(m-1)M^a[h_n])$. Реакцией на это решение становится переход остальных игроков к стадии наказания игрока $a$ сразу по завершении публикации ключей, так что вместо $\delta^{\mathrm{t}(s_0,n)}u^a_{M,n}(\mu)$ в хвосте розыгрыша игрок получает $\delta^{\mathrm{t}(s_0,n)}u^a(\breve{\mu}^a)$. Такое отклонение делает невыгодным ограничение на $\delta$, накладываемое условием 1 формулировки теоремы.

Во-вторых, на основной стадии розыгрыша любой игрок $a$ может, вычислив очередной псевдослучайный набор $s_i$ отказаться играть предписанную стратегию $s^a_i$ в пользу более выгодной, получив разовый доход, не превосходящий $(1-\delta)\delta^i\Delta u^a$. Заметив это, остальные игрокаи переходят к стадии наказания, что уменьшает его доход в хвосте розыгрыша с $\delta^{i+1}u^a_{M,n}(\mu)$ до $\delta^{i+1}u^a(\breve{\mu}^a)$. Та-

кое отклонение делает невыгодным ограничение на $\delta$, накладываемое условием 2 формулировки теоремы.

В-третьих, поскольку слепые наказания опираются на то, что наказываемый игрок $a$ не может предсказать биты CSPRNG, инициированного общим секретным ключом, вычисление которого производилось без использования его собственной пары ключей, он может попытаться ослабить наказание, «взломав» секретный ключ путём обращения односторонней функции на одном из открытых ключей. Если это происходит на $i$-й итерации игры, то он должен потратить на это $(1-\delta)\delta^i M^a[f_n^{-1}]$, получив в результате не более чем $\delta^{i+1}\Delta u^a$ дохода от хвоста розыгрыша. Такое отклонение делает невыгодным ограничение на $\delta$, накладываемое условием 3 формулировки теоремы.

Таким образом предписанная процедура розыгрыша бесконечной повторяющейся игры $(\Gamma)^\delta_M$ действительно оказывается равновесием по Нэшу с искомыми ожидаемыми выигрышами. □

Несложно заметить, что доказанное утверждение является аналогом скорее самых первых формулировок «народной» теоремы, в которых речь ещё не шла о равновесиях, совершенных по подыграм. Увы, но методы, при помощи которых строятся совершенные подыгровые равновесия в классическом случае, по объективным причинам сложно перенести на игры с учётом стоимости вычислений. Как уже было упомянуто в начале главы, обычно для этого используется схема бесконечного наказания последнего отклонившегося от предписанной стратегии, применяющаяся в том числе и в процессе наказания предыдущего отклонившегося. Здесь же такой наивный подход натыкается на препятствие — рассмотрим ситуацию, в которой игрок $a$ решил сэкономить на создании ключей и вместо предписанной процедуры на стадии синхронизации просто играл смешанную стратегию $s_0^a$. Заметив это, остальные игроки по завершении обмена ключами начинают его слепое наказание коррелированным набором стратегий $\breve{\mu}^a$. Представим теперь, что будет, если один из наказывающих решит на очередной итерации использовать стратегию более выгодную для себя, чем предписывает в качестве наказания CSPRNG. По классической схеме такой игрок должен быть сам назначен наказываемым начиная со следующей итерации, причём в его наказании должен принимать участие в том числе и игрок $a$. Однако, поскольку игрок $a$ сэкономил на создании своей пары ключей, он просто не имеет возможности

вычислить общий секретный ключ, требующийся для этого, так что любое наказание, в котором он должен участвовать, перестаёт быть эффективной угрозой.

Ещё одним заметным недостатком доказанной теоремы можно считать то, что она неявно опирается на наблюдаемость стратегий, используемых игроками. Подразумевается, что единственная тайна, которую игроки скрывают от своих оппонентов - это конкретные значения ключей, тогда как применяемые ими алгоритмы известны публично. Однако, утверждение могло бы стать намного сильнее и убедительнее, если бы мы считали публично известными только конкретные чистые стратегии, играемые участниками. Это имеет значение, например, когда мы говорим, что игрок, решивший сэкономить на создании ключей, назначается наказываемым по окончании стадии синхронизации — ведь если игроки могут судить о том, создавал кто-то ключи или нет, только по совершаемым ходам, то в течение некоторого количества первых итераций стадии розыгрыша отклонившийся мог бы случайно угадывать, какую стратегию предписывает CSPRNG, даже без общего секретного ключа, просто выбирая наиболее вероятную в соответствии с распределением $\mu$ стратегию. Причём, если распределение $\mu$ таково, что в нём кто-то должен играть одну и ту же чистую стратегию с вероятностью $1$, то ему вообще не имеет смысла создавать ключи, поскольку отказ от их создания никогда не будет раскрыт.

Эту же уязвимость можно использовать ещё более тонким образом, если доход игрока $a$ от синхронизационного набора смешанных стратегий $s_0$ превышает его доход от целевого распределения $\mu$. Если вместо случайного выбора значения $\chi^a$ при создании ключей игрок будет «подкручивать» его дробную часть так, чтобы она была близка к $0$ или $1$, то тем самым он может произвольно увеличивать продолжительность стадии синхронизации и, соответственно, свой итоговый доход. Описанные проблемы, возникающие при отказе от наблюдаемости используемых игроками алгоритмов, вряд ли можно назвать непреодолимыми, однако попытки их решения в рамках данной работы значительно усложнили бы формальные рассуждения, не привнеся при этом ничего ценного для понимания центральных её идей.

Кроме того следует обратить внимание на то, что, поскольку условия теоремы ограничивают значение дисконтирующего коэффициента $\delta$ как снизу, так и сверху, её невозможно сформулировать в более изящной форме для сколь угодно малых $\varepsilon$-приближений к вектору выплат $u_{M,n}(\mu)$. Однако мы можем отобразить её параметры на объекты реального мира, чтобы иметь возможность судить о

её практических следствиях. Представим себе, что используемый игроками набор вычислительных устройств $M$ — это современные компьютеры, а $n = 256$, что совпадает с наиболее распространённой в современной криптографии длинной ключей. Для удачно подобранных[1] смешанных равновесий $s_0$ можно ожидать, что средняя продолжительность стадии обмена ключами $\mathrm{t}(s_0, n)$ по порядку величины будет совпадать со значением $n$, то есть измеряться сотнями итераций. Это значит, что в сериях розыгрышей с хотя бы ста тысячами значимых итераций вклад стадии синхронизации уже заведомо не будет превышать одного процента от итогового результата. Учитывая, что, к примеру, системы для автоматизированного трейдинга на биржах вполне могут совершать сотни тысяч транзакций в день, для многих практических применений это можно считать неплохим приближением.

Далее, стоимость вычисления функций, использующихся при создании общих секретных ключей, т.е. $M^a[f_{256}]$ и $M^a[h_{256}]$ хотя и нельзя считать пренебрежимо малой, но для её оценки можно заметить, что каждое открытие интернет-страницы современным браузером в подавляющем большинстве случаев подразумевает генерацию нескольких ключевых пар и соответствующих общих секретных ключей. Наконец, стоимость генерации псевдослучайных последовательностей современными CSPRNG, т.е. $M^a[G_{256}]$ на масштабе в миллионы битов уже можно считать пренебрежимо малой, так как, скажем, передача изображения с видеокарты на монитор современного компьютера по цифровому интерфейсу HDMI подразумевает шифрование потока, измеряющегося десятками гигабит в секунду, а алгоритм, использующийся в процессе этого шифрования, может использоваться и для генерации псевдослучайных последовательностей.

Наконец, остаётся заметить, что обращение односторонней функции с 256-битным аргументом считается на данный момент невозможным и предполагается, что оно останется таковым вплоть до создания функционирующих квантовых компьютеров. Это означает, что значение $M^a[f_{256}^{-1}]$ для практических применений можно считать почти бесконечным, что позволяет $\delta$ приближаться к 1 на сколь угодно малое (в смысле реальных конфликтов) расстояние.

[1] Здесь подразумевается, что никто из игроков не выбирает одну из своих чистых стратегий с вероятностью близкой к 1.

## 3.6 Обобщение результатов, перспективы и гипотезы

Для того, чтобы оценить значение этого феномена, следует отступить на пару шагов от конкретики описанной игры и попытаться охватить взглядом более широкую картину. Во-первых, благодаря обобщению народной теоремы становится очевидно, что сам по себе трёхсторонний чёт-нечет выступает в роли не более чем относительно произвольно сконструированного примера игры, чувствительной к дополнительной информационной асимметрии. Вышеописанные криптографические стратегии наказания не используют фактически никаких других свойств данного конфликта и нет причин думать, что они не могут быть обобщены на множество других игр, проявляющих то же свойство. К примеру, если мы возьмём в качестве отдельной итерации игру $\Gamma_n^3$ из второй главы этой работы, то окажется, что при её повторении можно аналогичным образом кодировать открытые ключи алфавитом, состоящим из $n$ символов по числу компьютеров в вычислительном центре, а потом использовать полученный общий секретный ключ в качестве зерна генератора, псевдослучайно выбирающего из опять же $n$ элементов.

Во-вторых, имеет смысл задаться вопросом о том, исчерпывает ли описанная схема криптографических стратегий наказания все возможности для пополнения множества совершенных подыгровых равновесий. Здравый смысл подсказывает, что нет хотя бы потому, что оба использованных здесь криптографических примитива (и протокол совместной выработки ключа, и криптографически стойкий генератор псевдослучайных чисел) имеют немало реализаций, опирающихся на самые разные математические формализмы, список которых год от года пополняется благодаря бурному развитию соответствующих областей знания. Более того, построение стратегии наказания из протокола DH с последующим использованием полученного ключа в качестве зерна CSPRNG само по себе достаточно произвольно — мы использовали инструменты, изначально создававшиеся в совершенно ином контексте для других целей, просто потому, что они уже есть и имеют доказанные свойства, удобные для решения нашей задачи.

Эти рассуждения позволяют обоснованно предположить, что и сам трёхсторонний чёт-нечет, и представленные криптографические стратегии наказания — всего лишь наиболее очевидные представители более широкого класса пока ещё

не исследованных математических формализмов. Говоря максимально общим языком, рациональные агенты, участвуя в повторяющихся конфликтах, могут вырабатывать секретные коррелированные стратегии поведения, используя лишь специальным образом выбираемые публичные действия и наблюдая за аналогично действующим контрагентом. Секретность при этом обеспечивается за счёт того, что присоединение к корреляции требует от наблюдающей ту же последовательность публичных действий третьей стороны когнитивных усилий, превосходящих её возможности. Кроме того, обобщая связь между удельной стоимостью вычислений и требуемой длиной ключей, можно предположить, что чем большие когнитивные усилия способна приложить сторона, от которой заговорщики пытаются скрыть свою общую стратегию, тем сложнее этот процесс и тем меньший доход (за счёт растущего дисконтирования в хвосте розыгрышей) приносит такая секретность.

В самом деле, если представить себе обычных людей, играющих в чувствительную к дополнительной информационной асимметрии игру без применения специальных технических средств, мы вряд ли можем ожидать, что они будут производить в уме вычисления, необходимые для связки DH+CSPRNG. При этом, вполне вероятно, что повсеместно распространены примеры того, как люди могут добиваться необходимой тайной синхронизации неосознанно, воспринимая результат как самоочевидный, не требующий объяснений факт. В данном случае имеются в виду опытные картёжники, специализирующиеся на сложных интеллектуальных играх, таких как бридж или преферанс. В их среде считается неоспоримым, что помимо индивидуальных навыков на исход розыгрышей сильно влияет опыт именно совместной игры — пара игроков, по отдельности не хватающих звёзд с небес, могут оказаться грозными соперниками, если у них за плечами много партий за одним столом. Если верны вышеизложенные предположения о достаточно общем характере построенной нами модели, то феномен такой «сыгранности» может найти удовлетворительное объяснение в её рамках.

Следует заметить, что если мы захотим исследовать с этой точки зрения стратегии игроков в уже существующие салонные игры, на нашем пути могут встать затруднения, связанные с тем, что правила тех из них, что можно заподозрить в чувствительности к дополнительной информационной асимметрии, сложны даже без учёта этого их свойства. Скажем, бридж или преферанс останутся, очевидно, весьма нетривиальными, даже если играть в них отдельными партиями, каждый раз подбирая состав анонимных участников случайно

из большого пула кандидатов (удалённо по сети, например). Для облегчения задачи будущих исследователей неплохо было бы сконструировать специальную карточную игру, в которой использование эффекта «сыгранности» было бы необходимым элементом любой успешной стратегии. Попытка создания такой новой игры под названием «Тессеракт» вынесена в Приложение Г — будем надеяться, что в будущем она окажется полезна как в научных, так и в развлекательных целях.

Завершить данную работу хотелось бы формулировкой достаточно смелой неформальной гипотезы, продолжающей линию рассуждений последней главы в русле популяционных игр:

**Гипотеза 3.6.1.** Если в популяции периодически (много раз на протяжении жизни одной особи) возникают конфликтные ситуации, модель которых чувствительна к дополнительной информационной асимметрии, и вероятность продолжения рода отдельными особями существенно зависит от их успеха в этих конфликтах, то давление отбора закрепляет в популяции признаки, способствующие увеличению когнитивного потенциала следующих поколений (понимаемого в общем смысле, как способность производить Тьюринг-полные вычисления над произвольными данными).

Если эта гипотеза верна, то чувствительность игр к дополнительной информационной асимметрии может оказаться «Святым Граалем» эволюционной теории игр — фактором, порождающим неограниченную гонку вооружений в сфере способностей к сложному поведению. Любые игры с этим свойством, даже будучи очень просты сами по себе, поощряют когнитивный потенциал участников необходимостью строить и раскрывать заговоры, так что его изучение может как обогатить наше понимание эволюции интеллекта наших предков, так и стать инструментом совершенствования технологий искусственного разума.

## Заключение

Основные результаты работы заключаются в следующем.

1. На основе анализа понятия коррелированного равновесия в контексте многосторонних конфликтов было сформулировано свойство чувствительности игр к дополнительной информационной асимметрии.
2. Исследование изоморфизма пространств корреляции позволило ввести сужающий их формализм пространства заговоров, с применением которого удобно рассуждать о влиянии дополнительной информационной асимметрии на решения игр.
3. Моделирование проблемы планирования заданий при допущении немонотонности функций отдачи показало, что в пространствах заговоров концепция структурной согласованности равновесий может использоваться как функциональный аналог классических критериев коллективной рациональности по отношению к равновесиям Нэша в смешанных стратегиях.
4. Для демонстрации значимости феномена чувствительности игр к дополнительной информационной асимметрии была построена модель повторяющихся конфликтов с учётом стоимости вычисления очередного шага стратегии.
5. В рамках построенной модели было показано, как в повторяющихся играх можно даже без дополнительной информационной асимметрии как таковой использовать современные криптографические примитивы для конструирования эффективных стратегий наказания, использующих чувствительность к ней.

Хочется надеяться, что эта работа привлечёт внимание специалистов к проблематике влияния дополнительной информационной асимметрии на исходы многосторонних конфликтов.

В заключение автор выражает благодарность и большую признательность научному руководителю Васину А. А. за поддержку, помощь, обсуждение результатов и научное руководство. Также автор благодарит Морозова В. В. за активное участие в работе над доказательствами теорем и авторов шаблона *Russian-Phd-LaTeX-Dissertation-Template* за помощь в оформлении диссертации.

## Словарь терминов

**пространство корреляции** : Дополнительный параметр коррелированного расширения игр в нормальной форме, характеризующий априорные знания игроков о событиях, напрямую не влияющих на исход конфликта

**пространство заговоров** : Пространство корреляции специальной структуры с простым конечным описанием в виде семейства групп игроков, называемых заговорами

**заговор** : Подмножество игроков, объединённое возможностью наблюдать за общим тайным механизмом корреляции, сигналы которого непредсказуемы для аутсайдеров

## Список литературы


1. *Aumann*, *R. J.* Subjectivity and correlation in randomized strategies [Text] / R. J. Aumann // Journal of Mathematical Economics. — 1974. — Mar. — Vol. 1, no. 1. — P. 67—96.
2. *Николенко*, *С.* Теория экономических механизмов: учебное пособие [Текст] / С. Николенко. — Москва : Интернет-университет информационных технологий БИНОМ. Лаборатория знаний, 2009. — (Основы экономики и менеджмента).
3. *Fudenberg*, *D.* The Folk Theorem in Repeated Games with Discounting or with Incomplete Information [Text] / D. Fudenberg, E. Maskin // Econometrica. — 1986. — Vol. 54, no. 3. — P. 533—554.
4. *Савченко*, *М. А.* Частично коррелированные равновесия в игровых моделях конкуренции [Текст] / М. А. Савченко, А. А. Васин // Ломоносовские чтения - 2017. — 2017.
5. *Савченко*, *М. А.* Влияние дополнительной информационной асимметрии на решения игр [Текст] / М. А. Савченко // Ломоносовские чтения - 2021. — 2021.
6. *Савченко*, *М. А.* Axiomatic approach to conspiracy theory [Text] / М. А. Савченко // IX Московская международная конференция по исследованию операций (ORM2018): Москва, 22–27 октября 2018 г.: Труды. — 2018.
7. *Савченко*, *М. А.* Computational complexity of strategies in repeated games sensitive to additional information asymmetry [Text] / М. А. Савченко // Конференция молодых ученых по математической экономике и экономической теории. — 2021.
8. *Савченко*, *М. А.* Нормативная теория заговоров [Текст] / М. А. Савченко // Математическая Теория Игр и её Приложения. — 2020. — Т. 12, № 1. — С. 33—59.
9. *Савченко*, *М. А.* Карточная игра «Тессеракт» [Текст] / М. А. Савченко // Математическая Теория Игр и её Приложения. — 2021. — Т. 13, № 3. — С. 58—74.

10. *Савченко*, *М. А.* Планирование заданий с немонотонной отдачей [Текст] / М. А. Савченко // Математическая Теория Игр и её Приложения. — 2022. — Т. 14, № 1. — С. 85—101.

11. *Savchenko*, *M. A.* Normative Conspiracy Theory [Text] / M. A. Savchenko // Automation and Remote Control. — 2021. — Vol. 82, no. 4. — P. 706—721.

12. *Колмогоров*, *А.* Основные понятия теории вероятностей [Текст] / А. Колмогоров. — 2-е изд. — М.: Наука, 1974.

13. *Богачев*, *В.* Основы теории меры [Текст]. Т. 1 / В. Богачев. — Москва-Ижевск : НИЦ «Регулярная и хаотическая динамика», 2003.

14. *Koutsoupias*, *E.* Worst-Case Equilibria [Text] / E. Koutsoupias, C. Papadimitriou // STACS 99. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1999. — P. 404—413.

15. *Agussurja*, *L.* The Price of Stability in Selfish Scheduling Games [Text] / L. Agussurja, H. Lau //. Vol. 7. — 12/2007. — P. 305—311.

16. *Aumann*, *R. J.* Acceptable points in general cooperative $n$-person games [Text] / R. J. Aumann // Annals of Mathematics Studies. — 1959. — Vol. 40. — P. 287—324.

17. *Bernheim*, *B.* Coalition-Proof Nash Equilibria I. Concepts [Text] / B. Bernheim, B. Peleg, M. D. Whinston // Journal of Economic Theory. — 1987. — Vol. 42, no. 1. — P. 1—12.

18. *Vasin*, *A.* The Folk theorem for dominance solutions [Text] / A. Vasin // International Journal of Game Theory. — 1999. — Vol. 28, no. 1. — P. 15—24.

19. *Boyd*, *C.* Protocols for Authentication and Key Establishment [Text] / C. Boyd, A. Mathuria. — Springer, 2003. — (Information Security and Cryptography).

20. *Gutmann*, *P. C.* Software Generation of Practically Strong Random Numbers [Text] / P. C. Gutmann // USENIX Security Symposium. — 1998.

21. *Bernstein*, *D. J.* Curve25519: New Diffie-Hellman Speed Records [Text] / D. J. Bernstein // Public Key Cryptography - PKC 2006. — Berlin, Heidelberg : Springer, 2006. — P. 207—228.

22. *Hoang*, *V. T.* Security Analysis of NIST CTR-DRBG [Text] / V. T. Hoang, Y. Shen // Advances in Cryptology – CRYPTO 2020 / ed. by D. Micciancio, T. Ristenpart. — Cham : Springer International Publishing, 2020. — P. 218—247.

23. *Myerson*, *R. B.* Optimal coordination mechanisms in generalized principal–agent problems [Text] / R. B. Myerson // Journal of Mathematical Economics. — 1982. — Vol. 10, no. 1. — P. 67—81.

24. *Myerson*, *R. B.* Multistage Games with Communication [Text] / R. B. Myerson // Econometrica. — 1986. — Vol. 54, no. 2. — P. 323—358.

25. *Aumann*, *R. J.* Correlated Equilibrium as an Expression of Bayesian Rationality [Text] / R. J. Aumann // Econometrica. — 1987. — Vol. 55, no. 1. — P. 1—18.

26. *Dhillon*, *A.* The Folk Theorem in Repeated Games with Discounting or with Incomplete Information [Text] / A. Dhillon, J. F. Mertens // Journal of Economic Theory. — 1996. — Vol. 68, no. 2. — P. 279—302.

27. *Hart*, *S.* A Simple Adaptive Procedure Leading to Correlated Equilibrium [Text] / S. Hart, A. Mas-Colell // Econometrica. — 2000. — Vol. 68, no. 5. — P. 1127—1150.

28. *Энгелькинг*, *Р.* Общая топология [Текст] / Р. Энгелькинг. — М. : Мир, 1986.

## Список рисунков

# Приложение А

## Краткий обзор литературы, посвящённой коррелированному расширению игр в нормальной форме

Концепция коррелированного расширения стала важным общеупотребимым инструментом во многих областях теории игр, и в частности на неё опирается знаменитый дизайн механизмов. В связи с этим нельзя не упомянуть статью Роджера Майерсона «Optimal coordination mechanisms in generalized principal-agent problems» [23]. В ней формулируется обобщённая задача принципал-агентов, в которой агенты обладают как тайной информацией, так и возможностью принимать решения, неподконтрольные принципалу. Показывается, что принципал может ограничиваться целенаправленно побуждающими прямыми механизмами координации, в которых агенты докладывают свою информацию принципалу, рекомендующему в ответ стратегии, образующие коррелированное равновесие. В конечном случае оптимальные механизмы координации могут быть найдены при помощи линейного программирования. Кроме того обсуждается проблематика систем с многими принципалами, в которых может не существовать некооперативного равновесия, так что вводится определение и показывается существование квази-равновесия.

Коррелированное расширение нашло своё место и применительно к исследованию игр в развёрнутой форме. Ещё одна статья Роджера Майерсона «Multistage Games with Communication» [24] рассматривает многостадийные игры с коммуникационным механизмом, функционирующим по принципу централизованного посредника. В коммуникационном равновесии ни один игрок не должен иметь возможность в одиночку увеличить свой выигрыш, манипулируя своими отчётами или действиями. Последовательное коммуникационное равновесие — это коммуникационное равновесие с системой условных вероятностей при которой ни один игрок не может получить выгоду от подобных манипуляций, даже если случаются события нулевой вероятности. Кодоминируемые действия определяются таким образом, что любое коммуникационное равновесие последовательно в том и только том случае, когда никто не использует кодоминируемых действий. Преобладающее коммуникационное равновесие определяется

как результат последовательного исключения кодоминируемых действий, и показывается его существование.

Ещё одной важной вехой стала статья «Correlated equilibrium as an expression of Bayesian rationality» [25], в которой Ауман показал, что формализм коррелированного равновесия снимает противоречие между «байесовским» и «теоретико-игровым» взглядом на мир. С байесовской позиции вероятности могут быть сопоставлены с чем угодно, даже с возможностью для игрока выбрать какую-либо стратегию в некоторой игре. С точки зрения самой теории игр, напротив, традиционно считается, что нельзя говорить о вероятностях событий, происходящих по воле рациональных агентов, нужно вместо этого использовать понятие равновесности (или другие теоретико-игровые конструкты). Предложенный формализм же объединяет две эти точки зрения — на коррелированное равновесие можно смотреть как на следствие байесовской рациональности, поскольку условие равновесности представляет собой простую максимизацию выгоды каждым из игроков с учётом известной им информации. При таком подходе не требуется явной рандомизации в действиях игроков. Даже если игрок выбирает конкретную чистую стратегию без элемента случайности, вероятностная природа стратегий отражает неуверенность остальных игроков в его выборе, что и показывается на примерах.

Вопросы совместимости коррелированных равновесий с более строгими принципами оптимальности поднимались в статье Амриты Дхиллона и Жана Франсуа Мертенса «Perfect Correlated Equilibria» [26]. В ней вводится понятие $(\varepsilon)$-совершенных кореллированных равновесий (РСЕ), обусловленных $(\varepsilon)$-совершенным равновесием некоторого корреляционного устройства. Показывается, что «принцип выявления» для этой концепции теряет силу — прямой механизм может и не обеспечивать совершенного равновесия. Так называемые приблизительно совершенные коррелированные равновесия (АРСЕ) оказываются пределами $\varepsilon$-РСЕ, и авторы достигают для них полной характеризации. В ходе рассуждений о «приемлемости» АРСЕ в некотором смысле, приводятся однако иллюстрированные доводы в пользу того, что среди них именно РСЕ представляются «хорошими».

Динамический аспект формализма коррелированного расширения тоже не оставался без внимания исследователей. Предлагалось немало процедур разыгрывания для итеративных игр, обеспечивающих сходимость к коррелированным равновесиям. Среди множества работ на эту тему выделяется статья Серджиу

Харта и Андреу Мас-Колелла «A simple adaptive procedure leading to correlated equilibrium» [27], в которой авторы предложили так называемую процедуру сопоставления потерь. Применяя её, игроки каждый раз отклоняются от своих текущих стратегий пропорционально мере понесённого ими на предыдущих ходах ущерба от не использования иных стратегий. Показывается, что такая адаптивная процедура гарантирует в любой игре сходимость с вероятностью 1 эмпирического распределения розыгрышей к множеству коррелированных равновесий.

# Приложение Б

## Доказательство теоремы об изоморфизме пространств корреляции[1]

Прежде чем перейти к доказательству основного утверждения потребуется ввести дополнительный инструментарий:

**Определение Б.0.1.** Измельчением множества исходов $X = X^1 \times \ldots \times X^m$ до конечного множества исходов $Y = Y^1 \times \ldots \times Y^m$ называется любое отображение $\rho = (\rho^1, \ldots, \rho^m)$, где каждая компонента $\rho^a$ отображает $Y^a$ в $X^a$.

При помощи измельчений можно задавать связи между разбиениями с различными кодоменами. Если разбиения $f : \Omega \to X$ и $g : \Omega \to Y$ таковы, что $f = \rho \circ g$, то $f^{-1}(x) = \bigcup_{y \in \rho^{-1}(x)} g^{-1}(y), \forall x \in X$. При этом $f$ можно называть измельчимым до $g$.

Разбиения одного и того же пространства можно комбинировать. Например, из разбиений $g_i : \Omega \to Y_i = Y_i^1 \times \ldots \times Y_i^m, i = \overline{1,n}$ можно построить их комбинацию $g_1 \diamond \ldots \diamond g_n : \Omega \to Y_{(n)}$, где $Y_{(n)}^a = Y_1^a \times \ldots \times Y_n^a$ и $(g_1 \diamond \ldots \diamond g_n)^a(\omega) = (g_1^a(\omega), \ldots, g_n^a(\omega)), \forall \omega \in \Omega, a = \overline{1,m}$. Эта комбинация разбиений связана со своими компонентами измельчениями-проекциями: $g_i = \pi_i \circ (g_1 \diamond \ldots \diamond g_n), \pi_i^a(x_1^a, \ldots, x_n^a) = x_i^a$.

Аналогично комбинируются и измельчения с общим кодоменом. Например, из измельчений $\rho_i : Y_i \to X, i = \overline{1,n}$ можно построить комбинацию $\rho_1 \wr \ldots \wr \rho_n : Y_{[n]} \to X$, где $Y_{[n]}^a = \{(y_1^a, \ldots, y_n^a) \in Y_{(n)}^a \mid \rho_1^a(y_1^a) = \ldots = \rho_n^a(y_n^a)\}, a = \overline{1,m}$, причём на своей области определения $\rho_1 \wr \ldots \wr \rho_n$ совпадает со всеми $\rho_i \circ \pi_i$. Заметим, что

$$f = \rho_i \circ g_i, i = \overline{1,n} \Leftrightarrow f = (\rho_1 \wr \ldots \wr \rho_n) \circ (g_1 \diamond \ldots \diamond g_n).$$

**Определение Б.0.2.** В пространстве корреляции $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$ структурой разбиения $f : \Omega \to X$, порождённой измельчением $\rho : Y \to X$, называется множество $H_{\Phi,\rho}(f) = \{\mathbb{P} \circ g^{-1} \mid g \models \Phi, f = \rho \circ g\}$, состоящее из мер $\mu : Y \to \mathbb{R}_{\geqslant 0}$. Также обозначим $H_{\Phi,\rho}^{-1}(\mu) = \{f \models \Phi \mid \mu \in H_{\Phi,\rho}(f)\}$.

[1] Цитируется по материалам статьи [8].

**Лемма Б.0.1.** *Для всех* $\rho : Y \to X$ *и* $\mu : Y \to \mathbb{R}_{\geqslant 0}$ *множество* $H^{-1}_{\Phi,\rho}(\mu) \subseteq X^{\Omega}$ *компактно в полуметрике*

$$\operatorname{dis}(f_1, f_2) = \frac{1}{2} \sum_{x \in X} \left| \mathbb{P}(f_1^{-1}(x)) - \mathbb{P}(f_2^{-1}(x)) \right|.$$

*Доказательство.* Переформулируем $H^{-1}_{\Phi,\rho}(\mu) = \rho \circ H^{-1}_{\Phi}(\mu)$, определив для этого отображение $H^{-1}_{\Phi}(\mu) = \{g \models \Phi \mid \mathbb{P} \circ g^{-1} = \mu\}$. Докажем сперва компактность $H^{-1}_{\Phi}(\mu)$, вводя $\operatorname{dis}(g_1, g_2)$ аналогично $\operatorname{dis}(f_1, f_2)$. Полуметрика dis вполне ограниченна, так как $\operatorname{dis}(g_1, g_2) = d(\mu_1^Y, \mu_2^Y)$, где $\mu_k^Y = \mathbb{P} \circ g_k^{-1}, k = 1{,}2$, а пространство вероятностных мер на любом конечном множестве вполне ограниченно. Замкнутость $H^{-1}_{\Phi}(\mu)$ очевидно следует из $\operatorname{dis}(g_1, g_2) = 0 \Leftrightarrow \mathbb{P} \circ g_1^{-1} = \mathbb{P} \circ g_2^{-1}$. Таким образом $H^{-1}_{\Phi}(\mu)$ компактно в полуметрике dis. Докажем непрерывность отображения $\rho \circ : Y^{\Omega} \to X^{\Omega}$, выразив ту же полуметрику по-другому:

$$\operatorname{dis}(f_1, f_2) = 1 - \sum_{x \in X} \min\left[\mathbb{P}(f_1^{-1}(x)), \mathbb{P}(f_2^{-1}(x))\right].$$

Пусть теперь $f_1 = \rho \circ g_1$ и $f_2 = \rho \circ g_2$:

$$\begin{aligned}
\operatorname{dis}(\rho \circ g_1, \rho \circ g_2) &= 1 - \sum_{x \in X} \min\left[\mathbb{P}(g_1^{-1}(\rho^{-1}(x))), \mathbb{P}(g_2^{-1}(\rho^{-1}(x)))\right] \\
&= 1 - \sum_{x \in X} \min\left[\sum_{y \in \rho^{-1}(x)} \mathbb{P}(g_1^{-1}(y)), \sum_{y \in \rho^{-1}(x)} \mathbb{P}(g_2^{-1}(y))\right] \\
&\leqslant 1 - \sum_{x \in X} \sum_{y \in \rho^{-1}(x)} \min\left[\mathbb{P}(g_1^{-1}(y)), \mathbb{P}(g_2^{-1}(y))\right] \\
&= 1 - \sum_{y \in Y} \min\left[\mathbb{P}(g_1^{-1}(y)), \mathbb{P}(g_2^{-1}(y))\right] = \operatorname{dis}(g_1, g_2).
\end{aligned}$$

Отображение $\rho \circ$ непрерывно, поскольку $\operatorname{dis}(\rho \circ g_1, \rho \circ g_2) \leqslant \operatorname{dis}(g_1, g_2)$. Так как непрерывные отображения сохраняют компактность[28, с. 199], $H^{-1}_{\Phi,\rho}(\mu) = \rho \circ H^{-1}_{\Phi}(\mu)$ компактно в полуметрике dis. □

**Определение Б.0.3.** Разбиение $f_2 \models \Phi_2$ называется точным образом разбиения $f_1 \models \Phi_1$ (далее $f_1 \precsim f_2$), если их кодомены совпадают ($X_1 = X_2 = X$) и $H_{\Phi_1,\rho}(f_1) \subseteq H_{\Phi_2,\rho}(f_2)$ для всех измельчений $\rho$ с тем же кодоменом. Множество всех точных образов далее будем обозначать $\widehat{\Phi}_2(f_1) = \{f_2 \models \Phi_2 \mid f_1 \precsim f_2\}$.

Отношение $f_1 \precsim f_2$ можно понять так — на какие бы измеримые части мы не делили компоненты разбиения $f_1$, в разбиении $f_2$ соответствующие компоненты всегда можно разделить на равные им по мере части.

**Замечание Б.0.1.** Очевидно, что $f_1 \precsim f_2 \wedge f_2 \precsim f_3 \Rightarrow f_1 \precsim f_3$.

**Лемма Б.0.2.** *Пусть в пространствах корреляции* $\Phi_1$ *и* $\Phi_2$ *разбиения* $g_1 : \Omega_1 \to Y$ *и* $g_2 : \Omega_2 \to Y$ *таковы, что* $g_1 \precsim g_2$. *Тогда* $\rho \circ g_1 \precsim \rho \circ g_2$ *для всех измельчений* $\rho : Y \to X$.

*Доказательство.* Возьмём любые $\rho_* : Y_* \to X$ и $\mu \in H_{\Phi_1,\rho_*}(\rho \circ g_1)$. По определению структуры разбиения, $\exists g_{1*} : \rho_* \circ g_{1*} = \rho \circ g_1, \mathbb{P}_1 \circ g_{1*}^{-1} = \mu$, а доказать требуется, по определению точного образа, что $\exists g_{2*} : \rho_* \circ g_{2*} = \rho \circ g_2, \mathbb{P}_2 \circ g_{2*}^{-1} = \mu$. Рассмотрим комбинацию $g_{1+} = g_1 \diamond g_{1*}$, где $g_1 = \pi \circ g_{1+}$ и $g_{1*} = \pi_* \circ g_{1+}$. Здесь $g_{1+} : \Omega_1 \to Y_+, Y_+^a = Y^a \times Y_*^a, a = \overline{1,m}$. По определению структуры разбиения, $\mathbb{P}_1 \circ g_{1+}^{-1} \in H_{\Phi_1,\pi}(g_1)$, а значит, поскольку $g_1 \precsim g_2$, существует $g_{2+} : \Omega_2 \to Y_+$ такое, что $\mathbb{P}_1 \circ g_{1+}^{-1} = \mathbb{P}_2 \circ g_{2+}^{-1} \in H_{\Phi_2,\pi}(g_2)$, т.е. $\pi \circ g_{2+} = g_2$. Из этого с очевидностью следует, что и $\mathbb{P}_2 \circ (\pi_* \circ g_{2+})^{-1} = \mathbb{P}_1 \circ (\pi_* \circ g_{1+})^{-1}$, а значит $g_{2*} = \pi_* \circ g_{2+}$ искомое. □

**Лемма Б.0.3.** *Пусть в пространствах корреляции* $\Phi_1$ *и* $\Phi_2$ *разбиения* $f_1 : \Omega_1 \to X$ *и* $f_2 : \Omega_2 \to X$ *таковы, что* $f_1 \precsim f_2$. *Тогда для каждого измельчения* $\rho : Y \to X$ *и каждого разбиения* $g_1 : \Omega_1 \to Y$ *такого, что* $f_1 = \rho \circ g_1$ *существует разбиение* $g_2 : \Omega_2 \to Y$ *такое, что* $f_2 = \rho \circ g_2$ *и* $g_1 \precsim g_2$.

*Доказательство.* Сформулируем требуемое как $\exists g_2 \in \widehat{\Phi}_2(g_1) : f_2 = \rho \circ g_2$ и выразим $\widehat{\Phi}_2$ через структуры разбиений:

$$\widehat{\Phi}_2(g_1) = \bigcap_{\forall Z,\xi:Z\to Y,\mu\in H_{\Phi_1,\xi}(g_1)} H^{-1}_{\Phi_2,\xi}(\mu).$$

По лемме Б.0.1 множество $\widehat{\Phi}_2(g_1)$ является пересечением семейства компактов. Следовательно, для доказательства содержания в нём элемента $g_2 : f_2 = \rho \circ g_2$, достаточно доказать, что такой элемент содержится в пересечении каждого конечного подсемейства тех же компактов:

$$\exists g_{2*} \in \bigcap_{i=1}^{n} H^{-1}_{\Phi_2,\xi_i}(\mu_i) : f_2 = \rho \circ g_{2*},$$

где $\xi_i : Z_i \to Y$ — произвольные измельчения с произвольными доменами $Z_i$ и $\mu_i \in H_{\Phi_1,\xi_i}(g_1)$ также выбраны произвольно.

По определению структуры разбиения $\exists h_{1,i} \models \Phi_1 : g_1 = \xi_i \circ h_{1,i}, \mathbb{P} \circ h_{1,i}^{-1} = \mu_i$. Построим их комбинацию $h_1 = h_{1,1} \diamond ... \diamond h_{1,n}$, где $h_{1,i} = \pi_i \circ h_1$, и обозначим

$\xi = \xi_1 \wr ... \wr \xi_n$. По определению точного отображения $\exists h_2 \models \Phi_2 : f_2 = \rho \circ \xi \circ h_2, \mathbb{P}_1 \circ h_1^{-1} = \mathbb{P}_2 \circ h_2^{-1}$, а значит можно взять $g_{2*} = \xi \circ h_2$. По построению $f_2 = \rho \circ g_{2*}$ и $\mathbb{P}_1 \circ h_{1,i}^{-1} = \mathbb{P}_1 \circ (\pi_i \circ h_1)^{-1} = \mathbb{P}_2 \circ (\pi_i \circ h_2)^{-1} = \mathbb{P}_2 \circ h_{2,i}^{-1}$, следовательно $g_{2*}$ — искомое. □

**Следствие Б.0.1.** *Если пространства корреляции $\Phi_1 \precsim \Phi_2$, то для каждого разбиения $f_1 \models \Phi_1$ существует $f_2 \models \Phi_2$ такое, что $f_1 \precsim f_2$.*

**Следствие Б.0.2.** *Леммы Б.0.2, Б.0.3 и следствие Б.0.1 также верны для строгого отношения $f_1 \prec f_2 \equiv f_1 \precsim f_2 \cap \neg(f_1 \succsim f_2)$.*

**Лемма Б.0.4.** *$f_1 \precsim f_2 \Leftrightarrow f_1 \succsim f_2$ для любых разбиений одного и того же пространства корреляции.*

*Доказательство.* Предположим обратное — существование $f_1 \prec f_2$ с кодоменом $X$. Тривиальное измельчение $\theta(x) = (0, \ldots, 0), \forall x \in X$ очевидно даёт $\theta \circ f_1 = \theta \circ f_2$. Это противоречит $\theta \circ f_1 \prec \theta \circ f_2$, следующему из леммы Б.0.2. □

**Следствие Б.0.3.** *$f_1 \precsim f_2 \Leftrightarrow f_1 \succsim f_2$ для любых разбиений изоморфных пространств корреляции.*

*Доказательство теоремы об изоморфных пространствах.* Рассмотрим в игре $\Gamma|\Phi_1$ произвольный профиль стратегий $\mathbf{s}_1$. Этот профиль, очевидно, является разбиением пространства корреляции $\Phi_1$. По следствию Б.0.1 существует разбиение $\mathbf{s}_2$ пространства корреляции $\Phi_2$ такое, что $\mathbf{s}_1 \precsim \mathbf{s}_2$, причём, аналогично, $\mathbf{s}_2$ является ещё и профилем стратегий в игре $\Gamma|\Phi_2$. Докажем вложения в обоих направлениях: 1. $U^{A_*}_{\Gamma|\Phi_1}(\mathbf{s}_1) \subseteq U^{A_*}_{\Gamma|\Phi_2}(\mathbf{s}_2)$ и 2. $U^{A_*}_{\Gamma|\Phi_1}(\mathbf{s}_1) \supseteq U^{A_*}_{\Gamma|\Phi_2}(\mathbf{s}_2)$ для любой группы игроков $A_*$:

1. Рассмотрим произвольный профиль $\mathbf{s}_{1*} \models \Phi_1$, отличающийся от $\mathbf{s}_1$ стратегиями группы $A_*$. Обозначим $\mathbf{s}_{1+} = \mathbf{s}_1 \diamond \mathbf{s}_{1*}$, где $\mathbf{s}_1 = \pi \circ \mathbf{s}_{1+}$ и $\mathbf{s}_{1*} = \pi_* \circ \mathbf{s}_{1+}$. По определению точного образа $H_{\Phi_1,\pi}(\mathbf{s}_1) \subseteq H_{\Phi_2,\pi}(\mathbf{s}_2)$, т.е. $\exists \mathbf{s}_{2+} \models \Phi_2 : \mathbb{P}_1 \circ \mathbf{s}_{1+} = \mathbb{P}_2 \circ \mathbf{s}_{2+}, \mathbf{s}_2 = \pi \circ \mathbf{s}_{2+}$. По построению $\mathbf{s}_{2*} = \pi_* \circ \mathbf{s}_{2+}$ отличается от $\mathbf{s}_2$ ходами тех же игроков, что отличают $\mathbf{s}_{1*}$ от $\mathbf{s}_1$, и $\mathbb{P}_1 \circ \mathbf{s}_{1*}^{-1} = \mathbb{P}_2 \circ \mathbf{s}_{2*}^{-1}$, а значит аналогичным образом $u^a(\mathbf{s}_{1*}) = u^a(\mathbf{s}_{2*})$. В силу произвольности выбора $\mathbf{s}_{1*}$ это влечёт $U^{A_*}_{\Gamma|\Phi_1}(\mathbf{s}_1) \subseteq U^{A_*}_{\Gamma|\Phi_2}(\mathbf{s}_2)$.
2. Так как $\mathbf{s}_1 \succsim \mathbf{s}_2$ по следствию Б.0.3, рассуждения предыдущего пункта применимы и в обратном направлении.

□

## Приложение B

## Доказательство теоремы о пространствах заговоров одной структуры[1]

Для доказательства теоремы об изоморфизме пространств заговоров так же понадобится несколько лемм.

**Лемма B.0.1.** *Для любого счётного семейства множеств $\mathfrak{F}$ найдётся цепь множеств $\mathfrak{T}$ такая, что* $\sigma(\mathfrak{F}) = \sigma(\mathfrak{T})$.

*Доказательство.* Пусть $\mathfrak{F} = \{F_1, F_2, \ldots\}$. Построим индуктивно последовательность цепей $(\mathfrak{T}_i)$, где каждая следующая цепь включает в себя предыдущую и $\sigma(\mathfrak{T}_i) = \sigma(\{F_1, \ldots, F_i\})$. В качестве базы возьмём $\mathfrak{T}_1 = \{F_1\}$. Шаг индукции: пусть $\mathfrak{T}_{i-1} = \{T_1, \ldots, T_n\}, T_1 \subset \ldots \subset T_n$ и $\sigma(\mathfrak{T}_{i-1}) = \sigma(\{F_1, \ldots, F_{i-1}\})$. Разложим следующий элемент $\mathfrak{F}$ на непересекающиеся дизъюнкты: $F_i = (F_i \cap T_1) \cup (F_i \cap T_2 \setminus T_1) \cup \ldots \cup (F_i \cap T_n \setminus T_{n-1}) \cup (F_i \setminus T_n)$. В этой записи $j$-й дизъюнкт вложен в соответствующую разность $T_j \setminus T_{j-1}$ соседних элементов цепи. Следовательно, для его порождения достаточно пополнить $\mathfrak{T}_{i-1}$ множеством $T_{j-} = F_i \cap T_j \cup T_{j-1}$, сохраняющим структуру цепи, поскольку $T_{j-1} \subseteq T_{j-} \subseteq T_j$. Таким образом, чтобы получить $F_i$ целиком,

$$\mathfrak{T}_i = \mathfrak{T}_{i-1} \cup \left\{ \begin{array}{l} F_i \cap T_1, \\ F_i \cap T_2 \cup T_1, \\ \ldots \\ F_i \cap T_n \cup T_{n-1}, \\ F_i \cup T_n \end{array} \right\}$$

Покажем, что предел последовательности $(\mathfrak{T}_i)$ — искомая цепь. В самом деле, любой элемент из $\sigma(\mathfrak{F})$ — это счётное объединение конечных пересечений множеств $F_i$. Поэтому

$$\sigma(\mathfrak{F}) = \bigcup_{i=1}^{\infty} \sigma(\{F_1, \ldots, F_i\}) = \bigcup_{i=1}^{\infty} \sigma(\mathfrak{T}_i) = \sigma(\mathfrak{T}).$$

□

[1] Цитируется по материалам статьи [8].

**Лемма В.0.2.** *Максимальная цепь измеримых множеств в безатомическом пространстве порождает безатомическую* σ*-алгебру.*

*Доказательство.* Пусть максимальная цепь $\mathfrak{T}$ измеримых множеств безатомического пространства $\langle\Omega,\mathfrak{B},\mathbb{P}\rangle$ порождает алгебру $\sigma(\mathfrak{T})$. Докажем, что для любого $B\in\sigma(\mathfrak{T})$ меры $\mathbb{P}(B)>0$ найдётся $B'\in\sigma(\mathfrak{T})$ такое, что $B'\subset B$ и $\mathbb{P}(B)>\mathbb{P}(B')>0$. Для этого, очевидно, достаточно доказать, что в цепи $\mathfrak{T}$ найдётся множество $T$ такое, что $0<\mathbb{P}(T\cap B)<\mathbb{P}(B)$. Рассмотрим множества

$$\underline{T}=\bigcup_{T_-\in\mathfrak{T}:\mathbb{P}(T_-\cap B)=0}T_-\quad\text{и}\quad\overline{T}=\bigcap_{T_+\in\mathfrak{T}:\mathbb{P}(T_+\cap B)=\mathbb{P}(B)}T_+,$$

по построению вложенные $\underline{T}\subset\overline{T}$ так, что $\mathbb{P}(\overline{T})-\mathbb{P}(\underline{T})\geqslant\mathbb{P}(B)$. Поскольку цепь $\mathfrak{T}$ максимальна в безатомическом пространстве, существует $T_0\in\mathfrak{T}$ такое, что $\underline{T}\subset T_0\subset\overline{T}$. Так как $\underline{T}\subset T_0\Rightarrow\mathbb{P}(T_0\cap B)>0$ и $T_0\subset\overline{T}\Rightarrow\mathbb{P}(T_0\cap B)<\mathbb{P}(B)$, значит $T_0$ искомое. □

**Определение В.0.1.** Для любых семейств измеримых множеств $\mathfrak{T}\subseteq 2^\Omega$ и мер $\mathbb{P}:\mathfrak{T}\to\mathbb{R}_{\geqslant 0}$ определим отображение $\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle:\Omega\to\mathbb{R}_{\geqslant 0}$, называемое наименьшей мерой включения и вычисляемое по формуле $\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle(\omega)=\inf\{\mathbb{P}(T)\mid\omega\in T\in\mathfrak{T}\}$.

**Лемма В.0.3.** *Если* $\mathfrak{T}\subset 2^\Omega$ *— цепь множеств, порождающая безатомическую* σ*-алгебру, то* $\mathbb{P}\circ\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle^{-1}$ *совпадает с мерой Лебега на отрезке* $[0,\mathbb{P}(\Omega)]$.

*Доказательство.* Поскольку $\mathfrak{T}$ — цепь, $\omega\in T\Leftrightarrow\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle(\omega)\leqslant\mathbb{P}(T),\forall\omega\in\Omega,T\in\mathfrak{T}$. Так как $\mathfrak{T}$ вдобавок порождает безатомическую σ-алгебру, то для каждого $0<t<\mathbb{P}(\Omega)$ найдётся $T\in\mathfrak{T}$ такое, что $\mathbb{P}(T)=t$. Следовательно, функция $\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle$ отображает множества $T\in\mathfrak{T}$ на отрезки $[0,\mathbb{P}(T)]$, что очевидно влечёт цель доказательства. □

**Лемма В.0.4.** *Пусть* $\langle\Omega,\mathfrak{B},\mathbb{P}\rangle$ *— любое безатомическое вероятностное пространство с* σ*-алгеброй, разложимой на* $n$ *безатомических компонент* $\mathfrak{B}=\sigma(\mathfrak{B}_1\cup\ldots\cup\mathfrak{B}_n)$ *таких, что все события из разных компонент совместно независимы, т.е.* $\mathbb{P}(B_1\cap\ldots\cap B_n)=\mathbb{P}(B_1)\ldots\mathbb{P}(B_n)$ *для любых* $B_i\in\mathfrak{B}_i,i=\overline{1,n}$. *Тогда любая измеримая функция с конечным кодоменом* $f:\Omega\to X$ *может быть представлена в виде* $f=\varphi\circ\mathfrak{r}$, *где* $\mathfrak{r}:\Omega\to[0,1]^n$ *такова, что* $\mathbb{P}\circ\mathfrak{r}^{-1}$ *совпадает с мерой Лебега, а* $\varphi:[0,1]^n\to X$ *— борелевская.*

*Доказательство.* Рассмотрим обратную функцию $f^{-1} : X \to \mathfrak{B}$. В силу разложимости $\mathfrak{B}$ её можно представить как предел последовательности конъюнкций:

$$f^{-1}(x) = \bigcup_{j=1}^{\infty} F_1^j(x) \cap \ldots \cap F_n^j(x),\ F_i^j : X \to \mathfrak{B}_i.$$

Обозначим семейства множеств $\mathfrak{F}_i = \{F_i^j(x) \mid j \in \mathbb{N}, x \in X\}$ и заметим, что $f$ измерима по $\sigma(\mathfrak{F}_1 \cup \ldots \cup \mathfrak{F}_n)$. По лемме B.0.1, существуют цепи множеств $\mathfrak{T}_i \subset \mathfrak{B}_i$ такие, что $\sigma(\mathfrak{F}_i) = \sigma(\mathfrak{T}_i)$. Согласно принципу максимума Хаусдорфа каждая такая цепь вложена в максимальную цепь $\overline{\mathfrak{T}}_i \subset \mathfrak{B}_i$, порождающую безатомическую $\sigma$-алгебру по лемме B.0.2. Построим искомые функции: $\mathfrak{r} = (\mathrm{mim}\langle\overline{\mathfrak{T}}_1, \mathbb{P}\rangle, \ldots, \mathrm{mim}\langle\overline{\mathfrak{T}}_n, \mathbb{P}\rangle)$ и $\varphi = f \circ \mathfrak{r}^{-1}$. Необходимые свойства соблюдаются по построению. □

*Доказательство теоремы 1.3.1.* Применим лемму B.0.4 к произвольному пространству заговоров $\Phi_1$ структуры $\mathfrak{A} = \{A_1, \ldots, A_n\}$, используя в качестве компонент разложения $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$ $\sigma$-алгебры тайны соответствующих групп заговорщиков. Это даёт для любого разбиения $f_1 \models \Phi_1$ разложение $f_1 = \varphi \circ \mathfrak{r}$. В любом другом пространстве заговоров $\Phi_2$ той же структуры $\mathfrak{A}$ соответствующее разбиение $f_2 \models \Phi_2$ построим похожим образом: $f_2 = \varphi \circ \mathfrak{u}$. Здесь $\varphi$ то же самое, а $\mathfrak{u} = (\mathrm{mim}\langle\mathfrak{W}_1, \mathbb{P}_2\rangle, \ldots, \mathrm{mim}\langle\mathfrak{W}_n, \mathbb{P}_2\rangle)$, где $\mathfrak{W}_i$ - произвольные максимальные цепи, вложенные в $\sigma$-алгебры соответствующих тайн пространства заговоров $\Phi_2$. Поскольку и $\mathbb{P}_1 \circ \mathfrak{r}^{-1}$, и $\mathbb{P}_2 \circ \mathfrak{u}^{-1}$ обе совпадают с мерой Лебега, то и $\mathbb{P}_1 \circ f_1^{-1} = \mathbb{P}_2 \circ f_2^{-1}$, а значит теорема доказана. □

# Приложение Г

# Карточная игра «Тессеракт»

## Г.1 Правила[1]

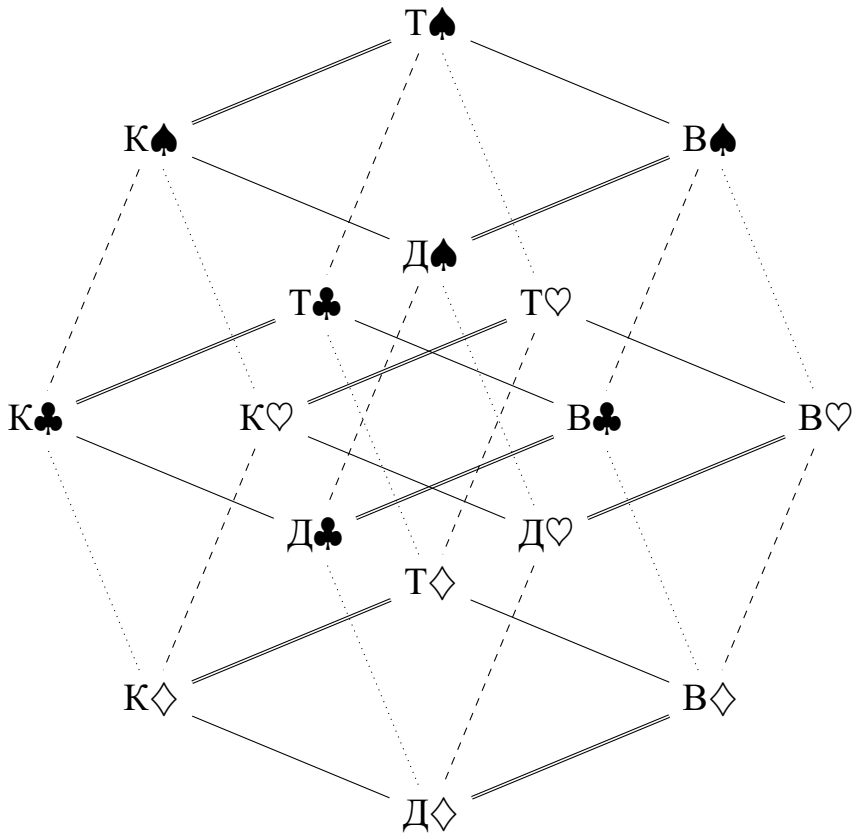


Рисунок Г.1 — Тессеракт парных карт

Для игры в тессеракт необходимы:

– 4 игрока;
– преферансная колода (4 масти с достоинствами от семёрки до туза, всего 32 карты);
– фишки или иной способ подсчёта очков;
– игрокам, только знакомящимся с игрой, поначалу может быть полезна распечатка диаграммы на рис. Г.1.

[1]Раздел уточняет и дополняет материалы статьи [9].

Игра состоит из любого (заранее обговорённого и/или по достижении лимита выигрышей/проигрышей) числа независимых раздач. Результатом одной раздачи может стать перераспределение между игроками (с нулевой суммой) некоторого количества фиксированных ставок. Ни один игрок не может проиграть или выиграть более 3 ставок за раздачу.

Раздача начинается с деления колоды на старшие (В, Д, К, Т) и младшие (7, 8, 9, 10) карты.[2] Старшая колода перемешивается и сдаётся игрокам в открытую (лицом вверх), по 4 карты каждому. Младшая колода раздаётся без перемешивания (тут масти и достоинства не имеют значения), также по 4 карты на игрока. После того как все увидели расклад, каждый игрок подбирает сданные ему старшие и младшие карты, объединяя их в закрытой руке. После этого начинается розыгрыш, состоящий из четырёх кругов.

В течение каждого круга ходов игроки должны в произвольном порядке совершить по два действия: а) сыграть одну карту перед собой рубашкой вверх и б) сбросить одну карту в общую стопку сброса рубашкой вверх. После того как все закончат, сыгранные (но не сброшенные) карты раскрываются. По завершении всех четырёх кругов у игроков не остаётся карт в руках, перед каждым лежат лицом вверх по 4 сыгранные карты, и подводится итог розыгрыша. Каждый игрок должен сосчитать вскрытые непарные карты и, соответственно, свой штраф.

С точки зрения каждого игрока 16 старших карт по своему разбиваются на 8 пар. Способ разбиения определяется в зависимости от его порядкового номера за столом:

1. парны валеты и дамы одной масти, парны короли и тузы одной масти;
2. парны трефы и пики одного достоинства, парны червы и бубны одного достоинства;
3. парны пики и червы одного достоинства, парны бубны и трефы одного достоинства;
4. парны валеты и тузы одной масти, парны дамы и короли одной масти.

[2]Можно перемешивать и раздавать колоду целиком, не разделяя, по 8 карт каждому лицом вверх, однако в таком случае будут нередко случаться расклады, существенно благоволящие одним игрокам в ущерб другим. Например, если кому-либо будет сдана рука из одних только младших карт, то он фактически превратится в болванчика, не имеющего возможности влиять на исход игры вообще. Игрок с одной старшей картой в руке, хотя и будет иметь возможность один раз за розыгрыш повлиять на игровую ситуацию, не сможет совершать тайных от других игроков осмысленных ходов, что сделает его стратегию более предсказуемой, и т.д.. Впрочем, если участники готовы мириться с усилением элемента случайности в игре, то подобный «ленивый» способ раздачи использовать не возбраняется.

На рис. Г.1 парность карт для разных игроков обозначена линиями различной штриховки. При этом легко заметить, что 16-ти старшим картам можно поставить в соответствие вершины четырёх-мерного гиперкуба (отсюда название «Тессеракт») таким образом, что для каждого игрока отношение парности соответствует своему набору параллельных рёбер.

В контексте подсчёта штрафов непарной картой для игрока считается вскрытая старшая карта, не образующая по его правилам пары с другими вскрытыми картами. Штраф игрока считается по формуле $|2l - 8|$, где $l$ — количество непарных с его точки зрения карт. Желающему избежать штрафа игроку следует ходить таким образом, чтобы к концу розыгрыша было сыграно ровно $4$ непарные для него карты, так как каждая карта отклонения в большую или меньшую сторону увеличивает его штраф на $2$. Средний штраф определяется как среднее арифметическое штрафов всех игроков. При окончательном расчёте игроки, чей штраф больше среднего, вносят в банк фишки кол-ом равным разнице между своим штрафом и средним. Те же игроки, чей штраф меньше среднего, наоборот, забирают из банка разницу между средним и своим штрафами.

## Г.2 Пример расклада[3]

Поскольку младшие карты не используются при подсчёте штрафов, начальная раздача определяется раскладом старших карт (таблица 2). Дальнейший процесс разыгрывания можно записывать так, как это демонстрируется в таблице 3.

Таблица 2 — Расклад A

| Игрок | Рука | | | |
|---|---|---|---|---|
| 1 | В♢ | Д♣ | К♣ | Т♣ |
| 2 | К♠ | К♡ | К♢ | В♣ |
| 3 | Д♠ | В♡ | Д♡ | Д♢ |
| 4 | В♠ | Т♠ | Т♡ | Т♢ |

[3] Раздел уточняет и дополняет материалы статьи [9].

Таблица 3 — Розыгрыш A1 расклада A

| Игрок | Круги ходов | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | | 2 | | 3 | | 4 | |
| 1 | Д♣ | Т♣ | | | | К♣ | | В♢ |
| 2 | К♠ | | | В♣ | | К♡ | К♢ | |
| 3 | В♡ | | Д♢ | | | Д♡ | Д♠ | |
| 4 | Т♡ | | Т♢ | | Т♠ | | | В♠ |

Здесь, опять же, младшие карты не показаны в силу их неразличимости с точки зрения правил, на белом фоне показаны сыгранные старшие карты, а на сером — сброшенные. Например, первый игрок на первом круге сыграл даму треф и сбросил туза треф, на втором круге сыграл и сбросил по младшей карте и т.д.. Посчитаем непарные карты с точки зрения каждого из игроков, записывая в скобках соответствующую сброшенную парную карту:

1. Д♣ (В♣), В♡ (Д♡), Т♡ (К♡), Д♢ (В♢), Д♠ (В♠)
2. К♠ (К♣), В♡ (В♢), Д♢ (Д♡), Т♠ (Т♣), К♢ (К♡)
3. К♠ (К♡), В♡ (В♠), Т♢ (Т♣), К♢ (К♣), Д♠ (Д♡)
4. Д♣ (К♣), Т♢ (В♢), Т♠ (В♠)

У первого игрока из 9 вскрытых карт 4 образуют пары: К♢-Т♢ и К♠-Т♠. Остаются 5 непарных карт, что соответствует $|2 \cdot 5 - 8| = 2$ очкам штрафа. Повторив ту же процедуру для остальных игроков, можно дополнить таблицу столбцом штрафов.

Таблица 4 — Штрафы розыгрыша A1

| Игрок | Круги ходов | | | | | | | | Штраф |
|---|---|---|---|---|---|---|---|---|---|
| | 1 | | 2 | | 3 | | 4 | | |
| 1 | Д♣ | Т♣ | | | | К♣ | | В♢ | 2 |
| 2 | К♠ | | | В♣ | | К♡ | К♢ | | 2 |
| 3 | В♡ | | Д♢ | | | Д♡ | Д♠ | | 2 |
| 4 | Т♡ | | Т♢ | | Т♠ | | | В♠ | 2 |

Штрафы всех игроков равны, а значит никто никому не платит.

### Г.3 Возможные исходы и простейшие стратегии

Интересно то, что в любой момент игры штрафы каждых двух участников либо равны, либо различаются на 4. Это несложным образом подтверждается перебором $2^{16}$ всевозможных исходов розыгрыша, что с точки зрения выплат оставляет всего 4 различимых класса ситуаций:

1. штрафы всех игроков равны, выплат нет;
2. штраф одного из игроков на 4 больше, чем у остальных троих, он платит каждому из них по 1 фишке;
3. штрафы двух пар игроков различаются на 4, каждый из проигравших платит по 1 фишке каждому из победителей;
4. штраф одного из игроков на 4 меньше, чем у остальных троих, они платят ему по 1 фишке каждый.

Поскольку каждый раз, когда играется старшая карта, соперники раскрывшего её игрока уменьшают меру своего незнания относительно оставшегося содержимого его руки, то тактически разумнее играть старшие карты после младших. Кроме того, легко убедиться, что для получения в качестве исхода розыгрыша представителя любого из вышеперечисленных классов достаточно не более 4 сыгранных всеми игроками карт. Таким образом, следующую стратегию в «Тессеракте» можно назвать базовой — на протяжении первых трёх ходов играются только младшие карты, а единственная старшая играется на последнем круге. Даже если за столом сидят только новички, ограничивающиеся базовыми стратегиями, то их розыгрыш может закончится исходом, принадлежащим к любому из вышеперечисленных классов.

По сути в рамках базовых стратегий в качестве модели «Тессеракта» может выступать игра в нормальной форме — если каждый участник знает, что остальные не будут играть старшие карты до последнего круга, то происходящее превращается в классическую матричную игру размером $5 \times 5 \times 5 \times 5$. Может возникнуть искушение подвергнуть «Тессеракт» в базовых стратегиях анализу на обычные равновесия по Нэшу, однако при этом мы сразу оказываемся в тупике — у типичного расклада оказывается слишком много решений даже в чистых стратегиях. К примеру, расклад из таблицы 2 имеет 21 равновесие по Нэшу, причём каждая стратегия каждого игрока участвует хотя бы в одном из них.

Таблица 5 — Равновесия по Нэшу в базовых стратегиях расклада А

| $s^1$ $u^1(s)$ | $s^2$ $u^2(s)$ | $s^3$ $u^3(s)$ | $s^4$ $u^4(s)$ |
|---|---|---|---|
| ∅ 0 | ∅ 0 | ∅ 0 | ∅ 0 |
| ∅ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |
| Д♣ -1 | К♠ -1 | Д♠ 3 | В♠ -1 |
| Д♣ -1 | К♠ -1 | Д♠ 3 | Т♠ -1 |
| Д♣ -2 | К♢ -2 | Д♠ 2 | Т♢ 2 |
| Д♣ -2 | К♡ -2 | Д♠ 2 | Т♡ 2 |
| Д♣ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |
| В♢ -2 | К♠ -2 | В♡ 2 | Т♠ 2 |
| Т♣ 2 | В♣ -2 | ∅ 2 | Т♠ -2 |
| Т♣ 2 | В♣ 2 | ∅ -2 | Т♢ -2 |
| Т♣ 2 | В♣ -2 | Д♢ 2 | Т♠ -2 |

| $s^1$ $u^1(s)$ | $s^2$ $u^2(s)$ | $s^3$ $u^3(s)$ | $s^4$ $u^4(s)$ |
|---|---|---|---|
| Т♣ 2 | В♣ -2 | Д♡ 2 | Т♠ -2 |
| Т♣ 2 | В♣ 2 | Д♡ -2 | Т♢ -2 |
| Т♣ -1 | К♠ -1 | Д♠ 3 | Т♠ -1 |
| Т♣ -1 | К♢ 3 | Д♢ -1 | Т♢ -1 |
| Т♣ 2 | К♡ -2 | Д♡ 2 | Т♠ -2 |
| Т♣ 2 | К♡ 2 | Д♡ -2 | Т♢ -2 |
| Т♣ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |
| К♣ -2 | К♢ 2 | Д♠ -2 | В♠ 2 |
| К♣ -1 | К♢ 3 | Д♢ -1 | Т♢ -1 |
| К♣ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |

На практике, очевидно, такое многообразие решений немногим лучше их полного отсутствия — результат не применим даже в качестве перечисления возможных соглашений, поскольку это требовало бы общего для всех 4 игроков знания о том, какое соглашение применяется для каждого из $\sim$ 63 миллионов возможных раскладов. Если отвергнуть идею о рациональных агентах с синхронизированной памятью на десятки миллионов ячеек как явно искусственную, получается, что даже в базовых стратегиях «Тессеракт» подразумевает использование игроками эвристик, параметризующихся не только платёжной матрицей расклада. То есть, исходя из наличия у игроков некоего внутреннего состояния, влияющего на выбор стратегии в соответствии с неким алгоритмом, мы неизбежно оказываемся в схеме с рисунка 3.1, что позволяет надеяться на применимость «Тессеракта» в исследованиях феномена «сыгранности».

M.V.Lomonosov Moscow State University

Printed as manuscript

Savchenko Maksim Alekseevich

# Influence of Additional Information Asymmetry on the Solutions of Non-Antagonistic Games

1.2.3. Theoretical Informatics and Cybernetics

Dissertation in support for Candidate of Physical and Mathematical Sciences degree

Translation from Russian

Research supervisor:
Doctor of Physical and Mathematical Sciences, Professor
Alexander Vasin

Moscow — 2022

## Contents

Стр.

Стр.

## Introduction

In game theory, modeling of conflicts with three or more parties independently pursuing own goals is, for many reasons, considered much more difficult comparing to modeling of classical bilateral confrontations. Among these reasons one plays very special part — the influence of information asymmetry exerted on course of a struggle. For games with two participants its effect generally comes down to the consequences of a priori incompleteness in their knowledge about the parameters of the conflict and is usually described with Bayesian models. Common knowledge in such cases leaves out players' payoff functions, so each of them acts according to their own, possibly different assumptions, expressed in the form of a probability distribution in the space of all payoff functions with a given set of strategies.

For multistage bilateral conflicts there can be another source of information asymmetry — the presence of a secret component in the actions of opponents. If this occurs, actions already performed by the player in the early stages may be completely or partially unknown to his opponent, who is forced to base the strategy of later stages on assumptions. Naturally, this is formalized through partitioning of the extensive-form game tree into information sets. Effectively, this two aspects exhaust the impact of information asymmetry on two-sided conflicts. However, addition of third participant induces a new phenomenon, noticed by Robert Aumann in his article [1] introducing now-familiar new formalism — correlated extension of normal form games.

This phenomenon reflects on comparison of the sets of Nash equilibria for the same games, calculated using mixed strategies on one level and involving external correlation mechanisms on the other. In case of two players, all vectors of expected utility in the correlated equilibria belong to the convex hull of the set of mixed equilibria utilities, i.e., correlation mechanisms can be thought of simply as a way to obtain linear combinations of classical solutions. With the advent of the third player, the picture changes — in some games, the presence of a non-public correlation mechanism allows reaching Nash equilibrium points with payoffs outside the convex hull of mixed solutions' utilities. Effectively, it means that asymmetry of knowledge can have a significant impact on the outcome of a multilateral conflict even in cases when its subject have no relation to the payout structure. Let's call the games prone to this effect *sensitive to additional information asymmetry*.

While the described phenomenon has been known for a while, most of the models built by researchers bypassed it, as it is considered rather feature of curiosity in some games of many players. An important exception worth noting is, perhaps, the most significant area of game theory actively using the correlated extension formalism of games in normal form — «mechanism design» [2] by Leonid Gurvitch, Eric Maskin, and Roger Myerson. Their approach aims to create economic instruments that incentivize selfish rational agents to behave optimally in alignment with common goal functions that formalize various social goods. Being an extremely fruitful area of research, mechanism design has spawned many directions and branches, united nevertheless by a number of integral common features arising from the information structure of games for which its main provisions are proved. A typical interaction scheme looks like this: players-agents, knowing their own preferences and capabilities, but being ignorant of these parameters for other participants, report their type to the central authority, which coins a set of correlated strategies based on this information. Next, the center actualizes it for an instance in the form of a pure strategies set and instructs each of the agents, who, in turn, make the final decision on a particular action. This implies that agents can lie at the first stage and disobey at the last. In paradigm of mechanism design the main goal is about the creation of such algorithms for the behavior of central authority that the strategies of truthfulness and obedience form a Nash equilibrium for agents.

Without diving into details, it can be said that mechanism design is based on a special case of information asymmetry — a kind of star connection structure, where a dedicated central agent controls the single correlation mechanism in his own interests, while subordinate agents are in complete isolation both from each other, and from the outside world. The name here accurately reflects the view of conflicts inherent for the model — through its lens, the players are seen as interchangeable parts of a single man-made mechanism, not connected by anything other than participation in it. Although modeling within the framework of this simplification can be useful in construction of formalized methods for conflict resolution, it doesn't cover cases where they are significantly affected by information asymmetries developing not as a result of calculated design, but naturally, as spontaneous interaction occurs between agents in an uncontrolled, external to the model environment. For example, it is difficult to overestimate the significance of corruption's influence on political and economic institutions, and yet it is made up of precisely such unplanned information links external to the institutions themselves.

For the reason described above, the study of the influence of additional information asymmetry on the solutions of multilateral games shouldn't be reduced to purely constructive models. Alas, outside of mechanism design disregard for this phenomenon became prevailing convention. For example, in the article [3] by Drew Fudenberg and Eric Maskin, you can find the following footnote: «In essence, if $n \geqslant 3$, the rest of the players get the opportunity to omit player $j$ payouts even lower, using a correlated strategy against him, in which player $j$ cannot observe the signal of the correlation mechanism (...). Adhering to the tradition that has developed in publications devoted to repetitive games, however, we will not consider such correlated strategies.» It would seem, however, that in the context of repeated games with discounting, the topic of using the secrecy of the correlation mechanism to strengthen punishment strategies is rather intriguing — examples of agent groups strengthening their collective long-term position through necessarily secret coordination of actions seemingly isn't hard to find in every field of research that uses the folk theorem, from anthropology to international politics. Disconcertingly, up to date game theory has very little to offer as an analysis tool for the described phenomenon to other sciences.

This study is **aim**ed toward development of new multilateral conflict model, that takes into account how its course is affected by additional informational asymmetry.

To approach stated goal following **tasks** had to be addressed:

1. Analyze the correlated extension of normal form games model in scope of the research.
2. Develop the notation aimed to describe the informational structures, that could be tying together participants of the arbitrary conflicts in a variety of fashions.
3. Analyze the impact of additional informational asymmetry on the solutions' conformity with the criteria of collective rationality.
4. Develop the reasonable solution concept for the games with additional informational asymmetry, taking into account the inter-agent relations.

**Scientific novelty:**

1. The games of many players, which are sensitive to additional information asymmetry, are singled out as an independent object of study.
2. A formalism of the conspiracy space is proposed, purposefully narrowing the formalism of the correlation space in order to model additional information asymmetry.

3. The concept of structurally consistent equilibrium is formulated, in many cases allowing to single out among the solutions of games in conspiracy spaces those that adhere to the principle of collective rationality.
4. The possibility of extending the set of perfect subgame equilibria in repeated games sensitive to additional information asymmetry with the help of modern cryptography tools is demonstrated.

The **practical significance** of the work stems from the obvious need to take into account, when modeling multilateral conflicts, the fact that the composition of their participants is not, in most cases, a random sample of agents that are not related to each other in any way. The classical formalism of games in normal form relies on the implicit assumption that the only significant characteristic of each player is the order of preference regarding the outcome of the draw, expressed in the form of a payoff function. At the same time, it is quite obvious that real people entering into a confrontation are often connected by relationships, significant for its outcome, the structure of which cannot be expressed by a simple combination of payment functions. Such connection can be clearly illustrated by comparing two imaginary games of bridge or preference with equally strong players, differing in that one table is occupied by strangers, while at the other some have been playing together for many years. Any sufficiently experienced card-player can confirm that, given equal skill, the «cohesion» factor between partners reliably provides a decisive advantage. Naturally, this phenomenon can be generalized to more significant conflicts: politics, business, diplomacy — wherever the outcome of the confrontation depends significantly on the coordination and unpredictability of actions, mutual understanding that does not require communication can often turn defeat into victory. Thus, to improve accuracy of predictions for the outcomes of multilateral conflicts, there is a compelling need for models that take this factor into account.

**Methodology and research methods.** The study utilizes frameworks of game theory, probability theory, topology and cryptography.

**Defense positions:**

1. Proof of the theorem on the isomorphism of correlation spaces, which defines equivalence classes for them, demarcating indistinguishable from the game-theoretic point of view spaces.
2. A proof of the theorem on conspiracy spaces of one structure, thanks to which the structure of a space describes it comprehensively.

3. Proof of sensitivity to additional information asymmetry of the symmetric task scheduling problem with nonmonotonic returns.
4. A solution to a three-way symmetric scheduling problem with a nonmonotonic rush premium function in an asymmetric conspiracy space that satisfies the structural consistency criterion.
5. A model of repeated games, that takes into account the cost of calculations required to choose a move at the each iteration.
6. Cryptographic punishment strategies for repeated three-player even-odd, widening the set of perfect subgame equilibria with points achievable only by taking into account the complexity of the algorithms.

**Work approbation.** The main results of the work were reported on: Lomonosov readings (2017, 2021) [4; 5], IX Moscow International Conference on Operations Research [6] and Conference for Young Scientists in Mathematical Economics and Economic Theory (MEET-2021) [7].

**Personal contribution.** The author independently obtained the results featured in the dissertation work in the form of theorems and other provisions submitted for defense. The obtained results were prepared for publication without co-authors.

**Publications.** The main results on the topic of the dissertation are presented in 7 published papers, 3 of which [8][9][10] were published in a periodical scientific journal recommended by the HAC and indexed by Web of Science and Scopus. The central work has an English translation[11]. 3 papers were published in conference abstracts.

**Volume and structure of work.** The dissertation consists of introduction, 3 chapters, conclusion and 4 appendices. The full volume of the dissertation is 86 pages, including 2 figures and 5 tables. The list of references contains 26 titles.

# Chapter 1. Conspiracy model

## 1.1 Correlated extension of normal-form game[1]

In the established scientific tradition additional information asymmetry is usualy described by formalism of the correlated extension of the normal-form games proposed by Robert Aumann in [1]. For convenience, its central elements will be presented here in a notation adapted to the Russian-speaking community. Consider the normal-form game $\Gamma = \langle A, S^a, u^a(s), a \in A \rangle$. The finite set of players from this point onward is denoted as $A = \{1, \ldots, m\}$, while the finite set of pure strategy profiles is denoted as $S = S^1 \times \ldots \times S^m$. In addition to the set of strategies $S^a$, each player is defined by the payoff function $u^a : S \to \mathbb{R}$.

Consider also a probability space [12] $\langle \Omega, \mathfrak{B}, \mathbb{P} \rangle$ in which the state of nature observed by the players is realized. Here $\Omega$ is the set of such states, $\mathfrak{B}$ is a σ-algebra of subsets of $\Omega$, and $\mathbb{P} : \mathfrak{B} \to \mathbb{R}_{\geqslant 0}$ is a probability measure. To each player $a \in A$, we assign *their own subspace* $\langle \Omega, \mathfrak{I}^a, \mathbb{P} \rangle$ such that $\mathfrak{I}^a \subseteq \mathfrak{B}$. The tuple of σ-algebras $\mathfrak{I} = (\mathfrak{I}^a, a \in A)$ reflects the players' awareness about the state of nature. In the situation described, the state of nature does not affect the payoff functions directly and serves solely as a means to synchronize the players' actions. This means that the σ-algebra $\mathfrak{B}$ itself is not a significant parameter of the model, and the measurability with respect to this algebra for $\mathbb{P}$ can be replaced by the measurability with respect to $\mathfrak{I}^a, \forall a \in A$.

Separately, it is worth noting that for the players' own subspaces the Aumannian formalism historically assumed the individuality of not only σ-algebras, but also their corresponding measures, thereby taking into account the possible subjectivity of estimates regarding the probability of certain events, which is important in cases where processes too complex for objective analysis (for example, sports competitions) act as a correlation mechanism. However, for the purposes of present study, this aspect does not make much sense, since the conspiracy model implies that conspirators can arbitrarily choose the mechanism of correlation, and in such situation, it is reasonable to expect that people will use simple sources of randomness with a known distribution (roulettes, dices, lots, etc.). For this reason, hereinafter, the model of correlated strategies is utilized

[1] The section refines and elaborates the materials of the [11] article.

in its simplified form, with an objective probability measure in the space of states of nature shared by all players.

Thus, we obtain the parameter tuple $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$ characterizing some correlation space for an arbitrary game with the set A of players. Note that one and the same *correlation space* can be used in games with one set of players but with different sets of pure strategies and payoff functions. However, a *correlated game extension* is completely determined by the pair $\Gamma|\Phi$. Let us describe the resulting new game in terms of normal form[2]:

$$\Gamma|\Phi = \langle A, \mathbf{S}^a, u^a(\mathbf{s}), a \in A \rangle.$$

Here the set $\mathbf{S}^a$ of correlated strategies available to a player $a$ consists of all $\mathfrak{I}^a$-measurable functions $\mathbf{s}^a : \Omega \to S^a$ mapping the set of possible states of nature onto the set of pure strategies available to this player. Accordingly, the payoff function is calculated by the formula for the expectation of a random variable,

$$u^a(\mathbf{s}) = \sum_{s \in S} \mathbb{P}(\mathbf{s}^{-1}(s)) u^a(s),\ \mathbf{s}^{-1}(s) = \{\omega \in \Omega \mid \mathbf{s}^a(\omega) = s^a, \forall a \in A\},$$

where the $\mathbb{P}(\mathbf{s}^{-1}(s))$ serve as the coefficients of the distribution on the game matrix.

In his article, Aumann demonstrates by examples how games can obtain new Nash equilibrium points using the power of the introduced formalism. Depending on the parameters of the correlation spaces, one can construct not only solutions with any payoffs from the convex hull of the payoff vectors at the points of the classical mixed Nash equilibrium, but for some games even solutions that lie outside such a convex hull. This allows us to formulate the key concept of this work:

**Definition 1.1.1.** Let $\Gamma$ be a game in normal form with $m$ players, and $U \subseteq \mathbb{R}^m$ be the set of all payoff vectors achievable in its mixed Nash equilibria. A game $\Gamma$ is said to be *sensitive to additional information asymmetry* when there exists a correlation space $\Phi$ such that for the game $\Gamma|\Phi$ there is a correlated Nash equilibrium with a payoff vector not belonging to the convex hull of the set $U$.

Additionally, in the same article it is proved that the presence of a public real-valued roulette in the correlation space, i.e. subspaces of events with a uniformly distributed real outcome in the range $[0, 1)$, implies the convexity of both the set of

[2]Following the notation introduced in [1], the sets of strategies and outcome sets of a correlated extension of the game are denoted in bold ($\mathbf{s}$ and $\mathbf{S}$ where the underlying game has $s$ and $S$).

attainable payoffs and the set of Nash equilibria in any game. Regarding the correlated expansion of normal form games, the above is quite enough to understand the ideas of this work, however the current state of knowledge on this topic can be traced in greater detail through the publications mentioned in Appendix A.

## 1.2 Isomorphism of correlation spaces[3]

It should be noted that the model of correlation spaces is, in a sense, essentially redundant, because events from the state of nature as such do not matter and are used only as signals for synchronizing strategies. Talking about the impact of additional information asymmetry on the outcomes of conflicts in a meaningful way inevitably requires the ability to abstract from its specific sources, focusing on structural differences in the awareness of opponents. If formally different correlation spaces turn out to be completely interchangeable from a game-theoretic point of view, then they should be assigned to the shared equivalence class, whose description is the effectively essential parameter of the model. We note right away that this applies not only to trivial replacements of the set of states of nature by another set of the same size with the corresponding bijection of the rest of the space parameters, but also to more complex cases. For example, if in the context of a certain game a group of players observes a common signal in the form of a real-valued roulette wheel, will their observation of a coin toss also matter? Common sense dictates that any general roulette-and-coin strategy can easily be converted into a roulette-only equivalent by dividing the wheel in half and mapping the individual options for heads and tails into the resulting two sectors. We describe this phenomenon in the form of an isomorphism:

**Definition 1.2.1.** A *partition* of a correlation space $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$ *into an arbitrary finite set of outcomes (codomain)* $X = X^1 \times ... \times X^m$ is a mapping $f : \Omega \to X$ consisting of the tuple of functions $(f^1, ..., f^m)$, where each $f^a : \Omega \to X^a$ is measurable with respect to $\mathfrak{I}^a$. In the sequel, a "partition $f$ of a correlation space $\Phi$" will be written in abbreviated form as $f \models \Phi$.

In the context of correlated extension, the sets of outcomes $X^a$ are associated with the sets of pure strategies $S^a$, and the elements of the partition $f^a$ are associated with

[3] The section refines and elaborates the materials of the [11] article.

the correlated strategies $\mathbf{s}^a$. In what follows, we also use the mappings $f^{-1} : X \to 2^\Omega$ inverse to the partitions of correlation spaces,

$$f^{-1}(x) = \bigcap_{a \in A} (f^a)^{-1}(x^a).$$

**Definition 1.2.2.** A space $\Phi_1$ with a measure $\mathbb{P}_1$ is said to be *mappable onto* $\Phi_2$ *with a measure* $\mathbb{P}_2$ (in the sequel, $\Phi_1 \precsim \Phi_2$) if their sets of players coincide and for each partition $f_1 \models \Phi_1$ there existsa partition $f_2 \models \Phi_2$ with the same codomain such that $\mathbb{P}_1 \circ f_1^{-1} = \mathbb{P}_2 \circ f_2^{-1}$. Mutually mappable correlation spaces are said to be *isomorphic* (in the sequel, $\Phi_1 \sim \Phi_2$).

This definition is easy to illustrate by the aforementioned example: for each partition $f_1 : [0,1) \times \{0,1\} \to X$ of the space consisting of a real roulette and a symmetric coin, one can construct the corresponding image $f_2 : [0,1) \to X$ in the space of a roulette alone,

$$f_2(\alpha) = \begin{cases} f_1(2\alpha, 0), & 0 \leqslant \alpha < \frac{1}{2} \\ f_1(2\alpha - 1, 1), & \frac{1}{2} \leqslant \alpha < 1 \end{cases}.$$

The reflexivity, symmetry, and transitivity of the isomorphism introduced using this definition are obvious, which means that this is indeed an equivalence relation on the set of correlation spaces. Moreover, although the definition of isomorphism was given in isolation from the correlated extension of games, the following theorem can be stated.

**Definition 1.2.3.** For a game $\Gamma = \langle A, S^a, u^a(s), a \in A \rangle$, the set of achievable payoffs based on the deviations of a cabal $A_*$ of players from a profile $s$ of strategies is defined as

$$U_\Gamma^{A_*}(s) = \{\bar{u} \mid \exists s_* \in S : u(s_*) = \bar{u}, \forall a \in A \setminus A_*, s^a = s_*^a\}.$$

**Theorem 1.2.1** (on isomorphic spaces)**.** *Let* $\Phi_1 \sim \Phi_2$. *Then for each normal-form game* $\Gamma$ *with finite sets of players' strategies, its correlated extensions* $\Gamma|\Phi_1$ *and* $\Gamma|\Phi_2$ *possess the following property. Let* $\mathbf{s}_1$ *be some profile of strategies of the game* $\Gamma|\Phi_1$. *Then there exists a profile* $\mathbf{s}_2$ *of strategies of the game* $\Gamma|\Phi_2$ *such that* $U_{\Gamma|\Phi_1}^{A_*}(\mathbf{s}_1) = U_{\Gamma|\Phi_2}^{A_*}(\mathbf{s}_2)$ *for each cabal* $A_*$ *of players.*

This theorem permits one to deem isomorphic correlation spaces indistinguishable in the context of searching of equilibria stable under both individual and group deviations. The proof, which is an exercise in topology without close connection to the central ideas of the study, is in Appendix Б.

## 1.3 Conspiracy spaces[4]

Now, having obtained a meaningful isomorphism for correlation spaces, from all possible equivalence classes we can isolate those that are of interest with regard to modeling additional information asymmetry. As Aumann showed, going beyond the convex hull of the set of solutions in mixed strategies is possible if some of the players (at least two) use a correlated strategy that depends on an event about which at least one of the other players is not informed. It is natural to call such a form of mutually beneficial secret coordination of actions *conspiracy*, and the signal used for synchronization — *secret*. Let there be a secret in the correlation space $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$, i.e. probability subspace $\langle \Omega, \mathfrak{S}, \mathbb{P} \rangle$. The desired information asymmetry suggests that some players observe events from $\mathfrak{S}$ (or others that correlate with them), and some — do not. Although theoretically one can imagine a conspiracy, the degree of involvement in which varies from player to player (someone can observe the events from $\mathfrak{S}$ partially or indirectly, through the observation of other events correlated with them), it makes sense to first consider the simplest case — dividing all players into «conspirators» $A_{\mathfrak{S}} \subseteq A$, who observe $\mathfrak{S}$ as a whole, and «outsiders» $A \setminus A_{\mathfrak{S}}$, in whose field of view only events, not correlated with $\mathfrak{S}$ elements.

The next logical question is about the structure of the secret itself. It is quite possible to imagine how the conspirators use various sources of randomness in its role: dice throws, card deck shuffling, lottery draws, etc., so it is not obvious at first glance, if we can confine ourselves to consideration of single natural in the occurring context mechanism. A positive answer can be obtained using the correlation space mappings introduced above. If we compare all possible spaces that differ only in the secrets of the cabal $A_* \subseteq A$, the relation $\precsim$ induces a partial order on their set. The lower bound of this order will be a degenerate correlation space in which the conspiracy secret consists of a single atomic event with probability $1$ — such a space is mappable to any other and, obviously, cannot be used at all for strategy correlation. The upper bound's samples are more interesting — quintessentially, their conspiracy secrets are an arbitrary atomless [13, c. 81] spaces. Such a correlation mechanism can be easily imagined as a real-value roulette whose rotation generates a uniformly distributed random variable in unit half-interval $[0, 1)$. By dividing it into sectors of the required sizes, the conspirators observing the roulette can agree on any profile of correlated strategies in games with a finite set

[4] The section refines and elaborates the materials of the [11] article.

of outcomes. Such a universal source of randomness provides maximum freedom of choice, thus making sense as first consideration.

Finally, one should think about correlation spaces with multiple secrets. In fact, nothing prevents players from observing several roulettes at once, choosing the opponents to correlate their strategy with depending on the situation. Moreover, a player's strategy can be tangibly dependent on more than one secret at the same time. Thus, correlation spaces consisting of distinct independent real-value roulettes, each characterized by a subset of players who can observe it, can be considered a natural subject of consideration. It remains to note that if there is two or more real-value roulettes belonging to the same circle of conspirators in the same correlation space, all but one can be discarded without damage to the model, since such duplication is obviously useless in games with finite sets of outcomes. Let us now turn to a more formal definition of the proposed concept. To do this, consider an arbitrary correlation space $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A\rangle$. In this space, for each non-empty group of players $A_* \subseteq A$, we define the following family of events[5]:

$$\mathfrak{S}_\Phi^{A_*} = \{U \in \bigcap_{a\in A_*} \mathfrak{I}^a \mid \mathbb{P}(U \cap V) = \mathbb{P}(U)\mathbb{P}(V), \forall V \in \sigma(\bigcup_{a\in A\setminus A_*} \mathfrak{I}^a)\}.$$

Thus, $\mathfrak{S}_\Phi^{A_*}$ is the set of all events such that all members of $A_*$ are aware of them, and each event is pairwise independent of all events known to nonmembers of $A_*$ even with their knowledge combined. Since an intersection of σ-algebras is a σ-algebra and the subset of events in a σ-algebra independent of a given event is again a σ-algebra, it follows that $\mathfrak{S}_\Phi^{A_*}$ is a σ-algebra. This allows one to speak of the probability subspace $\langle \Omega, \mathfrak{S}_\Phi^{A_*}, \mathbb{P}\rangle$, which can be logically called a secret of the cabal $A_*$. We single out two cases: we say that secrets with atomless measures are *complete* and secrets with trivial atomic measures with a single atom $\Omega$ are *empty*. This permits one to give the following definition.

**Definition 1.3.1.** A correlation space $\langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A\rangle$ is called a conspiracy space of the structure $\mathfrak{A} = \{A_1, ..., A_n\} \subseteq 2^A$ if

- $\{\{a\} \mid a \in A\} \subseteq \mathfrak{A}$;
- $\forall A_* \in \mathfrak{A}$ the secret $A_*$ is complete;
- $\forall A_* \notin \mathfrak{A}$ the secret $A_*$ is empty;
- $\mathfrak{I}^a = \sigma(\bigcup_{a\in A_*\in\mathfrak{A}} \mathfrak{S}_\Phi^{A_*})$, i.e. $\mathfrak{I}^a$ is the least σ-algebra containing all secret σ-algebras of cabals that each player $a$ belongs to.

[5]Here and below, $\sigma(\mathfrak{X})$ means the explement of the family of sets $\mathfrak{X}$ up to σ-algebra

Simply put, conspiracy spaces are correlation spaces such that a) the secret of any cabal of players is either complete or empty; b) each player is the cabal of his own with a complete secret; c) the players do not have any knowledge about the state of nature other than that generated by the secrets of the cabals to which they belong. For illustration, let us construct the simplest example of such a space:

– $A = \{1, 2, 3\}$,
– $\Omega = [0, 1)^2$,
– $\mathfrak{I}^1 = \sigma(\{[0, p_1) \times [0, 1) \mid 0 < p_1 \leqslant 1\})$,
– $\mathfrak{I}^2 = \sigma(\{[0, 1) \times [0, p_2) \mid 0 < p_2 \leqslant 1\})$,
– $\mathfrak{I}^3 = \sigma(\{[0, p_1) \times [0, p_2) \mid 0 < p_1 \leqslant 1, 0 < p_2 \leqslant 1\})$,
– $\mathbb{P}$ is the Lebesgue measure.

In this example, the correlation space consists of two independent real roulettes, players 1 and 2 observe one of these each, and player 3 observes both. In this case, it turns out that $\mathfrak{S}_\Phi^{\{1,3\}}$ coincides with $\mathfrak{I}^1$, $\mathfrak{S}_\Phi^{\{2,3\}}$ coincides with $\mathfrak{I}^2$, and for the other cabals $A_* \subseteq A$ the corresponding $\mathfrak{S}_\Phi^{A_*}$ is trivial. The structure of a space (or the *conspiracy family*) is the set of all cabals of players with complete secrets. In the above example, the structure of the space is $\mathfrak{A} = \{\{1,3\},\{2,3\}\}$. From the point of view of feasible strategy profiles, this means that any cabal of players in the conspiracy family can use a common secret to form a correlated strategy, and players outside this cabal cannot join the choice of strategies agreed in this way. In contrast, cabals of players outside of the conspiracy family do not have the above-described opportunity. The structure of the space can be viewed as its exhaustive final description, because the following theorem holds.

**Theorem 1.3.1.** *All conspiracy spaces of the same structure are isomorphic.*

Once again, proof of this theorem amounts to exercise in topology without close connection to the central ideas of the study and can be found in Appendix B. Now that it has been established that the set of all conspiracy spaces is divided into equivalence classes, it is not difficult to suggest a way to construct a standard representative of each class from the corresponding conspiracy family.

**Definition 1.3.2.** The standard space of a structure $\mathfrak{A} = \{A_1, A_2, ..., A_n\}$ is the correlation space $\Phi_\mathfrak{A} = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A\rangle$ with the parameters

– $A = \bigcup\limits_{i=1}^{n} A_i$,
– $\Omega = [0, 1)^n$,
– $\mathfrak{I}^a = \sigma(\{\prod\limits_{i=1}^{n} [0, p_i) \mid \textbf{if } a \in A_i \textbf{ then } 0 < p_i \leqslant 1 \textbf{ else } p_i = 1\})$,

– $\mathbb{P}$ is the Lebesgue measure.

The set of states of nature is the $n$-dimensional (according to the numbers of conspiracies in the family) unit cube, and the probability measure corresponds to the continuous uniform distribution. In this case, the σ-algebra of each player is the Borel algebra in the projections onto the axes corresponding to the conspiracies they are part of and is trivial in the projections onto the other axes. The choice of a standard representative for any conspiracy families allows one to use the notation $\Gamma|\mathfrak{A}$, by which we will understand $\Gamma|\Phi_{\mathfrak{A}}$. This notation emphasizes the fact that the choice of a particular correlation space among all conspiracy spaces of the required structure is irrelevant for us, and the standard space serves as the simplest representative suitable for practical calculations.

## 1.4 Three-player even-odd

The game of «three-way even-odd» can serve as an elementary example of a conflict sensitive to additional information asymmetry. It starts with each of the three participants secretly choosing «eagles» or «tails» on their coins and laying them on the table under their palms with the appropriate sides up. After that everyone simultaneously take off their hands and, depending on the combination, divide the fixed bank. When all three coins lie on the same side, the round is considered a draw and the players divide the pot equally. If only two of them matched, then the short-handed player is considered the loser and does not receive a share in the pot division. In matrix form, this can be described as follows:

Table 1 — Three-player even-odd

| | |
|---|---|
| $4,4,4$ | $6,0,6$ |
| $0,6,6$ | $6,6,0$ |

| | |
|---|---|
| $6,6,0$ | $0,6,6$ |
| $6,0,6$ | $4,4,4$ |

In the table 1, the first player chooses a row, the second — a column, and the third — a matrix. The solution of this game in pure strategies is two Nash equilibria corresponding to the synchronous choices of the same sides by all players. In mixed strategies, another degenerate solution is added, with each player making an equally probable random choice between heads and tails. All these solutions obviously give the

expectation of payments equal to $(4,4,4)$. In the framework of classical game theory, this would be the end of conflict analysis, but the addition of information asymmetry makes the situation more interesting. Consider the same game in the conspiracy space of structure $\{\{1,2\}\}$, i.e. in a situation where players 1 and 2 have the opportunity to use correlated strategies arranged in secrecy from player 3. Let $\alpha \in [0,1)$ be the value of the corresponding secret roulette wheel. Conspirators can use strategies of the form $\mathbf{s}^1, \mathbf{s}^2 : [0,1) \to P_{\{\mathbf{head},\mathbf{tail}\}}$, where $P_{\{\mathbf{head},\mathbf{tail}\}}$ denotes all possible probability measures on the set $\{\mathbf{head}, \mathbf{tail}\}$, i.e. the set of classical mixed strategies of the game under consideration. The outsider, on the other hand, has to be content with the $\mathbf{s}^3 \in P_{\{\mathbf{head},\mathbf{tail}\}}$ strategies, since he has no access to the conspiracy roulette. In order to find themselves at a more favorable, comparing to an equal division, equilibrium point, players 1 and 2 can choose any strategies that result in an equiprobable synchronous choice of the coin side:

$$\mathbf{s}^1(\alpha) = \mathbf{s}^2(\alpha) = \begin{cases} (1,0), & \alpha < \frac{1}{2}, \\ (0,1), & \alpha \geqslant \frac{1}{2}. \end{cases}$$

Moreover, any mixed strategy of player 3, owing to independence from the conspiracy roulette, ensures that it coincides with the others in exactly half of the cases. The payouts in this situation are $(5,5,2)$, and there is no profitable individual deviation for any of the players.

### 1.5 Necessary complexity of the conspiracy model

The conventional formalism of the matrix game in normal form identifies the profile of pure strategies with the game outcome — they are literally the same mathematical object. Almost the same can be said about its mixed extension — the space of profiles of mixed strategies is isomorphic to the space of outcomes, consisting of probability distributions on the game matrix that adheres to independence in the choice of rows and columns. Alas, the correlated extension as formulated by Robert Aumann messes up this rosy picture. Its space of game outcomes is even simpler than in the mixed case — any probability distribution on the set of elements of the game matrix goes, without additional conditions. But with strategic profiles, everything sharply becomes more complicated — the strategy of each player is a function, which

maps the set of states of nature into the set of his pure strategies, reckoning with observance of measurability in its awareness σ-algebra. Obviously this prevents any possibility of one-to-one correspondence between profiles and outcomes — depending on the correlation space parameters, some outcomes may not be achievable at all, while equiprobable events can be swapped around in the strategy domain without affecting the outcome. On top, when working with correlated strategies in Aumann's formulation, one can encounter multidimensional event spaces, Borel σ-algebras, and other non-trivial phenomena of Kolmogorov probability theory, which probably also contributes to how reluctant game theorists are about resorting to this tool in more applied research.

The conspiracy model proposed here narrows the correlated extension by extracting from a continuum of possible correlation spaces a finite (for any finite number of players) set, one for each conspiracy structure. At first glance, such a radical simplification of the parameter space gives hope that in the practical use of the model it would also be possible to do without the «esoteric» aspects of measure theory. Ideally, we'd like to identify in one way or another the space of strategic profiles with the set of outcomes in games with conspiracies, just as it happens in conventional formalisms. If we could, looking only at the probability distribution of the individual outcome realization in the game matrix, determine which strategy profile (or any representative from the family of indistinguishable profiles) was selected by the players, this would imply ability to also find all distributions achievable in certain deviations from the played strategy profile, thereby checking the situation for equilibrium without diving into the details of the Auman correlation model.

Alas, in the general case it is hardly possible — the loss of important information in the transition from sets of strategies to the result of correlation can be made clear, using the same tripartite even-odd described in the previous section. Imagine that the game is played in conspiracy space $\{\{1,2\},\{1,2,3\}\}$, that is, players 1 and 2 can correlate their actions both secretly from player 3 and together with him. The correlation space then turns out to consist of two roulettes $\alpha^{1,2}$ and $\alpha^{1,2,3}$ observed by the players indicated in the superscripts of their designation. Consider two sets of strategies: first

$$\mathbf{s}^1(\alpha^{1,2},\alpha^{1,2,3}) = \mathbf{s}^2(\alpha^{1,2},\alpha^{1,2,3}) = \begin{cases} (1,0), & \alpha^{1,2,3} < \frac{1}{2}, \\ (0,1), & \alpha^{1,2,3} \geqslant \frac{1}{2}, \end{cases} \mathbf{s}^3(\alpha^{1,2,3}) = (\frac{1}{2},\frac{1}{2}),$$

and second

$$\mathbf{s}^1(\alpha^{1,2},\alpha^{1,2,3}) = \mathbf{s}^2(\alpha^{1,2},\alpha^{1,2,3}) = \begin{cases} (1,0), & \alpha^{1,2} < \frac{1}{2}, \\ (0,1), & \alpha^{1,2} \geqslant \frac{1}{2}, \end{cases} \mathbf{s}^3(\alpha^{1,2,3}) = (\frac{1}{2},\frac{1}{2}).$$

In both cases, all players make an equally probable choice between heads and tails, provided that the first two players make it synchronously, while the third — independently of them. The probability distribution of individual outcomes in the $2\times2\times2$ matrix from the table 1, can be expressed for both sets like this: $\begin{array}{|c|c|}\hline \frac{1}{4} & 0 \\ \hline 0 & \frac{1}{4} \\ \hline \end{array}$ $\begin{array}{|c|c|}\hline \frac{1}{4} & 0 \\ \hline 0 & \frac{1}{4} \\ \hline \end{array}$. Of course, the payments here are also equal and amount to $(5, 5, 2)$. However, on a closer look, it can be seen that in the first case, players 1 and 2 for synchronization use the $\alpha^{1,2,3}$ roulette that they share with player 3, which allows him by changing his strategy to

$$\mathbf{s}^3(\alpha^{1,2,3}) = \begin{cases} (1,0), & \alpha^{1,2,3} < \frac{1}{2}, \\ (0,1), & \alpha^{1,2,3} \geqslant \frac{1}{2}, \end{cases}$$

to join them for the outcome with the probability distribution $\begin{array}{|c|c|}\hline \frac{1}{2} & 0 \\ \hline 0 & 0 \\ \hline \end{array}$ $\begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & \frac{1}{2} \\ \hline \end{array}$, where the payouts are $(4, 4, 4)$. Therefore the first point is not a Nash equilibrium. In the second case, players 1 and 2 use for synchronization the private roulette $\alpha^{1,2}$, which outcome player 3 cannot observe. Whichever strategy he chooses, it would coincide with the strategies of the conspirators exactly in half of the cases, meaning that the payments can not change. Since the other players also do not have favorable deviations, indeed, this situation is a Nash equilibrium.

Thus, we have constructed an example in which the same distribution of outcome probabilities in the game matrix corresponds to at least two sets of strategies so different that one of them is a Nash equilibrium, and the second is not. Obviously, it is impossible to combine these sets in one equivalence class in any reasonable way, which means that in the general case it is impossible to identify game situations with outcomes of the game, no matter how hard we try. Anyway, it should be noted that in simpler cases, when each player can't participate in more than one cabal, there is no way to construct such a clear and trivial counterexample — when solving practical problems, if the correlation manifested in the probability distribution on the game matrix could be obtained in only one way, nothing prevents us from working directly with probability distributions, and not with functions that map signals to outcomes. However, if we consider conspiracy theory as a modeling tool for information asymmetries that independent agents interactively develop in an uncontrolled environment, then such self-restraint, alas, would limit our framework without natural justification.

# Chapter 2. Collective rationality in conspiracy games

## 2.1 Task scheduling problem[1]

The concept of Nash equilibrium, being the foundation of conventional game theory models, often turns out to be an insufficiently strong formalism in itself. Analysis of multilateral conflicts often breeds situations when the set of Nash equilibria is too large to be considered a proper solution for the game. In such case, the collective rationality criteria come to the researchers' aid — cherry-picking the equilibrium points for strong or weak Pareto optimality in many cases significantly narrows the space of solutions due to the quite natural exclusion of obviously unfavorable for all participants. The presence of additional information asymmetry creates new difficulties, since the proposed model implies an inevitable element of motivation antagonism — at new equilibrium points, the increase in the payoffs of those participating in the correlation occurs at the expense of reducing the payoffs of those who cannot join it, thereby making the usual criteria of collective rationality unproductive. To demonstrate this effect, consider a trivial generalization of the canonical task scheduling problem [14], a prominent mark in the conceptual landscape of game theory. This conflict commonly illustrates the *prices of anarchy* and *prices of stability* concepts, giving perhaps the most telling example of differences between same game Nash equilibria in terms of their global optimality. However, we need to look at this game from a different angle, in which the notions of the anarchy and stability prices lose their meaning, making room for sensitivity to additional information asymmetry.

Let's start with the canonical task scheduling model. The computer center has $m$ employees, each of which is assigned to perform some calculation. They have $n$ computers at their disposal, each being able to run one or more programs that perform employee calculations. The machines have architectural differences, expressed by the matrix of constants $t_i^a \geqslant 0$, each denoting the execution time of the employee's program $a = \overline{1,\ldots,m}$ on the computer $i = \overline{1,\ldots,n}$. Each calculation can be performed by only one device. Several programs on the same computer run sequentially, but the results of their work are produced simultaneously after the last one is stopped. Thus, the employee's benefit comes from choosing such a computer for his calculation that

[1] The section refines and elaborates the materials of the [10] article.

total execution time of all programs running on it turns out to be minimal. Let us describe what is happening in terms of the normal form game

$$\Gamma = \langle A, S^a, u^a(s), a \in A \rangle \tag{2.1}$$

parametrized with:

- $A = \{1, \ldots, m\}$;
- $S^1 = \ldots = S^m = \{1, \ldots, n\}$;
- $u^a(s) = -t_{s^a}(s)$, where $t_i(s) = \sum\limits_{a \in A, s^a = i} t_i^a$.

Here we should focus on the definition of the payout function. By choosing $u^a(s) = -t_{s^a}(s)$, we simulate a situation where all calculations should have been completed yesterday, and employees are directly penalized for every extra second until their results land on boss's desk. However, it is possible to simulate a less stressful working moment by taking, for example, a stepwise payout function:

$$u^a(s) = \begin{cases} u^a_{GOOD}, & t_{s^a}(s) < t^a_{DEADLINE}; \\ u^a_{LATE}, & t_{s^a}(s) \geqslant t^a_{DEADLINE}. \end{cases}$$

In this case, we assign for each player $a$ the deadline $t^a_{DEADLINE}$, meeting which implies the successful completion of the task rewarded by a fixed payment $u^a_{GOOD}$ (including the bonus), and not meeting — $u^a_{LATE}$ (regular rate). One can come up with variety of more complex incentive schemes for employees, so let's formulate it in a general way:

$$u^a(s) = v^a(t_{s^a}(s)), \tag{2.2}$$

where $v^a(t)$ is a monotonically non-increasing promptness reward function assigned by employee $a$. Any normal form game built according to the scheme 2.1 with a payoff function of the form 2.2 is essentially a task scheduling problem, with the condition of monotonic non-increase of $v^a(t)$ being necessary, since the proof of property widely considered important for this game explicitly relies on it — the cost of stability being equal to 1 [15]. Let us recall that in optimization problems with selfish agents, the cost of stability is the ratio $\frac{t_{NASH}}{t_{BEST}}$, where $t_{NASH}$ is the value of the best Nash equilibria, and $t_{BEST}$ — the value of the globally optimal solution. This means that in the task scheduling problem there are bound to be Nash equilibria among all situations minimizing the time until the last computer stops. However, in this study, we propose to temporarily forget about minimizing the total computation time and instead analyze new properties of the model appearing in the absence of such a monotonicity constraint.

## 2.2 Individualism penalty[2]

Imagine a data center with computers requiring complex maintenance after a shift if at least one task was run on them. If employees who meet deadlines are rewarded regardless of that, it's not hard to imagine a situation where they, trying to guarantee themselves a bonus at any cost, will scatter tasks over an unreasonably large number of computers. Faced with such a prospect, to avoid systemic underutilization of machines, management might be tempted to incentivize its employees through fines. This can be modeled by a step promptness reward function of the following form:

$$v^a(t) = \begin{cases} u^a_{HAST}, & t < t^a_{BREAKAWAY}; \\ u^a_{GOOD}, & t^a_{BREAKAWAY} \leqslant t < t^a_{DEADLINE} \\ u^a_{LATE}, & t^a_{DEADLINE} \leqslant t \end{cases};$$

Here, for each employee $a$, along with the deadline $t^a_{DEADLINE}$, which must be met in order to receive the bonus, we also fix the minimum workload of the utilized machine $t^a_{BREAKAWAY}$, which must be reached in order not to run into a fine for wasting computing resources (whereby $u^a_{HAST} < u^a_{LATE} < u^a_{GOOD}$). The size of the minimum workload can be set, for example, depending on the importance of the corresponding task — if an urgent result pays for the use of additional machines, then it can be made lower or even equated to zero. If, on the contrary, the task is not so important, then a large minimal workload will force such employee to mind the interests of the company and cooperate with colleagues.

As you can see, employees in this case have to act on a non-monotonic promptness reward function, creating some effects unusual for the canonical formulation of the task scheduling problem. First, in such a scenario, it is expected that not for every game the cost of stability will be equal to $1$. It suffices to consider a game with $2$ employees and $2$ identical computers:

- $t^1_1 = t^1_2 = 8$,
  $t^2_1 = t^2_2 = 2$;
- $t^1_{DEADLINE} = t^2_{DEADLINE} = 9$,
  $t^1_{BREAKAWAY} = t^2_{BREAKAWAY} = 3$;
- $u^1_{HAST} < u^1_{LATE} < u^1_{GOOD}$,
  $u^2_{HAST} < u^2_{LATE} < u^2_{GOOD}$.

[2] The section refines and elaborates the materials of the [10] article.

Since the first player, definitely not having problems with underloading, fits into the deadline only by using the computer solo, obviously, strategy combinations of both players choosing the same machine cannot be Nash equilibria. Similarly, since it is more profitable for the second player to be late with the calculations than to be punished for running an insufficiently heavy task on a separate computer ($u^a_{HAST} < u^a_{LATE}$), no Nash equilibria can be found among situations where each employee uses his own machine too. In terms of the payoff structure, the game turns out to be indistinguishable from the even-odd game, which has no solutions in pure strategies at all, having the only Nash equilibrium point with both players making independent equiprobable choice between the alternatives. Note that the most loaded machine will work either $10$ hours if their choices match, or $8$ if they do not match with the probability $\frac{1}{2}$, which gives the expected value of stability equal to $\frac{9}{8}$. In fact, when the monotonicity of the promptness reward function is abandoned, it hardly makes sense to talk about the prices of stability and anarchy at all, since games clearly not related to the search for a minimum duration of computations are now included in the class.

## 2.3 Mixed equilibria of $\Gamma^3_n$ game[3]

Task scheduling with nonmonotonic returns is a fairly large class of conflicts, the analysis of which in general terms is beyond the scope of this work. For a compelling demonstration of the desired effect, a specially designed example will be quite sufficient. Let's consider the game $\Gamma^3_n$ of the same general scheme as in the previous section, but slightly more complicated, with $3$ tasks of the same type and $n \geqslant 2$ identical computers:

- $t^1_i = t^2_i = t^3_i = 2, i = \overline{1,n}$;
- $t^1_{DEADLINE} = t^2_{DEADLINE} = t^3_{DEADLINE} = 5$,
  $t^1_{BREAKAWAY} = t^2_{BREAKAWAY} = t^3_{BREAKAWAY} = 3$;
- $u^1_{HAST} = u^2_{HAST} = u^3_{HAST} = 0$,
  $u^1_{GOOD} = u^2_{GOOD} = u^3_{GOOD} = 3$,
  $u^1_{LATE} = u^2_{LATE} = u^3_{LATE} = 2$

Simply put, in the game $\Gamma^3_n$ it is most profitable to use a computer a deux — $4$ hours of total work time are just in the optimal gap between the underload limit and the

[3]The section refines and elaborates the materials of the [10] article.

deadline. The next most profitable option is to use one machine in threes, which results in a late fee. The least attractive is the choice of a computer running no other tasks — the player does not receive anything at all for such an expenditure of a public resource. At first glance, this game does not look too unusual. Nash equilibria in pure strategies are easy to find — all profiles $(i, i, i), i = \overline{1,n}$, and it is also obvious that no other solutions in pure strategies are possible. With mixed strategies, things get a little more interesting.

**Lemma 2.3.1.** *Let $T \subseteq \{1, \ldots, n\}$ be an arbitrary non-empty subset of computers. Then in the game $\Gamma_n^3$ the set of identical mixed strategies $s^1 = s^2 = s^3 = \left(\frac{[1 \in T]}{|T|}, \ldots, \frac{[n \in T]}{|T|}\right)$, where each player independently and equiprobably chooses one of the machines in the set $T$, is a Nash equilibrium.*[4]

*Доказательство.* We take advantage that it suffices to check deviations only in favor of pure strategies. Having symbol $s|_i^a$ stand for deviation from $s$ by player $a$ in favor of strategy $i$, we note that

$$\begin{aligned} u^a(s|_i^a) &= [i \in T]\left(\frac{(|T|-1)^2}{|T|^2}u^a_{HAST} + 2\frac{|T|-1}{|T|^2}u^a_{GOOD} + \frac{1}{|T|^2}u^a_{LATE}\right) \\ &= [i \in T]\frac{6\,|T|-4}{|T|^2}. \end{aligned}$$

Thus, for each player, the maximum expected payoff is achieved by deviating in favor of any computer in $T$. □

As such, without deviations, the mathematical expectation of payoffs amounts to $u^a(s) = \frac{6|T|-4}{|T|^2}, a = \overline{1,3}$. To prove that no other Nash equilibria in mixed strategies exist, we need a couple more lemmas:

**Lemma 2.3.2.** *In the game $\Gamma_n^3$, the set of mixed strategies $s = (s^1, s^2, s^3)$ can be a Nash equilibrium only if $s^1 = s^2 = s^3$.*

*Доказательство.* Let $s^a = (p_1^a, \ldots, p_n^a), a = \overline{1,3}$. If the strategies of the players do not coincide, then there is a computer $i$ for which (without loss of generality) the probabilities of choosing by the first and second players are $p_i^1 > p_i^2$. Due to the elementary properties of probabilities, there is also a computer $j$, where $p_j^1 < p_j^2$. Let us write down the mathematical expectation of the same players' payoffs when they

[4] Hereinafter the «Iverson bracket» notation is used to simplify and shorten the formulas: $[\text{TRUE}] = 1, [\text{FALSE}] = 0$.

choose the computer $i$ (for the $j$ everything coincides up to an index, obviously):

$$\begin{aligned} u^1(s|_i^1) &= (1-p_i^2)(1-p_i^3)u^1_{HAST} + (p_i^2 + p_i^3 - 2p_i^2p_i^3)u^1_{GOOD} + p_i^2p_i^3u^1_{LATE} \\ &= 3p_i^2 + 3p_i^3 - 4p_i^2p_i^3; \\ u^2(s|_i^2) &= 3p_i^1 + 3p_i^3 - 4p_i^1p_i^3; \\ u^3(s|_i^3) &= 3p_i^1 + 3p_i^2 - 4p_i^1p_i^2. \end{aligned}$$

About the function $f(x,y) = 3x+3y-4xy$ on the domain $0 \leqslant x \leqslant 1, 0 \leqslant y \leqslant 1$ one can notice the following — if $f(x_0, y_0) < 2$, then $f(x_0, y_0) < f(x_1, y_1)$ is true for any $x_1 > x_0, y_1 \geqslant y_0$ or $x_1 \geqslant x_0, y_1 > y_0$. Suppose $p_i^3 \leqslant p_j^3$ (if $p_i^3 \geqslant p_j^3$, the arguments are similar up to indices.) Consider the following cases:

- $p_i^2 < p_j^2$. Due to the elementary properties of probabilities, we can be sure that $p_i^2 < \frac{1}{2}$ and $p_i^3 \leqslant \frac{1}{2}$, whence $u^1(s|_i^1) < 2$, which means that $u^1(s|_i^1) < u^1(s|_j^1)$. Since $p_i^1 > p_i^2 \geqslant 0$, the first player chooses a non-optimal strategy with non-zero probability. $\perp$
- $p_i^2 \geqslant p_j^2$, which implies $p_i^1 > p_j^1$, and hence $u^3(s|_j^3) < u^3(s|_i^3)$ similarly to the previous point. If $p_j^3 > 0$, then the third player chooses a non-optimal strategy with non-zero probability. $\perp$
- $p_i^2 \geqslant p_j^2$, as in the previous case, but now $p_i^3 = p_j^3 = 0$. $p_j^1 < p_i^1$ similarly implies $u^2(s|_j^2) < u^2(s|_i^2)$, and so $p_j^2 > p_j^1 \geqslant 0$ implies the choice of a non-optimal strategy with non-zero probability by the second player this time. $\perp$

Thus, assumption that the existence of a computer for which the probability of being chosen by one player differs from the probability being chosen by another, contradicts the necessary condition of the Nash equilibrium in every case. □

**Lemma 2.3.3.** *In the game $\Gamma_n^3$, a set of identical mixed strategies can be a Nash equilibrium only if all computers chosen with non-zero probability are chosen with equal probabilities.*

*Доказательство.* Take any profile of identical strategies $(p_1, \ldots, p_n)$, where $0 < p_i < p_j$. Using the payoff formula from the previous lemma, $u^a(s|_i^a) = 2p_i(3-2p_i)$. Again, $p_i < \frac{1}{2}$ implies $u^a(s|_i^a) < u^a(s|_j^a)$, and so all players have chosen a non-optimal strategy with non-zero probability, which contradicts the necessary condition of Nash equilibrium. □

Having proved that the proposed equilibrium points exhaust the mixed strategy solution space, we can construct the convex hull of the set of attainable payoff vectors.

Since the set lies entirely on the line $(u,u,u)$, it suffices to find the minimum and maximum expected payoffs:

$$\min_{\varnothing\subset T\subseteq\{1,\dots,n\}}\frac{6\left|T\right|-4}{\left|T\right|^2}=\frac{6n-4}{n^2};$$
$$\max_{\varnothing\subset T\subseteq\{1,\dots,n\}}\frac{6\left|T\right|-4}{\left|T\right|^2}=2.$$

Thus, the desired convex hull is a segment connecting the points $(2,2,2)$ and $(\frac{6n-4}{n^2},\frac{6n-4}{n^2},\frac{6n-4}{n^2})$. If the game under consideration was not sensitive to additional information asymmetry, then its analysis would be completed — all players are in an equal position and, acting optimally, can expect equal payoffs from the indicated interval. However, through the lens of the conspiracy model this conflict looks much more interesting.

### 2.4 Correlated equilibria of the $\Gamma_n^3$ game in the conspiracy space[5]

Let's analyze the same conflict from the standpoint of conspiracy theory by moving on to the game $\Gamma_n^3|\{\{1,2\}\}$. Now, the game $\Gamma_n^3$ is supplemented by one real-value roulette, which result is known before choosing a strategy to players $1$ and $2$, but not $3$. To obtain an equilibrium set of correlated strategies that extricate payoffs from the convex hull of the solution set in mixed strategies, it is enough for the conspirators to take any of the classical Nash equilibrium points with $|T|\geqslant 2$, but instead of choosing between the elements of $T\subseteq\{1,\dots,n\}$ independently, they must divide the secret roulette into $|T|$ equal sectors and make their choice in unison, depending on the sector hit. Let us describe this more formally using the correlation space

$$\Phi=\langle A,\Omega,\mathfrak{I}^a,\mathbb{P},a\in A\rangle$$

In this case, the set of states of nature is $\Omega=[0,1)$, player awareness σ-algebras $\mathfrak{I}^1=\mathfrak{I}^2$ are Borel, $\mathfrak{I}^3=\{\varnothing,\Omega\}$ and the measure is $\mathbb{P}(X)=|X|$. The above strategies in the game $\Gamma_n^3|\Phi$ can be represented as functions that map the set of states of nature

[5]The section refines and elaborates the materials of the [10] article.

into the space of mixed strategies:

$$\mathbf{s}^1(\omega) = \mathbf{s}^2(\omega) = ([\zeta(\omega) = 1], \ldots, [\zeta(\omega) = n]);$$
$$\mathbf{s}^3(\omega) = \left(\frac{[1 \in T]}{|T|}, \ldots, \frac{[n \in T]}{|T|}\right),$$

where the function $\zeta : \Omega \to T$ common for players 1 and 2 determines the partition of the roulette into $|T|$ equal sectors.

The payouts in this profile are no longer symmetrical:

$$u^1(\mathbf{s}) = u^2(\mathbf{s}) = \frac{|T| - 1}{|T|} u^a_{GOOD} + \frac{1}{|T|} u^a_{LATE} = \frac{3\,|T| - 1}{|T|};$$
$$u^3(\mathbf{s}) = \frac{|T| - 1}{|T|} u^a_{HAST} + \frac{1}{|T|} u^a_{LATE} = \frac{2}{|T|}.$$

In this case, the situation is indeed a Nash equilibrium, since the first and second players can use as strategies any functions that map $\Omega$ into the space of probability measures on $\{1, \ldots, n\}$, while the third player has to be content only with constant ones, since the correlation mechanism does not inform him about the state of nature. Noticing that $\frac{3|T|-1}{|T|} > 2$ for $|T| \geqslant 2$, we confirm the sensitivity of the $\Gamma^3_n$ game to additional information asymmetry — in the new solutions, players observing a random experiment not directly related to payoffs increase their payoff compared to the best result achievable in the canonical mixed case.

## 2.5 Collective rationality of decisions[6]

When considering the solution set of the game $\Gamma^3_n$ in ordinary mixed strategies, one should pay attention to the fact that for $|T| > 2$, the resulting Nash equilibrium points lack not only strong Pareto optimality, but even weak too. Indeed, payouts to all players at points where $|T| = 1$ or $|T| = 2$ are equal to 2, but for larger sizes of the set $\frac{6|T|-4}{|T|^2} < 2$. Such circumstances endow solutions using one or two computers with a special status — we can expect agents familiar with the principle of collective rationality to agree not to end up in a situation totally dominated by the other solution. The question naturally follows, is it possible to filter out in a similar way the solutions, that both

[6]The section refines and elaborates the materials of the [10] article.

take into account the additional information asymmetry, and satisfy the principles of collective rationality in at least some sense?

When you add a conspiracy space, consisting of the group $\{1, 2\}$, to the game it catches the attention that the classical principles of collective rationality become useless. At the new equilibrium points, the payoffs of the players 1 and 2 are now $u^1(\mathbf{s}) = u^2(\mathbf{s}) > 2$ and grow with the growth of $k$, while the utility of the third is $u^3(\mathbf{s}) < 2$ and declines, which indicates a direct antagonism of interests, making it impossible to agree on a collectively rational choice in the usual sense between a mixed equilibrium with $|T|$ equal to 1 or 2 and correlated solutions with different $k$. However, one can try applying a more subtle optimality criterion based on a slightly extended interpretation of what is happening in the game — let's call this formalism *structurally coherent Nash equilibrium*.

Structural coherency of equilibria in games with conspiracies is the quite simple idea — if we assume that the groups of players included in the family of conspiracies are united not only by a common correlation mechanism, but also, in broader terms, great opportunities for coordinating actions, then among the usual Nash equilibria in correlated strategies it is possible to single out those that are resistant to deviations not only individually, but also collectively, bearing in mind exclusively the groups included in the conspiracy family. For the game $\Gamma_n^3|\{\{1,2\}\}$, specifically, equilibria allowing a deviation by players 1 and 2, mutually increasing their payoffs, will be structurally incoherent. In the most general terms, this can be expressed as follows:

**Definition 2.5.1.** In a conspiracy game $\Gamma|\mathfrak{A}$, a situation $\mathbf{s}$ is a structurally coherent equilibrium if for all conspiracies $A_* \in \mathfrak{A}$ there exist no acceptable deviations from the situation $\mathbf{s}$.

There remains to formulate what, within the framework of this model, can be considered a deviation acceptable for various cabals. If we look at this question as a problem of multi-criteria optimization, where the criteria are the payoffs of individual participants, then two options arise:

1. Deviation is acceptable if it increases the payoff of all conspirators; (weak Pareto)
2. Deviation is acceptable if it increases the payoff of at least one conspirator without decreasing the payoff of the others. (strong Pareto)

Alas, for our purposes suitability of both options is questionable. It would be reasonable to expect that the addition of «dummy» to any conspiracy, i.e. player with

a single pure strategy and constant payoff, should not change anything in the solution of the game. However, a conspiracy with such «dummy» in the lineup cannot have acceptable deviations in the weak Pareto sense at all, which means that its participants lose the opportunity to use collective rationality. This obviously makes the first of the proposed options too weak. On the other hand, considering the three-way even-odd game (see 1.4) with two cabals creates an unpleasant problem for the second option as well. If player 1 is in a cabal with player 2, and player 2 with player 3, then we can expect outcomes with payments formed by any mixture of $(5, 5, 2)$ and $(2, 5, 5)$, with the choice of proportion at the behest of player 2. The catch is that strong Pareto acceptability encourages player 2 in the $(5,5,2)$ situation to deviate conspiring with player 3 to improve the other's payoff. Similarly, in the $(2,5,5)$ situation, player 2 has to help player 1. In intermediate situations, player 2 can help both, which means that such altruism rules out the existence of a structurally coherent equilibrium in the problem at all, making the second version of the acceptability definition too strong. To bypass both problems, an intermediate definition of deviation should be proposed, which will be stronger than weak Pareto, but weaker than strong Pareto:

**Definition 2.5.2.** In the conspiracy game $\Gamma|\mathfrak{A}$ a situation $\mathbf{s}_* \neq \mathbf{s}$ is called a deviation from $\mathbf{s}$ acceptable for the cabal $A_* \in \mathfrak{A}$ if

– $\forall a \notin A_* \quad \mathbf{s}^a = \mathbf{s}^a_*$;
– $\forall a \in A_* \quad u^a(\mathbf{s}_*) \geqslant u^a(\mathbf{s})$;
– $\forall a : \mathbf{s}^a \neq \mathbf{s}^a_* \quad u^a(\mathbf{s}_*) > u^a(\mathbf{s})$.

It is easy to see that the proposed optimality criterion is related to the concept of strong Nash equilibrium [16], which implies resistance to all kinds of group deviations that benefit all its participants. In fact, structurally coherent equilibrium can be considered a modification of the strong one, which differs in two aspects, one of which noticeably weakens it, and the other slightly sharpens it. The weakening stems from the fact that collective deviations are not allowed for all possible groups of players, but only for those included in the conspiracy structure. What leads to sharpening is that as the success criterion for deviation we consider profit not for all members of the group, but only for those who actively participate in the deviation, changing their strategy, while passive observers from the same group can be content with the absence of losses.

If we were talking only about Nash equilibria in pure and mixed strategies, even such an optimality criterion would turn out to be too strong — indeed, the simultaneous choice by the first and second players of the computer $i$, chosen by the third with

probability $p_i^3 < 1$, gives both payoffs $(1 - p_i^3)u_{GOOD}^a + p_i^3 u_{LATE}^a = 3 - p_i^3 > 2$, which eliminates all solutions in the game $\Gamma_n^3$ For the game with conspiracies, however, the following can be formulated:

**Theorem 2.5.1.** *In the conspiracy game $\Gamma_n^3|\mathfrak{A}$ a structurally coherent Nash equilibrium exists for any $n$ and $\mathfrak{A}$. For non-degenerate $\mathfrak{A}$, each two-participant cabal corresponds to an unique equilibrium like that.*

*Доказательство.* Three cases are possible depending on $\mathfrak{A}$:

1. $\mathfrak{A} = \varnothing$. With an empty family of conspiracies, group deviations are impossible, so any Nash equilibrium in pure or mixed strategies will be structurally coherent.
2. $\mathfrak{A} = \{\{1, 2, 3\}\}$. For a degenerate family of conspiracies with one public correlation mechanism, the set of solutions is a convex hull of mixed equilibrium payoff vectors, which, as shown in 2.3, gives a interval connecting $(2, 2, 2)$ and $(\frac{6n-4}{n^2}, \frac{6n-4}{n^2}, \frac{6n-4}{n^2})$. In which case, the criterion of structural coherency, obviously, filters out everything except the point $(2, 2, 2)$, corresponding to pure equilibria with the choice of any single shared strategy for everyone and mixed equilibria with an independent equiprobable choice of any pair of same strategies by each player.
3. $\mathfrak{A}$ contains $\{1, 2\}$, $\{1, 3\}$ or $\{2, 3\}$. As shown in the 2.4 section, the use of secret correlation mechanisms yields new equilibrium points with payoffs of $\frac{3k-1}{k}$ for conspirators and $\frac{2}{k}$ for outsider, where $k$ is the number of machines involved in the strategy profile. Since for $k \geqslant 2$ the each of the conspirators' payoff exceeds the best conventional result, no points of mixed equilibrium will be structurally coherent. Since with the growth of $k$ the conspirators' payoffs also increase, we filter out all correlated equilibria too, except for those that maximize the income of any couple of conspirators at $k = n$. Thus, each cabal in the structure of conspiracies corresponds to one (up to permutations of roulettes) point of structurally coherent equilibrium, in which players choose equiprobably from the entire available computer pool, with the choice of cabal members always coinciding while being independent from the choice of the remaining player.

□

For new structurally coherent equilibria, it is easy to find a fairly natural interpretation. If we imagine that two employees can coordinate their activities

unbeknownst to a third, then it is not surprising that they tend to choose one computer for two in order to avoid an underload penalty, while minimizing the chance for a third player to stumble upon them coincidentally, depriving them of their promptness bonus. Logically, this is achieved when the highest probability of choosing each of the machines is minimal, i.e. with an equiprobable sweeping choice. Similarly, the goal for the third player is to maximize the smallest probability of choosing each of the computers, since he understands that the conspirators are acting together and trying to avoid meeting him, and this is also achieved in a situation of equiprobable choice from the entire computer pool.

Thus, it is the combination in conspiracies of the group deviation ability with the presence of a secret correlation mechanism that produces $\Gamma_n^3|\mathfrak{A}$ solutions meeting the criteria of both collective and individual rationality. Note that in the absence of additional information asymmetry, the game $\Gamma_n^3$ does not have such solutions even with the coalition-proof Nash equilibrium formalism [17], which is more subtle and complex than strong equilibrium. This makes the criterion of structural coherency a powerful tool for the study of conflicts that provoke their participants to secretly coordinate actions. It is important, however, to understand that a structurally coherent equilibrium will not be found in every game with conspiracies — an obvious example is the classic prisoner's dilemma, where collective and individual rationalities are in irreconcilable contradiction, which, of course, is not removed by the addition of a correlation mechanism.

## 2.6 Preservation of conspiracy secrets amid consensus building

As is known, matrix games frequently have several points of Nash equilibrium (like coordination games), with profiles of strategies from different points being not equilibria themselves. Interpretation of such equilibrium points as game solutions requires stipulation that the players essentially choose equilibrium strategies not independently — the preference for one equilibrium point over another must be universal among the players. In canonical games with complete information, this does not create big problems, since the procedure leading to consensus may be wholly transparent, but when it comes to modeling conflicts with conspiracies, this issue begins to require a much more careful approach. When information asymmetry appears in

the game, significantly affecting its outcome, it may become beneficial for players to change the configuration of this asymmetry (for example, notifying of the secret signal players who should not know it according to the correlation space structure), for which, in case of bad design, the same consensus mechanisms can be used. In order to understand what can go wrong, it makes sense to start with the canonical case. If we imagine an arbitrary matrix game as a real process with live players under the control of an impartial host who monitors the game protocol, then something like the following procedure can be used to obtain a Nash equilibrium:

1. The host announces the payout matrix;
2. Players publicly discuss the choice of strategies;
3. Players secretly inform the host about their moves;
4. The host announces the aggregated strategy profile;
5. The host can choose any of the players with a non-zero probability and offer him to retract the move;
6. The host calculates and announces the winnings.

This procedure is quite sufficient if we are talking about canonical Nash equilibria in pure and mixed strategies. In the second case, it should only be clarified that the implementation of a specific outcome, determined by a set of mixed strategies, either does not occur at all (the host announces the mathematical expectations of the payoffs), or occurs only at the last stage. However, when correlation spaces are added to the model, the situation becomes somewhat more complicated. Since any functions mapping the signals received by the players into mixed strategies can serve as correlated strategies, it seems natural to imagine the players themselves calculating their own functions upon receiving all the relevant signals:

1. The host announces the payout matrix;
2. Players publicly discuss the choice of correlated strategies;
3. The host generates a state of nature and notifies the players about the corresponding events from their awareness σ-algebras;
4. Players secretly calculate mixed strategies and inform the host about their moves;
5. The host announces the aggregated mixed strategy profile;
6. The host can choose any of the players with a non-zero probability and offer him to retract the move;
7. The host calculates and announces the winnings.

Unfortunately, such a naive approach has a significant drawback — it works as expected only in symmetric correlation spaces, where the awareness σ-algebras of all players coincide. If we are talking about conspiracy spaces, then two problems arise at once. Firstly, between steps 3 and 4, some of the players may be tempted to divulge the private signal value, if this can induce players who are not aware of it to choose a strategy more profitable for the leaker. While this issue could be fixed by adding to the algorithm a ban on communication between players starting after stage 2, but, alas, this is only one of the problems.

Secondly, which is somewhat more difficult to correct, in the presence of information asymmetry, the ability of any player to change the chosen strategy at stage 6 ceases corresponding to the concept of Nash equilibrium. In the symmetrical case, between the initial choice of the mixed strategy at stage 4 and the possible deviation from it at stage 6, the player does not receive any additional information, since the publicity of the signal already allows calculating the mixed strategies chosen by other players — by announcing them, the host, in fact, only fixes the result of the public agreement reached at stage 2. Asymmetric correlation spaces, on the other hand, contain events about which only a part of the players are notified at stage 3. In this case, each player can reliably calculate his own mixed strategy, but not the strategies of opponents tied to signals hidden from him. In this situation, the announcement by the host of the aggregated mixed strategies at step 5 increases the knowledge of the players before one of them decides to deviate, which contradicts the idea of Nash equilibrium. To bring the above procedure in line with the modeled formalism, it must be changed in a somewhat counterintuitive way:

1. The host announces the payout matrix;
2. Players publicly discuss the choice of correlated strategies;
3. Players secretly inform the host about their chosen correlated strategies;
4. The host announces the aggregated correlated strategy profile;
5. The host generates a state of nature and calculates mixed strategies of players;
6. The host can choose any of the players with a non-zero probability, notify him about the realized events from his awareness σ-algebras and offer him to revise mixed strategy calculated by the host;
7. The host calculates and announces the winnings.

Thus, in contrast to the symmetrical case, the conspiracy model disallows looking at correlated strategies as «black boxes» in the players' heads, that simply prompt synchronous responses to stimuli. Here, sets of correlated strategies have to

be interpreted as spoken and formally fixed agreements, since the concept of Nash equilibrium implies the possibility of deviation precisely at the moment when only the intentions of the players to respond in one way or another to secret signals are generally known, but not their specific reactions yet.

Interestingly, when we try to generalize this procedure to obtain structurally coherent equilibria in conspiracy spaces, we again run into a similar problem. At first glance, it would be enough to clarify only stage 6, so that the host could propose deviations from the chosen strategies both to individual players and to entire groups of conspirators. However, this only works as expected for the most simple families with non-overlapping cabals. In the case, where two cabals share participants, now group deviations cease corresponding to the formalism — because if, before discussing them, the leader informs each conspirator about the roulettes of all the cabals he is included in, then one of them could divulge the secret of another cabal, thereby improperly increasing the knowledge of non-participants before deviation decision. The easiest way to fix this is by moving group deviations into a separate stage, preceding the generation of the state of nature:

1. The host announces the payout matrix;
2. Players publicly discuss the choice of correlated strategies;
3. Players secretly inform the host about their chosen correlated strategies;
4. The host announces the aggregated correlated strategy profile;
5. The host can choose any of the cabals with a non-zero probability and offer its members to revise chosen correlated strategies;
6. The host generates a state of nature and calculates mixed strategies of players;
7. The host can choose any of the players with a non-zero probability, notify him about the realized events from his awareness σ-algebras and offer him to revise mixed strategy calculated by the host;
8. The host calculates and announces the winnings.

Note that stage 5 (discussion and approval of group deviation by the conspirators) is itself a multi-stage process in which those who want to increase their gain by changing strategy propose a deviation project, while the remaining conspirators can individually impose a veto if this project brings them a loss. Thus, the structural coherence of the equilibrium implies that cabals can deviate at the planning stage, before the players receive information about the state of nature, while individual deviations are possible after the correlation mechanisms comes into action, but before the announcement of actual mixed strategies played by opponents.

## 2.7 Nonmonotonic returns in other scheduling conflicts

Using the $\Gamma_n^3$ game, we demonstrated, first, that task scheduling with a nonmonotonic promptness reward function can be sensitive to additional information asymmetry, and, second, that in conspiracy games, despite their inherent partial antagonism of interests, it is possible for solutions to meet the principle of collective rationality. We emphasize the usefulness of these results by noting that the task scheduling problem is much broader than the example we have considered, both in the sense of the possible values of the parameters (the matrix of coefficients $(t_i^a) \in \mathbb{R}_{\geqslant 0}^{m \times n}$ and reward functions $v^a : \mathbb{R}_{\geqslant 0} \to \mathbb{R}, a = \overline{1,m}$), and in the sense of a variety of practical applications models. In the context of this work, it makes no sense to go into too much detail on more complex cases, but in order to show the possible connection of the model with the real world outside of data centers with strange employee incentive schemes, we will try to build a couple of examples with a more substantial application domain.

Let's start with economics by imagining how $m$ companies are preparing to enter the market with high-tech product offerings, while facing the choice between $n$ different open standards for the same important aspect of it. For example, it can be a variety of industrial robots and standards for their integration into a «smart» shop. When the company $a \in \{1, \ldots, m\}$ enters the market of the $i \in \{1, \ldots, n\}$ standard, it thereby makes a contribution to its development characterized by the vector constant $t_i^a \in \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0}$, the components of which correspond to separate independent aspects (for example, purposes which robots are fulfilling). If in the situation $s$ several companies use the same standard $i$, then by simply summing up their contributions, we can calculate the overall development index $t_i(s) = [s^1 = i]t_i^1 + \ldots + [s^m = i]t_i^m$. The expected return on investment in each of the standards is significantly affected by two discounting factors: the network effect and market saturation.

By network effect, we mean the dependence of consumer enthusiasm on the general development index of the standard — the function $0 \leqslant \alpha^a(t) \leqslant 1$ characterizes the share of buyers who are ready to purchase company $a$ robots made according to the standard with a common development index of $t$. A more developed standard always attracts more consumers, so the functions $\alpha^a(t)$ are monotonically nondecreasing, i.e. $\alpha^a(t) \leqslant \alpha^a(t + \Delta), \forall t, \Delta \succeq (0, \ldots, 0)$. Market saturation, on the other hand, implies limited demand — with an excess of investment in any of the standards, the buyers' solvency is no longer enough for everyone, prices have to go down, and revenues go

down with them. Accordingly, one more function $0 \leqslant \beta^a(t) \leqslant 1$ characterizes what fraction limits the company $a$ profit, making possible to maintain the competitiveness of its robots in the market of the standard with a common development index $t$. This function, for obvious reasons, is monotonically non-increasing, i.e. $\beta^a(t) \geqslant \beta^a(t + \Delta), \forall t, \Delta \succeq (0, \ldots, 0)$. Company $a$'s goal in choosing strategy $s^a$ is to maximize the combination of discount factors $u^a(s) = \alpha^a(t_{s^a}(s))\beta^a(t_{s^a}(s))$.

One can imagine a political interpretation of the same game. Let $n$ candidates try to be elected to some collegiate elective body (independently, without party lists), and $m$ tycoons choose which of them to campaign for in subordinate institutions. When oligarch $a$ decides to support candidate $i$, he thereby contributes to his popularity, characterized by the vector constant $t_i^a \in \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0}$, whose components correspond to electorally significant demographic groups. If in the situation $s$ candidate $i$ is supported by several oligarchs, then by simply summing up their contributions, one can obtain the overall popularity index of the candidate $t_i(s) = [s^1 = i]t_i^1 + \ldots + [s^m = i]t_i^m$. There are two discounting factors that influence the expected benefit of supporting a particular candidate: political influence and willingness to cooperate.

The political influence of a candidate in matters of interest to the oligarch who supported him obviously grows along with his overall popularity index, which is expressed by the function $0 \leqslant \alpha^a(t) \leqslant \alpha^a(t + \Delta) \leqslant 1, \forall t, \Delta \succeq (0, \ldots, 0)$. The willingness of a candidate to cooperate with each of his supporters, on the contrary, decreases with the growth of his total popularity, which is expressed by the function $1 \geqslant \beta^a(t) \geqslant \beta^a(t+\Delta) \geqslant 0, \forall t, \Delta \succeq (0, \ldots, 0)$. The goal of oligarch $a$ in choosing strategy $s^a$ is to maximize the combination of discount factors $u^a(s) = \alpha^a(t_{s^a}(s))\beta^a(t_{s^a}(s))$.

Let us reduce the description of both conflicts to a matrix game in normal form:

$$\Gamma = \langle A, S^a, u^a(s), a \in A \rangle;$$

$$A = \{1, \ldots, m\}, S^1 = \ldots = S^m = \{1, \ldots, n\};$$

$$u^a(s) = \alpha^a(t_{s^a}(s))\beta^a(t_{s^a}(s)), a = \overline{1,m};$$

$$\alpha^a, \beta^a : \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0} \to [0, 1];$$

$$0 \leqslant \alpha^a(t) \leqslant \alpha^a(t + \Delta) \leqslant 1, \forall t, \Delta \succeq (0, \ldots, 0);$$

$$1 \geqslant \beta^a(t) \geqslant \beta^a(t + \Delta) \geqslant 0, \forall t, \Delta \succeq (0, \ldots, 0);$$

$$t_i(s) = [s^1 = i]t_i^1 + \ldots + [s^m = i]t_i^m, i = \overline{1,n}.$$

It is easy to see the similarity of this game to the task scheduling problem, which we have tried to emphasize here by using the same symbols for variables and constants. In fact, the only significant difference is that in task scheduling, time $t$ was a scalar, not a vector. The promptness reward functions in the new formulations correspond to $v^a(t) = \alpha^a(t)\beta^a(t)$, the form of which determines our expectations from the outcome of the conflict. Earlier we said that the task scheduling problem analysis in general, for arbitrary $(t_i^a)$ and $(v^a)$ is an extremely difficult problem, and, of course, the transition from scalars to vectors in the domain of reward functions doesn't make things any easier. Here, the best we can do is to give a qualitative forecast for some informally described subclasses of conflict based on common sense, intuition and analogy with the special case of $\Gamma_n^3$ analyzed above.

To avoid overcomplication, we restrict ourselves to the case of quasiconcave reward functions $v^a(t) = \alpha^a(t)\beta^a(t)$, naturally generalizing this concept to multidimensional domains. First, denote by $T^a_{\nearrow}$ the set of all $t$ such that $t_* \prec t \Rightarrow v^a(t_*) \leqslant v^a(t) \wedge t_* \in T^a_{\nearrow}$. Similarly, by $T^a_{\searrow}$ we denote the set of all $t$ such that $t_* \succ t \Rightarrow v^a(t_*) \leqslant v^a(t) \wedge t_* \in T^a_{\searrow}$. These will be regions of continuous non-decreasing and non-increasing of $v^a(t)$, respectively. If these two sets cover the entire applicable domain, i.e. $T^a_{\nearrow} \cup T^a_{\searrow} = \mathbb{R}_{\geqslant 0} \times \ldots \times \mathbb{R}_{\geqslant 0}$, then the function $v^a(t)$ is quasiconcave. For similar functions, we can also denote «ridge» $T^a_{\sim} = T^a_{\nearrow} \cap T^a_{\searrow}$, which in the one-dimensional case corresponds to the maximum.

Let's try to depict logic of the conflict for the simplest case with a two-element family of plots $\mathfrak{A} = \{A_p, A_q\}, A_p \cap A_q = \varnothing, A_p \cup A_q = A$. We shorten the formulas using the following notation:

$$t_i^{A_*} = \sum_{a \in A_*} t_i^a, \forall A_* \subseteq A;$$

$$\check{u}^a = \min_{1 \leqslant i \leqslant n} v^a(t_i^A), \hat{u}^a = \max_{1 \leqslant i \leqslant n} v^a(t_i^A), \forall a \in A.$$

Here $t_i^{A_*}$ corresponds to the $i$th total standard development (candidate's popularity) index when it is chosen by the group of players $A_* \subseteq A$. Also, for each player $a$, the base payoff interval is the interval from $\check{u}^a$ to $\hat{u}^a$, i.e. from the smallest to the largest possible payoffs from the unanimous choice of a common strategy by all conflict participants. Consider games restricted by the following preconditions:

– $\forall a \in A, i = \overline{1,n}, v^a(t_i^{A_p \cup \{a\}}) < \check{u}^a$, i.e. no player can reach the lower bound of their base payoff interval if only the group $A_p$ chooses the same strategy;

– $\forall a \in A, i = \overline{1,n}, v^a(t_i^{A_q \cup \{a\}}) > \check{u}^a$, i.e. each player overcomes the lower limit of his base payment interval when choosing any strategy together with the group $A_q$;
– $\forall a \in A_q, i = \overline{1,n}, t_i^{A_q} \in T^a_{\searrow}$, i.e. for all members of the group $A_q$, the choice of a common strategy brings the total index into the region of non-increasing of the reward function.

Thus, we have outlined the range of situations in which the participants of the conflict are divided into two non-overlapping groups of conspirators. From the viewpoint of each conspiracy, assuming that outsiders are not involved in the game at all, it is easy to see that any strategy profile in which the conspirators choose one joint strategy will be a good candidate for Nash equilibrium. This does not mean that there cannot be other equilibria, but for the sake of clarity, we will deliberately restrict ourselves to the analysis of sets characterized by two independent probability distributions $p = (p_1, \ldots, p_n)$ and $q = (q_1, \ldots, q_n)$, where participants in the $A_p$ and $A_q$ conspiracies choose strategies $i = \overline{1,n}$ synchronously within groups but independently between groups with probabilities $p_i$ and $q_i$, respectively, using the appropriate private correlation mechanism. In this case, payments are calculated according to the formula

$$u^a(p,q) = \sum_{i=1}^{n} p_i((1-q_i)v^a(t_i^{A_p}) + q_i v^a(t_i^A)), \forall a \in A_p,$$

$$u^a(p,q) = \sum_{i=1}^{n} q_i((1-p_i)v^a(t_i^{A_q}) + p_i v^a(t_i^A)), \forall a \in A_q,$$

According to the preconditions, the $A_p$ cabal is not large enough to maximize the profits of its participants, so each of them would prefer to join the strategy chosen by the $A_q$ cabal. However, since the secret of the hostile conspiracy is not available to the players, they can only deviate from the strategy prescribed by the correlation mechanism in favor of another pure strategy. Thus, to make a profit as a result of an individual deviation from the distribution pair $(p,q)$, it is necessary and sufficient for the conspirator $a \in A_p$ to find such indices $i \neq j \in \{1, \ldots, n\}$ that for $p_i > 0$ the inequation holds

$$(1-q_i)v^a(t_i^{A_p}) + q_i v^a(t_i^A) < (1-q_j)v^a(t_j^a) + q_j v^a(t_j^{A_q \cup \{a\}}).$$

It is easy to see that with growth of any $q_j$, the number of indices $i$ for which this inequation holds also gradually increases, and as $q_j$ approaches 1, sooner or later it starts

to hold for all $i \neq j$. By fixing an arbitrary distribution $q$, for each conspirator $a \in A_p$ one can calculate the set $S_q^a \subseteq \{1, \ldots, n\}$, which consists of strategies that allow such productive deviations. At the same time, since the participants in the $A_q$ conspiracy, deviating from the prescribed strategy, inevitably suffer losses, nothing needs to be checked for them. As a result, an arbitrary pair of distributions $(p, q)$ describes a Nash equilibrium if and only if

$$\forall i \in \bigcup_{a \in A_p} S_q^a, p_i = 0.$$

Thus, if we are talking about equilibria only in the classical Nash sense without taking into account collective rationality, then in the described confrontation, the members of a large cabal do not have to think about possible betrayal on the part of comrades-in-arms, while a small cabal must carefully choose a common strategy so that its participants were not tempted to try guessing the strategy chosen by the big one. The desire to ascertain the structural coherency of the indicated solutions gives a slightly more interesting picture.

Let us make a reservation right away that, within the established constraints, it is difficult to accurately verify the structural coherency even for a narrow set of $(p, q)$-profiles under consideration, since, for example, collective deviations, dividing the $A_q$ cabal into two groups choosing different strategies, are quite possible. At the same time, one receives profit as a result of getting rid of unnecessary participants (see the constraint $t_i^{A_q} \in T_{\searrow}^a$, i.e., the unanimous choice points belonging to the non-increasing area of the recoil function). The second one potentially increases the income by joining the strategy chosen by the $A_p$ cabal, if there is a large enough $p_i$. Of course, one can try to impose additional restrictions on the parameters of the conflict, preventing such and even more exotic deviations, but this will greatly complicate the formulation without adding too much demonstrativeness.

Instead, we restrict ourselves to searching for only those $(p, q)$-tuples from which there are no successful collective deviations in favor of other $(p, q)$-tuples. The found equilibrium points can still be suspected of the lack of structural coherency, but we will at least exclude a large class of obviously inconsistent ones. So, for the profitability of the collective deviation of the small cabal, it suffices to find indices $i \neq j \in \{1, \ldots, n\}$ such that, for $p_i > 0$, for each $a \in A_p$ the following inequation holds:

$$(1 - q_i)v^a(t_i^{A_p}) + q_i v^a(t_i^A) < (1 - q_j)v^a(t_j^{A_p}) + q_j v^a(t_j^A).$$

Similarly, for a large cabal, the deviation is successful if there are indices $i \neq j \in \{1, \ldots, n\}$ such that for $q_i > 0$ for each $a \in A_q$ the inequation holds

$$(1 - p_i)v^a(t_i^{A_q}) + p_i v^a(t_i^A) < (1 - p_j)v^a(t_j^{A_q}) + p_j v^a(t_j^A).$$

Considering these inequations in the light of the constraints we have imposed on the parameters of the conflict, it is easy to see that collective rationality encourages both groups of players to minimize the highest probabilities of choosing individual strategies, but for opposite reasons. It is beneficial for the members of a small cabal to either individually or jointly adhere to the strategy chosen by the large cabal, the payments to whose members such an overlap of strategies obviously reduces. Translating into the language of the preestablished interpretations, a weak cartel participants would gladly take advantage of the standard development (or the candidate standing) selected by a large cartel, but a large cartel, on the contrary, does not relish at the prospect of sharing the limited demand in an already saturated market (or compete for attention of a politician already confident about his election) with unnecessary competitors.

At the level of collectively rational decisions, the game thus becomes a kind of two-sided hide-and-seek, where one group seeks to meet another who is trying to avoid this collision, and conspiracies serve to take advantage of the combined efforts while minimizing the likelihood of undesirable companions joining the profit carve-up. In fact, the formalism of structurally coherent equilibrium in conspiracy games is not some complicated economic concept, but only the embodiment of an intuitive principle that probably had applications even in the preliterate era. It is quite possible that some hunter, noticing a wounded mammoth while walking around the tribal lands, guesstimated: «Seemingly I won't overwhelm him alone, but it makes no sense to call the whole tribe. I'd rather whisper in the ear of a couple of friends — how much honor and glory it will be to hunt so much meat for only three of us.» The world history of conspiracies could begin with a reasoning similar to this.

# Chapter 3. Computational Complexity of Strategies in Repeated Games with Discounting

## 3.1 «Folk» theorem in conspiracy spaces

In order to understand how repetition affects conflicts that are sensitive to additional information asymmetry, it is necessary first to analyze how the «folk» theorem can be generalized to games in conspiracy spaces. Previously, this theorem has already been proved in various forms for the correlated expansion of games [3], deliberately restricted to the case of public correlation mechanisms. We need to take one more step away from this limitation. In fact, the main change is that the use of private correlation mechanisms can often further reduce the reserve payoffs of players who do not have access to them. Recall that the reserve payoff of player $a$ is

$$u_*^a = \min_{s \in \overline{S}_a} u^a(s), \overline{S}_a = \{\overline{s} \in S \mid \overline{s}^a \in \arg\max_{s^a \in S^a} u^a(\overline{s}|s^a)\},$$

that is, his smallest payoff among all possible outcomes in which he uses the strategy of the best response. Essentially, the reserve payoff denotes an utility margin below which the expected payoff of the respective player is impossible to lower down, even if all other players unite to achieve this goal, regardless of the damage to their own profits. The strategy profile leading to such an outcome is called minimax for player $a$. The vector $u_* = (u_*^1, \ldots, u_*^m)$, composed of the reserve payoffs of each player, is called the minimax point of the game. The reserve equilibrium payoff of player $a$ can be defined similarly:

$$\tilde{u}_*^a = \min_{s \in \tilde{S}} u^a(s), \text{where } \tilde{S} \text{ is the set of Nash equilibrium profiles},$$

which form the vector $\tilde{u}_* = (\tilde{u}_*^1, \ldots, \tilde{u}_*^m)$, which is called the equilibrium minimax point of the game. It is obvious that $\tilde{u}_* \succeq u_*$.

The central idea behind the proof of most «folk» theorems is the use of minimax sets of strategies to punish players who deviate from the designated chain of actions expected of them by their opponents. Any draw sequence $(s_i)$ with payoffs converging (in the mean or discounted sense, depending on the version of the theorem) to a vector $u_0 = (u_0^1, \ldots, u_0^m)$ strictly dominating the minimax point of the game (i.e., $u_0^a > u_*^a, a = \overline{1,m}$), can be the equilibrium outcome (in the ordinary Nash or subgame perfection

senses, depending on the version of the theorem) of a repeated game. If at iteration $i$ player $a$ deviates from the expected strategy $s_i^a$, then, starting from the next iteration, the remaining players proceed to apply the strategy from the minimax profile for this player, continuing to do so for a sufficiently long time (in some versions of the proofs, infinitely) so that the damage they inflict on player $a$ exceeds his profit from the deviation.

Correlated strategies in the context of repetitive games are usually understood in the limited sense — only public signals are considered, which, from our model's point of view, corresponds to conspiracy spaces of the structure $\{A\}$, that is, consisting of one cabal involving all players. The set of payoff vectors attainable in the game $\Gamma|\{A\}$ is the convex hull of the set of vectors entering into the payoff matrix of the game $\Gamma$. The set of correlated Nash equilibria of the game $\Gamma|\{A\}$ is the convex hull of the set of mixed equilibria of the game $\Gamma$. At the same time, as was shown in previous chapters, adding to the conspiracy space cabals that do not include all players can enrich the set of correlated Nash equilibria with points lying outside the convex hull of the set of mixed equilibria. Also, through the use of secrecy, the reserve payoffs of players can be additionally reduced if they do not have the opportunity to observe every signal.

For the proofs of the most «folk» theorem versions, the transition to more complex conspiracy spaces is probably not a big problem, as the logic of the reasoning remains the same — it is enough, if necessary, to take into account new minimax values and correlated equilibria outside the convex hull of the mixed set. Fortunately, in the context of this work, we do not even need its modern formulations — the classical, relatively weak statement is quite sufficient:

**Theorem 3.1.1.** *Let $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ be a normal form game with a finite set of outcomes, $V$ be the convex hull of the payoff vectors set of its matrix, and $\mathfrak{A} \subseteq 2^A$ be an arbitrary conspiracy space. If the payoff vector $v \in V$ strictly dominates the minimax point of the game $\Gamma|\mathfrak{A}$, then there is a discount factor $0 < \delta < 1$ such that in the infinitely repeating game $\Gamma|\mathfrak{A}$ there will be a Nash equilibrium with payoffs converging to $v$. If the vector $v$ also dominates the equilibrium minimax point of the same game, then in an infinitely repeated game with a sufficiently large discount factor, there will be a perfect subgame equilibrium with payoffs converging to $v$.*

*Доказательство.* If $A \in \mathfrak{A}$, then a sequence of sets with payoffs converging to $v$ is constructed from correlated strategies based on a public signal and directly mixing pure strategy profiles in proportions that provide the required payoff vector. If $A \notin \mathfrak{A}$, then we can use a sequence of pure strategy profiles that converges at the limit to

the same point. If any player deviates from the prescribed strategies, the rest switch to punishing him with the corresponding minimax sets of strategies. The profit of player $a$, who deviates at the $i$-th iteration in favor of the strategy $\hat{s}_i^a$, is finite and amounts to $u^a(s_i|\hat{s}_i^a) - u^a(s_i)$, so that for a sufficiently large $\delta$ the damage from the eternal punishment by the minimax for all subsequent iterations will obviously be greater. Punishment by the ordinary minimax may include strategies that are not optimal from the punishing players' point of view, so that the resulting equilibrium points are generally not subgame perfect. Punishment by the equilibrium minimax does not have this disadvantage, which means that the equilibria based on it will indeed be subgame perfect. □

For our purposes, this is enough, since we consider a repetition of the game, for which the points of the ordinary and equilibrium minimax coincide in all plot spaces. However, if the need arises, nothing prevents a similar generalization for more modern, strengthened formulations [18]. In order not to overload the work with more cumbersome reasoning, which in fact would be an almost word-for-word citation of the proofs authored by Vasin A.A., we confine ourselves to a brief retelling of their central idea. Participation in the ordinary minimax punishment of the first player deviating from the prescribed strategy can be made optimal strategy for punishers using a slightly more complex threat format. It is enough for the players to agree that the punishment of the first divergent will not be eternal, but interrupted at the moment when someone refuses to take part in it. As soon as one of the punishers deviates from the strategy prescribed by the minimax set, the previous divergent is forgiven and everyone proceeds to the same conditionally eternal punishment of the last «evader», in which everyone participates, including the just forgiven player. Thus, the process turns into something like a «tag-game», creating an effective threat of being the last to be punished, which expands the set of subgame-perfect equilibria to all points that dominate the usual minimax. Adding a conspiracy space here, again, doesn't pose much of a problem — the reasoning keeps working even when synchronization with secret signals is used in punishments.

### 3.2 Repeated three-way even-odd

You can demonstrate the application of the generalization of the «folk» theorem to games with conspiracies using the example of the same three-way even-odd (see table 1). Here $V$ is a triangle with vertices $(6, 6, 0)$, $(6, 0, 6)$ and $(0, 6, 6)$. The game has two Nash equilibrium points in pure strategies (synchronous choice of heads or tails by all players) and one additional point in mixed strategies (equiprobable independent choice between heads and tails by all players), entailing the same payoff vector $(4, 4, 4)$, which is also the minimax point of the game. Indeed, let the first player choose the strategy $(p, 1 - p)$, and the second — $(q, 1 - q)$. Then the payoffs of the third player when choosing pure strategies are:

$$u^3(p, q, 1) = 6(p + q) - 8pq;$$
$$u^3(p, q, 0) = 2(p + q) - 8pq + 4.$$

It is easy to see that

$$p \geqslant q \geqslant \frac{1}{2} \Rightarrow u^3(p, q, 1) \geqslant 4;$$
$$p \geqslant 1-q \geqslant \frac{1}{2} \Rightarrow u^3(p, q, 1) \geqslant 4;$$
$$q \geqslant p \geqslant \frac{1}{2} \Rightarrow u^3(p, q, 1) \geqslant 4;$$
$$q \geqslant 1-p \geqslant \frac{1}{2} \Rightarrow u^3(p, q, 1) \geqslant 4;$$
$$p \leqslant q \leqslant \frac{1}{2} \Rightarrow u^3(p, q, 0) \geqslant 4;$$
$$p \leqslant 1-q \leqslant \frac{1}{2} \Rightarrow u^3(p, q, 0) \geqslant 4;$$
$$q \leqslant p \leqslant \frac{1}{2} \Rightarrow u^3(p, q, 0) \geqslant 4;$$
$$q \leqslant 1-p \leqslant \frac{1}{2} \Rightarrow u^3(p, q, 0) \geqslant 4.$$

These options exhaust the entire space of possible situations, so that no combination of two players' mixed strategies can be an effective punishment for the third. Thus, in the absence of private correlation mechanisms, the folk theorem does not expand the set of solutions of the repeated even-odd in any way. However,

adding to the conspiracy space, for example, the pair $\{1,2\}$ changes the picture — correlated equilibria with payoffs $(5,5,2)$ appear in the game in a situation where all players again make an equiprobable the choice is between heads and tails, but due to the secret mechanism of correlation, the choice of players 1 and 2 is always synchronous. This reduces the reserve (in the ordinary and equilibrium sense) payoffs of player 3, giving us a new minimax point — $(4,4,2)$. In accordance with the version of the «folk» theorem formulated above, in the conspiracy space $\{\{1,2\}\}$, a repeating three-way even-odd has new subgame-perfect equilibria in a triangle with vertices $(6,4,2)$, $(4,6,2)$ and $(4,4,4)$.

Similarly, in the conspiracy space $\{\{1,2\},\{2,3\}\}$ the minimax point of the game moves to $(2,4,2)$, which expands the solution set to a flat trapezoid with vertices $(4,6,2)$, $(2,6,4)$, $(2,4,6)$ and $(6,4,2)$. Finally, the space $\{\{1,2\},\{2,3\},\{1,3\}\}$, which includes all pairwise plots, gives the minimax point $(2,2,2)$, turning the set of payoffs attainable in perfect subgame equilibria into a flat hexagon with vertices $(6,4,2)$, $(6,2,4)$, $(4,2,6)$, $(2,4,6)$, $(2,6,4)$ and $(4,6,2)$. This illustration goes well with the intuitive notion that groups of agents that have the ability to coordinate their actions in secrecy can use this as a threat to outsiders, forcing them to agree to conflict outcomes that, in the absence of collusion, would be rejected as disadvantageous. However, the effect of sensitivity to additional information asymmetry on repetitive games is not limited to this. Further, it will be shown that even in the absence of a priori information asymmetry (i.e., events external to the conflict, of which its participants are informed differently), players, limited in the complexity of the calculations they can make to select the strategies, can use the threat of artificial creation of information asymmetries with the help of specially organized joint public actions.

### 3.3 Model of repeated games accounting for the calculation costs

The construction of the desired model implies the specification of the method by which rational agents calculate the strategy of behavior. Any formalism that allows algorithmically complete calculations with probabilistic branching will do for this purpose. In addition, we need the ability to store an arbitrary internal state in memory for use at subsequent iterations and, obviously, a method for numerically estimating the complexity of the calculation performed at each iteration.

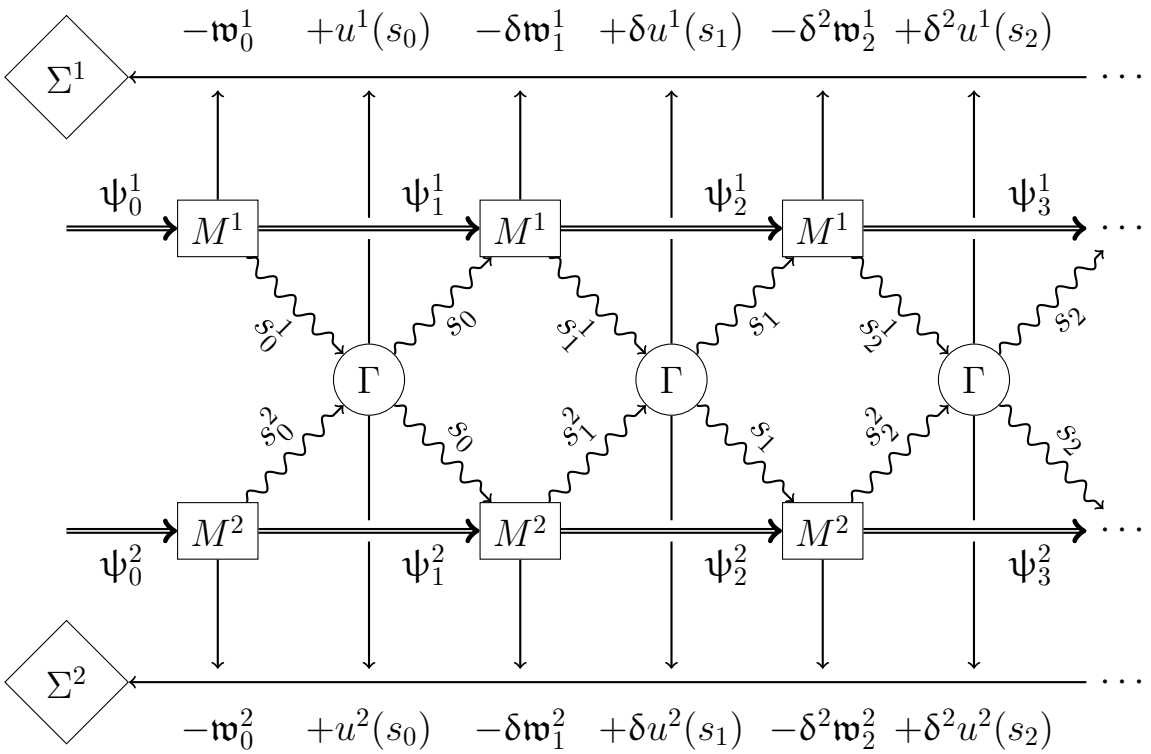


Figure 3.1 — Repeated game accounting for the calculation costs

The diagram in the figure 3.1 depicts the general scheme of interaction between agents and the environment for two players (naturally extensible to any finite number of them). At the nodes labeled with the letter $\Gamma$, successive plays of an arbitrary game $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ take place. In the $i$-th draw, player $a$ chooses his strategy $s_i^a$ by applying the probabilistic algorithm $M^a$, which is in the $\psi_i^a$ state, to the result of the previous draw $s_{i-1}$ (if there was one) and storing the results of calculations necessary for future iterations in the new state $\psi_{i+1}^a$. The $\Sigma^a$ nodes represent the successive summation of the difference between the payoff $u^a(s_i)$ and the cost of the calculation $\mathfrak{w}_i^a$, taking into account the exponentially decreasing discount factor $\delta^i$.

Since we are talking about conflicts between rational agents, it makes sense to consider only universal $M^a$ algorithms that allow us to encode any set of computable strategies for a repeated game in initial memory states $\psi_0^a$. The notation $M^a[g]$ will denote the average cost of computing an arbitrary function $g$ for its optimal implementation by $M^a$. In addition, if $\mathfrak{s}$ denotes a set of strategies for a discounted iterative game, then the notation $M^a[\mathfrak{s}]$ is suitable for denoting the cost of the total amount of computation required by player $a$ to select each move, taking into account the same coefficient $\delta$. Thus, in a repetitive game, taking into account the cost of

calculations, each player $a$ optimizes not just $u^a(\mathfrak{s})$, but

$$\hat{u}^a(\mathfrak{s}) = u^a(\mathfrak{s}) - M^a[\mathfrak{s}].$$

### 3.4 Cryptographic strategy synchronization

Although, as shown earlier, in the absence of additional information asymmetry, the three-way even-odd does not allow two players to punish the third using only mixed strategies, even in the case when players cannot use private correlation mechanisms, accounting for the cost of calculations allows in repeated games application of punishment strategies based on the achievements of modern cryptography. To demonstrate this, we need two common cryptographic primitives.

First, *distributed key-agreement protocol* [19] is needed. In cryptography, this term refers to a mechanism by which Alice and Bob can create a common secret sequence of bits, a priori having only public knowledge about the configuration and the parameters of the mechanism itself, through exchanging messages over an insecure communication channel. At the same time, Carol, having the same a priori knowledge and being able to read their messages, cannot calculate the desired secret sequence of bits, since this requires solving an algorithmically difficult problem (one that requires the number of operations that depends exponentially on the key length). For example, the family of Diffie-Hellman (hereinafter DH) protocols based on integer factorization or discrete logarithm (in a finite multiplicative group or on an elliptic curve) problems can act as such a mechanism. Let us describe the general scheme of an arbitrary DH protocol without going into technical details.

Let there be a family of bijections $f_n : \mathbb{N}_{<2^n} \leftrightarrow \mathbb{N}_{<2^n}, n \in \mathbb{N}$ that have the one-wayness property, i.e., for any universal computing device $M^*$ holds both $M^*[f_n] \in o(2^n)$ (the cost of calculating the function itself grows polynomially with $n$) and $M^*[f_n^{-1}] \in \Theta(2^n)$ (the cost of calculating the inverse function grows exponentially with $n$). In addition, let there be a family of binary functions $h_n : \mathbb{N}_{<2^n} \times \mathbb{N}_{<2^n} \to \mathbb{N}_{<2^n}$ such that

– $\forall x, y \in \mathbb{N}_{<2^n}, h_n(f_n(x), y) = h_n(x, f_n(y))$;
– $\forall x, y, z \in \mathbb{N}_{<2^n}, h_n(h_n(x, y), z) = h_n(x, h_n(y, z))$;
– $h_n(x_1, y_1) = h_n(x_2, y_2) \Rightarrow x_1 = x_2 \cap y_1 = y_2 \cup x_1 \neq x_2 \cap y_1 \neq y_2$.;

– $M^*[h_n] \in o(2^n)$.

Alice chooses a random natural number $0 \leqslant x < 2^n$ as her private key and computes $X = f_n(x)$ as her public key. At the other end, Bob similarly generates a pair of keys $y$ and $Y = f_n(y)$. Alice and Bob exchange public keys over the communication channel that Carol is listening to. Now Alice, knowing her private key $x$ and Bob's public key $Y$, can calculate $h_n(x, Y)$, and Bob, respectively, $h_n(X, y)$. Due to the properties of the function $h_n$, the values calculated by them can be considered as the desired shared secret key $K = h_n(x, Y) = h_n(X, y)$. In this case, for Carol, who knows only the public keys $X$ and $Y$, the calculation of the shared secret requires the calculation of either $f_n^{-1}(X)$ or $f_n^{-1}(Y)$. Due to the difference between the asymptotic complexity of the direct and inverse functions, it is always possible to choose $n$ such that the cost of calculating $f_n$ and $h_n$ is acceptable, while calculating $f_n^{-1}$ is prohibitively expensive. Also note that due to the associativity of $h_n$ functions can be considered polyadic, and arbitrary sized groups of agents can combine shared secret keys with publishing each member's public key — for example, $K = h_n(x, Y, Z) = h_n(X, y, Z) = h_n(X, Y, z)$ for three sides.

The second cryptographic primitive required for the punishment strategy is *cryptographically strong pseudo-random number generator* [20], henceforth referred to as CSPRNG. It can be represented as a family of functions $G_n : \mathbb{N}_{<2^n} \times \mathbb{N} \to \{0, 1\}$, whose first argument is called the seed, and the second — position. A program that calculates for a given $K \in \mathbb{N}_{<2^n}$ the successive values of $G_n(K, i), i = 1, 2, \ldots$, must perform each step over a polynomial in $n$ number of operations, while the generator must pass the test for the next bit, i.e. there must not exist an algorithm polynomially complex in $n$ that can, without knowing $K$ and having the first $i$ bits of generated sequence, to guess $G_n(K, i + 1)$ with a probability different from $\frac{1}{2}$.

Now, using the primitives described above, we can construct three new types of strategies for repeating three-way even-odd. Imagine that the players are sitting at a round table so that player 1 sits to the right of player 2, player 2 — to the right of player 3, and player 3 — to the right of player 1. Let's call the first of the new strategies $\mathfrak{s}_n^L$ «left handshake»:

1. Choose a random number $x \in \mathbb{N}_{<2^n}$.
2. Calculate $X = f_n(x)$ and represent it as a bit sequence $(X_i) \in \{0, 1\}^n$.
3. For each $i = 1 \ldots n$ play one round of the game, picking tails if $X_i = 1$ and heads otherwise. Store the strategy chosen by the player sitting on the left (with

the same comparison) as the next element of the bit sequence $(Y_i) \in \{0,1\}^n$ corresponding to the number $Y \in \mathbb{N}_{<2^n}$.

4. Calculate $K = h_n(x, Y)$.
5. Play all subsequent rounds choosing a strategy in accordance with the sequentially generated CSPRNG values $G_n(K, i), i = 1, 2, \ldots$.

We build the strategy $\mathfrak{s}_n^R$ «right handshake» in a similar way, replacing «left» with «right» and swapping $x$ with $y$, $X$ with $Y$ and $h_n(x, Y)$ with $h_n(X, y)$. These paired strategies with equal key length allow any two players to turn the first $n$ rounds of the game into a sort of «synching dance», producing a shared secret seed for a pseudo-random bit generator whose output on subsequent rounds is used as a correlation mechanism. The third player, if this occurs, has to use the $\mathfrak{s}_n^*$ «cracking» strategy to join the agreed upon choice:

1. For the first $n$ rounds, play a mixed strategy of equiprobable choice and memorize opponents' moves to get their public keys $X$ and $Y$.
2. Calculate $K = h_n(f_n^{-1}(X), Y)$ or $K = h_n(X, f_n^{-1}(Y))$.
3. Play all subsequent rounds choosing a strategy in accordance with the sequentially generated CSPRNG values $G_n(K, i), i = 1, 2, \ldots$.

We also denote the strategy $\mathfrak{s}^\varnothing$ «fold», when using which the player at each iteration simply chooses between heads and tails randomly and equiprobably. It is easy to see that if we confine ourselves to considering only the four above-listed classes of strategies, then almost all their combinations are indistinguishable in payoffs from the canonical equilibrium point in mixed strategies $u(\mathfrak{s}^\varnothing, \mathfrak{s}^\varnothing, \mathfrak{s}^\varnothing) = (4, 4, 4)$. The only exception is when any two players apply the corresponding «handshakes» to each other with the same $n$, and the third player does not apply the «cracking» with the same key length — for example, $u(\mathfrak{s}_n^L, \mathfrak{s}_n^R, \mathfrak{s}^\varnothing) = (4 + \delta^n, 4 + \delta^n, 4 - 2\delta^n)$: Here, the first two players spend their first $n$ rounds on a key exchange, which is indistinguishable from a random choice in terms of payoffs, and after that they use the common CSPRNG as a correlation mechanism, taking away half of his winnings from the third. If the third could not answer them with a «cracking» strategy, then, applying the folk theorem, profiles with two «handshakes» could be used as his punishment equilibrium. Since a mutual handshake is possible in any pair of players, cracking prohibition would provide this game with an equilibrium minimax point $(4 - 2\delta^n, 4 - 2\delta^n, 4 - 2\delta^n)$, which for $delta^n > \frac{1}{2}$ would allow, for example, to construct perfect subgame equilibria with the payoff vector $(6, 3, 3)$, which is unattainable in any single three-way even-odd Nash equilibria.

We now show how taking into account the cost of computations allows us to achieve the necessary ban on the «cracking» strategy by choosing the key length $n$ correctly. For each of the proposed strategies, we write out the discounted costs of strategy selection:

– $M^a[\mathfrak{s}^\varnothing] = 0$, since for any reasonable computing device, the basic mixed strategies can obviously be considered free or almost free;
– $M^a[\mathfrak{s}_n^L] = M^a[\mathfrak{s}_n^R] = (1-\delta)M^a[f_n] + \delta^n((1-\delta)M^a[h_n] + M_a[G_n])$, since for handshake strategies it is necessary to create a pair of keys once before the first move, after $n$ moves calculate the shared secret key, and then generate one CSPRNG bit each round;
– $M^a[\mathfrak{s}_n^*] = \delta^n((1-\delta)(M^a[f_n^{-1}] + M^a[h_n]) + M_a[G_n])$, because for the cracking strategy it is necessary to calculate the secret key once after $n$ moves, having only a pair of public keys, and then generate one bit of CSPRNG every round.

Let us now check the situation $(\mathfrak{s}_n^L, \mathfrak{s}_n^R, \mathfrak{s}^\varnothing)$ for Nash equilibrium, taking into account the cost of computations. For the first two players, it is required that the costs of cryptographic synchronization do not exceed the income from the tail of the rounds, i.e. $\frac{1-\delta}{\delta^n}M^a[f_n] + (1-\delta)M^a[h_n] + M^a[G_n] \leqslant 1$. It is easy to see that as long as $M^a[G_n] < 1$, you can always choose $\delta$ large enough to level out one-time preparatory costs. For the third player, on the contrary, it is necessary to select a sufficiently large bit length of the key so that the procedure for cracking it turns out to be more expensive than the potential income in the tail of the rounds, i.e. $(1-\delta)(M^a[f_n^{-1}] + M^a[h_n]) + M_a[G_n] \geqslant 2$. Here, the exponentially growing cost of inverting the one-way function — for $M^a[f_n^{-1}] \geqslant \frac{2}{1-\delta}$, joining the correlated strategy completely loses meaning. Thus, for the point under consideration to be a Nash equilibrium, it is sufficient that the following set of conditions be satisfied:

$$\begin{cases} (1-\delta)(\delta^{-n}M^1[f_n] + M^1[h_n]) + M^1[G_n] < 1; \\ (1-\delta)(\delta^{-n}M^2[f_n] + M^2[h_n]) + M^2[G_n] < 1; \\ (1-\delta)M^3[f_n^{-1}] \geqslant 2. \end{cases}$$

Since we are talking about comparing the performance of abstract computing devices with dimensionless quantities characterizing the preferences of rational agents, attempts to prove any formal statements regarding the compatibility of this system of inequalities seem unproductive. Nevertheless, we may still try to map the range of admissible values $n$ and $\delta$ marked out by inequations onto the corresponding objects of the real world. In practice, cryptosystems that use discrete logarithms on elliptic curves

are considered secure already with 256-bit keys (Curve25519 [21], for example), i.e. the cost of breaking them certainly exceeds the capabilities available to human civilization at the current stage of technological development. At the same time, pseudo-random number generators with 256-bit seeds exist and are widely used, while being considered cryptographically secure (CTR-DRBG [22], for example). This gives the discount factor an acceptability range of $0 < \varepsilon \leqslant 1 - \delta \leqslant \frac{1}{370}$, and since the calculation of $f_{256}^{-1}$ is currently considered impossible, $\varepsilon$ can be considered infinitely small. Thus, if players who have modern computing devices at their disposal play repeated three-way even-odd with real stakes, then the length of the series starting from several hundred rounds will be enough for the use of cryptographic strategy syncing to become a real way to gain an advantage.

### 3.5 Folk theorem for games considering the cost of computation

Using a refined version of the «folk» theorem, the trick demonstrated in the previous section can be generalized to expand the set of perfect subgame equilibria of any repeated game, individual iterations of which are sensitive to additional information asymmetry. To this end, sets correlated in a conspiracy space consisting of a single group including all players except the one being punished can be used as punishments for a player who deviates from the prescribed strategy. Since, in this case, the strategies depend on no more than one correlation mechanism, we can simplify the reasoning by passing to probability distributions on the payoff matrix. Considering the game $\Gamma = \langle A, S^a, u^a(s), a \in A \rangle$ with sets of participants $A = \{1, \ldots, m\}$ and outcomes $S = S^1 \times \ldots \times S^m$ respectively, let's introduce the notation:

$$\mathbf{P}_S = \{\mu : S \to [0,1] \mid \sum_{s \in S} \mu(s) = 1\};$$

$$\mathbf{P}_S^{\setminus a} = \{\mu \in \mathbf{P}_S \mid \forall s_1, s_2 \in S, s^a \in S^a, \mu(s_1)\mu(s_2|s^a) = \mu(s_2)\mu(s_1|s^a)\}.$$

Here $\mathbf{P}_S$ represents all possible probability measures on the set of outcomes $S$, and $\mathbf{P}_S^{\setminus a}$ — all probability measures guaranteeing the pairwise independence of the strategy choice between player $a$ and everyone else. Obviously, the payouts are calculated according to the expectation formula:

$$u^a(\mu) = \sum_{s \in S} \mu(s) u^a(s).$$

In addition, for convenience, we denote the deviation of the player $a$ in favor of the pure strategy $s_0^a$ in a similar way to the classical notation:

$$\mu|s_0^a(s) = \begin{cases} \sum_{s_*^a \in S^a} \mu(s|s_*^a), & s^a = s_0^a; \\ 0, & s^a \neq s_0^a. \end{cases}$$

Now we can finally introduce the notion of reserve payoff refined for the model under consideration:

**Definition 3.5.1.** The blind reserve payoff of player $a$ in the game $\Gamma$ is his reserve payoff $u^a(\check{\mu}^a)$ in the game $\Gamma|\{A \setminus \{a\}\}$, i.e. with a conspiracy uniting all players except him:

$$\check{\mu}^a \in \arg\min_{\mu \in \check{\mathbf{P}}} u^a(\mu),$$

where $\check{\mathbf{P}} = \{\mu \in \mathbf{P}_S^{\setminus a} \mid u^a(\mu) \geqslant u^a(\mu|s^a), \forall s^a \in S^a\}$.

For the classical folk theorem, reserve payoffs directly determine the corresponding minimax point, but in our case, things are a little more complicated. Since CSPRNGs are used to synchronize both the prescribed strategies and the punishments, the cost of calculating the sequence of pseudo-random bits required to select the strategy profile must be taken into account. Let $\mathfrak{b}(\mu) \in \mathbb{R}_{\geqslant 0}$ denote the average number of bits required to select a correlated set of strategies using the following procedure. We enumerate all outcomes $\{s_1, \ldots, s_k\} \subseteq S$ participating in $\mu$ with nonzero probability, and construct a grid of non-decreasing numbers $\rho = (\rho_0 = 0, \rho_1, \ldots, \rho_{k-1}, \rho_k = 1)$ in the unit interval $[0, 1)$ splitting it so that $\rho_j - \rho_{j-1} = \mu(s_j), j = \overline{1,k}$.

1. Let $\mathcal{X}_{min} = 0$ and $\mathcal{X}_{max} = 1$.
2. Check if there is $j$ such that $\rho_{j-1} \leqslant \mathcal{X}_{min} < \mathcal{X}_{max} \leqslant \rho_j$. If there is, we stop the algorithm by settling on the choice of the strategic profile $s_j$.
3. Generate the next bit of the pseudo-random sequence. The value $\frac{\mathcal{X}_{min}+\mathcal{X}_{max}}{2}$ in the case of $0$ is assigned to the variable $\mathcal{X}_{max}$, and in the case of $1$ — to the $\mathcal{X}_{min}$.
4. Move back to step 2.

If all players use a CSPRNG with the same seed, it is obvious that they will end up in the same strategy profile utilizing the same number of pseudo-random bits, depending on the average only on the probability distribution $\mu$. Therefore, the expected income of player $a$, taking into account the cost of calculations, can be represented as $u^a_{M,n}(\mu) = u^a(\mu) - \mathfrak{b}(\mu)M^a[G_n]$, where $M^a[G_n]$ is the cost of generating one pseudo-random bit. Note that the value obtained also depends on $n$, i.e. the bit length of the

used CSPRNG seed, which begs to replace the concept of a minimax point with a more complex definition:

**Definition 3.5.2.** A probability distribution $\mu$ on the set of outcomes in normal form game $\Gamma = \langle A, S^a, u^a(s), a \in A \rangle$ is called $M$,$n$-acceptable if $u^a_{M,n}(\mu) > u^a(\breve{\mu}^a)$ for each player $a \in A$.

Note that we have so far talked about how players use CSPRNGs with a common seed to synchronize their actions, without specifying how exactly this common seed is generated. Similar to the example from the previous section, in this guise we will use the shared secret keys calculated using the DH protocol. Let us describe the procedure for generating and publishing keys. First, each player $a$ chooses a random real number $\chi^a$ uniformly distributed over the range $[0, 2^n)$. The rounding of this number $x^a = \lfloor \chi^a \rfloor \in \mathbb{N}_{<2^n}$ is used by him as a private key. Using a one-way function, the player calculates the public key $X^a = f(x^a) \in \mathbb{N}_{<2^n}$. To exchange $X^a$ values, players can use any distinctive *totally mixed* strategy profile:

**Definition 3.5.3.** A mixed strategy profile is said to be totally mixed when it does not contain a single pure strategy.

Since $f$ is a bijection, the random variable $\mathcal{X}^a = \chi^a - x^a + X^a$ is also uniformly distributed in the range $[0, 2^n)$. In order to reveal his value of $X^a$ to other players, each player uses the «fractal» method of encoding the number $\mathcal{X}^a$ in the sequence of moves he makes, indistinguishable in probability distribution from a mixed strategies $s^a_0 = (p^a_1, \ldots, p^a_{|S^a|})$ from the distinctive totally mixed profile $s_0$. Let us construct in the unit interval $[0, 1)$ a grid of non-decreasing numbers $\rho^a = (\rho^a_0 = 0, \rho^a_1, \ldots, \rho^a_{|S^a|-1}, \rho^a_{|S^a|} = 1)$ splitting it in such a way that $\rho^a_j - \rho^a_{j-1} = p^a_j, j = \overline{1,|S^a|}$. This allows the following encoding algorithm to be applied:

1. Before making the first move, other players know that $\mathcal{X}^a$ is uniformly distributed in the interval $[0, 2^n)$. Let $\mathcal{X}^a_{min} = 0$ and $\mathcal{X}^a_{max} = 2^n$.
2. Let us scale $\rho^a$ over the interval $[\mathcal{X}^a_{min}, \mathcal{X}^a_{max})$, getting the embedded in it mesh $\mathcal{P}^a = (\mathcal{X}^a_{min}(1 - \rho^a_j) + \mathcal{X}^a_{max}\rho^a_j, j = \overline{0, |S^a|})$.
3. At the next iteration, choose $s^a_j$ such that $\mathcal{P}^a_{j-1} \leqslant \mathcal{X}^a < \mathcal{P}^a_j$.
4. Now the other players know that $\mathcal{X}^a$ is uniformly distributed over the interval $\left[\mathcal{P}^a_{j-1}, \mathcal{P}^a_j\right)$. Let's go back to step 2 by setting $\mathcal{X}^a_{min} = \mathcal{P}^a_{j-1}$ and $\mathcal{X}^a_{max} = \mathcal{P}^a_j$.

This algorithm can be executed indefinitely, gradually decreasing the other players' lack of knowledge about the value of $\mathcal{X}^a$. Moreover, at each individual

iteration, the distribution of outcome probabilities is indistinguishable from the set of mixed strategies $s_0$. At the moment when the inequality $X^a \leqslant \mathcal{X}^a_{min} < \mathcal{X}^a_{max} \leqslant X^a + 1$ begins to hold, other players gain confidence about the value of $X^a$, and the public key of player $a$ is reputed as published. If all players start publishing keys at the same time, then the expected number of iterations until the publication of the last one is completed depends only on the utilized strategy profile $s_0$ and the value of $n$, so it can be denoted by the symbol $\mathrm{t}(s_0, n) \in \mathbb{N}$.

Before proceeding to the analogue of the folk theorem for repeated games, taking into account the cost of calculations, it is necessary to introduce one more notation. The vector $\Delta u = (\Delta u^a, a \in A) \in \mathbb{R}^m_{\geqslant 0}$, where

$$\Delta u^a = \max_{s \in S, s^a_* \in S^a} (u^a(s|s^a_*) - u^a(s)),$$

consists of the maximum income that each player can receive by deviating from a strategy out of arbitrary prescribed profile.

**Theorem 3.5.1.** *Let $\Gamma = \langle A, S^a, u^a(s), a \in A\rangle$ be an arbitrary matrix game of $m$ players that has at least one totally mixed equilibrium $s_0$. Let $M = (M^1, \ldots, M^m)$ be a collection of universal computing devices that the respective players can use to select the next step of a strategy in a repeated game. Let $(\Gamma)^\delta_M$ be an infinitely repeated game with $\Gamma$ iteration, $\delta$ discounting factor and taking into account the cost of operating computing devices $M$. Any $M$,$n$-acceptable probability distribution $\mu$ on the set of the game $\Gamma$ outcomes can be associated with a strategy profile for the game $(\Gamma)^\delta_M$ with the payoffs of each player $a$ equal to*

$$(1 - \delta^{\mathrm{t}(s_0,n)})u^a(s_0) + \delta^{\mathrm{t}(s_0,n)} u^a_{M,n}(\mu) - (1 - \delta)(M^a[f_n] + \delta^{\mathrm{t}(s_0,n)}(m-1)M^a[h_n]).$$

*Upon that, in order for this profile to be a Nash equilibrium, it is sufficient to satisfy the following conditions for each $a \in A$:*

1. $(1 - \delta)(M^a[f_n] + \delta^{\mathrm{t}(s_0,n)}(m-1)M^a[h_n]) < \delta^{\mathrm{t}(s_0,n)}(u^a_{M,n}(\mu) - u^a(\check{\mu}^a))$;
2. $(1 - \delta)\Delta u^a < \delta(u^a_{M,n}(\mu) - u^a(\check{\mu}^a))$;
3. $(1 - \delta)M^a[f_n^{-1}] > \delta\Delta u^a$.

*Proof.* The equilibrium corresponding to the $M$,$n$-acceptable probability distribution $\mu$ is constructed as a three-stage process:

– *Synchronization.* First, each player $a$ creates a key pair of length $n$, incurring a loss equal to $(1-\delta)M^a[f_n]$. Then, using the fractal coding algorithm described above over a totally mixed equilibrium $s_0$, he publishes his public key. This

phase continues until all keys have been published, which takes $\mathfrak{t}(s_0, n)$ moves on average, giving a total payoff of $(1 - \delta^{\mathfrak{t}(s_0,n)})u^a(s_0)$. The stage ends with the calculation of the shared secret key, for which the function $h_n$ needs to be calculated $m - 1$ times by each player, which corresponds to a loss of $(1 - \delta)\delta^{\mathfrak{t}(s_0,n)}(m-1)M^a[h_n]$.

– *Playout.* Using a CSPRNG initiated by a shared secret, the players at each iteration pseudo-randomly choose a new pure strategy profile according to the distribution $\mu$, so that each player $a$ gets on infinite repetition the expected total payoff $\delta^{\mathfrak{t}(s_0,n)}u^a_{M,n}(\mu)$. If none of the players deviated from the prescribed behavior either at the previous stage or at this stage, then the final payoffs in the limit correspond to those predicted in the statement of the theorem.

– *Punishment.* If any of the players in the playout phase choose a pure strategy that does not align with the prescribed by CSPRNG, the other players switch to his punishment mode. The same thing happens immediately after the synchronization stage, if through it one of the players ignores the key generation procedure. To do this, they calculate a new shared secret key, this time excluding the public key of the penalized player $a$. Initiating the CSPRNG with this new key, they pseudo-randomly select a new pure strategy profile at each iteration according to the $\breve{\mu}^a$ distribution.

Several kinds of individual deviations are possible from this scheme of prescribed actions. First, at the synchronization stage, any player $a$ can try to cut corners by forgoing creation of a key pair and calculation of a shared secret key. Since the profile $s_0$ is a Nash equilibrium, it is not possible to improve the payoff comparing to $(1 - \delta^{\mathfrak{t}(s_0,n)})u^a(s_0)$, but you can use a simple mixed strategy instead to avoid cryptography costs of $(1-\delta)(M^a[f_n] + \delta^{\mathfrak{t}(s_0,n)}(m-1)M^a[h_n])$. The reaction to this decision is the transition of the other players to the stage of player $a$ punishment immediately after the publication of the keys is completed, so that instead of $\delta^{\mathfrak{t}(s_0,n)}u^a_{M,n}(\mu)$ at the end of the round, the player receives $\delta^{\mathfrak{t}(s_0,n)}u^a(\breve{\mu}^a)$. Such a deviation is made unfavorable by the restriction on $\delta$ imposed by condition 1 of the statement of the theorem.

Secondly, at the main stage of the playout, any player $a$ can, having calculated the next pseudo-random profile $s_i$, refuse to play the prescribed strategy $s^a_i$ in favor of a more profitable one, receiving a one-time income not exceeding $(1-\delta)\delta^i\Delta u^a$. Noticing this, the rest of the players go to the punishment stage, which reduces his income in the tail of the draw from $\delta^{i+1}u^a_{M,n}(\mu)$ to $\delta^{i+1}u^a(\breve{\mu}^a)$. Such a deviation is made unfavorable by the restriction on $\delta$ imposed by condition 2 of the statement of the theorem.

Third, since blind punishments rely on the fact that punished player $a$ cannot predict the bits of a CSPRNG initiated by a shared secret that was computed without using his own key pair, he can try to weaken the punishment by «cracking» the secret key by invoking a one-way function on one of the public keys. If this happens at the $i$-th iteration of the game, then he must spend $(1-\delta)\delta^i M^a[f_n^{-1}]$ on it, receiving at most $\delta^{i+1}\Delta u^a$ of income from the playout tail. Such a deviation is made unfavorable by the restriction on $\delta$ imposed by condition 3 of the theorem statement.

Thus, the prescribed procedure for playing the infinitely repeated game $(\Gamma)_M^\delta$ actually turns out to be a Nash equilibrium with the required expected payoffs. □

It is easy to see that the proved assertion is rather analogous to the very first formulations of the «folk» theorem, in which the subgame-perfect equilibria were not yet discussed. Alas, the application of methods by which perfect subgame equilibria are constructed in the conventional case becomes difficult for objective reasons, when we start taking into account the cost of calculations. As already mentioned at the beginning of the chapter, a scheme of endless punishment of the last deviant from the prescribed strategy, which is also used in the process of punishing the previous deviant, is a most common method. Here such a naive approach runs into an obstacle — consider the situation in which player $a$ decided to cut corners on creating keys and instead of the prescribed procedure at the synchronization stage, he simply played the mixed strategy $s_0^a$. Noticing this, the other players, upon completion of key exchange begin his blind punishment with the correlated strategy profile $\breve{\mu}^a$. Now imagine what happens if one of the punishers decides at the next iteration to use a strategy that is more beneficial for himself than the CSPRNG prescribes as a punishment. Such a player must himself be punished starting from the next iteration, and player $a$ should also take part in his punishment. However, since player $a$ saved on creating his key pair, he simply does not have the ability to calculate the shared secret key required for it, so any punishment he must participate in ceases to be an effective threat.

Another noticeable drawback of the proved theorem is that it implicitly relies on the observability of the strategies used by the players. It is understood that the only secret that players hide from their opponents is the specific values of the keys, while the algorithms they use are publicly known. However, the claim could become much stronger and more convincing if we considered only the specific pure strategies played by the participants to be publicly known. This matters, for example, when we say that a player who decides to cut corners on creating keys is subject to punishment at the end

of the synchronization stage, because if players can judge whether someone created keys or not, only by the moves they make, then during some number of first iterations of the playout stage, the deviant could randomly guess which strategy the CSPRNG prescribes, even without a shared secret key, by simply choosing the most probable strategy according to the $\mu$ distribution. Moreover, if the $\mu$ distribution is such that someone must play the same pure strategy in it with a probability of $1$, then it does not make sense for him to create keys at all, since forgoing their creation will never be disclosed.

The same vulnerability can be exploited in an even more subtle way if player $a$'s income from the synchronizing mixed strategy profile $s_0$ exceeds his income from the target distribution $\mu$. If, instead of randomly choosing the value of $\chi^a$, when creating keys, the player will «tamper» with its fractional part so that it approaches $0$ or $1$, then thereby he can arbitrarily increase the duration of the synchronization stage and, accordingly, his total income. The described problems arising from the rejection of the algorithms' observability by the other players can hardly be called insurmountable, however, attempts to solve them within the framework of this study would significantly complicate the formal reasoning, without adding anything valuable to understanding its central ideas.

In addition, one should pay attention to the fact that since the conditions of the theorem limit the value of the discount coefficient $\delta$ both from below and from above, it cannot be formulated in a more elegant form for arbitrarily small $\varepsilon$-approximations to the payout vector $u_{M,n}(\mu)$. However, we can map its parameters to real world objects in order to be able to judge its practical implications. Let's imagine that the collection $M$ of computing devices used by the players consists of modern processing units, and $n = 256$, which coincides with the most common key length in modern cryptography. For well-chosen[1] mixed equilibrium $s_0$, we can expect that the average duration of the key exchange stage $\mathfrak{t}(s_0, n)$ will coincide in order of magnitude with the value of $n$, that is, measured in hundreds of iterations, which means that in a series of draws with at least one hundred thousand significant iterations, the contribution of the synchronization stage will certainly not exceed one percent of the final result. Given that, for example, systems for automated stock trading can easily make hundreds of thousands of transactions per day, for many practical applications this can be considered a good approximation.

[1] This assumes that none of the players selects one of his pure strategies with a probability close to $1$.

Further, about the cost of calculating the functions used to generate the shared secret keys, i.e. $M^a[f_{256}]$ and $M^a[h_{256}]$ — although it cannot be considered negligible, but as an estimate it can be noted that each opening of a web page by a modern browser in the vast majority of cases implies generation of several key pairs and corresponding shared secret keys. Finally, the cost of generating pseudo-random sequences by modern CSPRNG, i.e. $M^a[G_{256}]$ on a scale of millions of bits can already be considered negligible, since, say, rendering an image from a video card to a modern computer monitor via the digital HDMI interface implies encryption of a stream measured in tens of gigabits per second, while the algorithm used in this encryption process can also be used to generate pseudo-random sequences.

Finally, it remains to note that the inversion of a one-way function with a 256-bit argument is currently considered impossible and is expected to remain so until the creation of functioning quantum computers. This means that the value of $M^a[f_{256}^{-1}]$ for practical applications can be considered almost infinite, which allows $\delta$ to approach $1$ by an arbitrarily small (in the sense of real conflicts) distance.

## 3.6 Generalization of results, prospects and suppositions

In order to appreciate the significance of this phenomenon, one should drop back a couple of steps from the specifics of the described game and try to glance over the larger picture. First, by generalizing the folk theorem, it becomes clear that the three-way even-odd itself is nothing more than a relatively arbitrarily constructed example of a game that is sensitive to additional information asymmetry. The cryptographic punishment strategies described above use virtually no other properties of a given conflict, and there is no reason to think that they cannot be generalized to many other games that exhibit the same property. For example, if we take the game $\Gamma_n^3$ from the second chapter of this work as a single iteration, then it turns out that when it is repeated, it is possible to encode public keys in a similar way with an alphabet consisting of $n$ characters according to the number of computers in the computer center, and then use the resulting shared secret key as the seed of the generator, pseudo-randomly choosing from same $n$ elements.

Secondly, it makes sense to ask whether the described scheme of cryptographic punishment strategies exhausts all possibilities for expanding the set of perfect subgame

equilibria. Common sense suggests that it is not, at least because both cryptographic primitives used here (the distributed key-agreement protocol and the cryptographically secure pseudo-random number generator alike) have many implementations based on a variety of mathematical formalisms, the list of which is replenished year by year due to the rapid developments in the relevant areas of knowledge. Moreover, building a punishment strategy from the DH protocol followed by utilizing the resulting key as a CSPRNG seed is itself quite arbitrary — we used tools that were originally created in a completely different context for other purposes, simply because they already exist and have proven properties convenient for solving our problem.

These considerations allow us to reasonably assume that both the three-way even-odd itself and the presented cryptographic punishment strategies are just the most obvious representatives of a wider class of mathematical formalisms that have not yet been explored. In the most general terms, rational agents, participating in repeated conflicts, can develop secret correlated strategies of behavior, using only specially selected public actions and observing a similarly acting counterparty. The secrecy is ensured due to the fact that joining the correlation requires cognitive efforts that exceed capabilities of any third party observing the same sequence of public actions. In addition, generalizing the relationship between the normalized cost of computation and the required key length, it can be assumed that the more cognitive effort the party from which the conspirators are trying to hide their shared strategy can apply, the more difficult this process is and the less income (due to the growing discounting in the tail rounds) brings such secrecy.

Indeed, if we imagine ordinary people playing a game sensitive to additional information asymmetry without the use of special technical means, we can hardly expect that they will perform the mental calculations necessary for the DH+CSPRNG routine. At the same time, it is likely that there are ubiquitous examples of how people can achieve the necessary secret synchronization unconsciously, perceiving the result as a self-evident, self-explanatory fact. In this case, we think of experienced gamblers who specialize in complex intellectual games, such as bridge or preference. Among them, it is considered undeniable that, in addition to individual skills, the outcome of the draws is strongly influenced by the joint playing experience — a pair of players who individually are no great shakes can turn out to be formidable opponents if they have many games at the same table behind them. If the above assumptions about the rather general nature of the constructed model are correct, then the phenomenon of such «cohesion» can find a satisfactory explanation within its framework.

It should be noted that while aiming to analyze from this point of view the strategies of players in already existing parlor games, we may encounter difficulties related to the fact that the rules of those that can be suspected of being sensitive to additional information asymmetry are complex even without taking into account this property. For example, bridge or preference will obviously remain very non-trivial, even if you play them in separate draws, each time choosing the composition of anonymous participants randomly from a large pool of candidates (remotely over the network, for example). To facilitate the task of future researchers, it would be nice to design a special card game in which the use of the «cohesion» effect would be a necessary element of any successful strategy. An attempt to create such a new game called «Tesseract» is in the Appendix Г — hopefully in the future it will be useful for both scientific and entertainment purposes.

It would be fancy to complete this work by formulating a rather bold informal hypothesis that continues the line of reasoning of the last chapter in line with population games:

**Conjecture 3.6.1.** If conflict situations, the model of which is sensitive to additional information asymmetry, periodically (many times during the life of one individual) arise in a population and the probability of the genus proliferation by individual specimens significantly depends on their success in these conflicts, then evolutionary pressure on the population fortifies traits that contribute to an increase in the cognitive potential of the next generations (understood in a general sense as the ability to perform Turing-complete calculations on arbitrary data).

If this hypothesis is correct, then the sensitivity of games to additional information asymmetry may turn out to be the «Holy Grail» of evolutionary game theory — a factor that generates an unrestrained arms race in the field of complex behavior abilities. Any games with this property, even being very simple on its own, encourage the cognitive potential of participants with the need to build and unravel conspiracies, and therefore its study can both enrich our understanding of the intelligence evolution in our ancestors, and become a tool for improving artificial intelligence technologies.

## Conclusion

The main results of the work are as follows.

1. Based on the analysis of the correlated equilibrium concept in the context of multilateral conflicts, the sensitivity of games to additional information asymmetry property was formulated.
2. The study of the correlation spaces isomorphism made it possible to narrow them through introduction of the conspiracy space formalism, with the use of which it is convenient to argue about the influence of additional information asymmetry on game solutions.
3. Modeling the task scheduling problem under the assumption of non-monotonicity of the returns functions showed that in conspiracy spaces the concept of structurally coherent equilibria can be used as a functional substitute for the application of the conventional collective rationality criteria to Nash equilibria in mixed strategies.
4. To demonstrate the significance of the game sensitivity to additional information asymmetry phenomenon, a model of repeated conflicts was built taking into account the cost of calculating the next step of the strategy.
5. Within the framework of the constructed model, it was shown how in repeated games even without actual additional information asymmetry it is possible to use modern cryptographic primitives to construct effective punishment strategies that use sensitivity to it.

Hopefully, this work will draw the attention of specialists to the problem of the influence of additional information asymmetry on the outcomes of multilateral conflicts.

In conclusion, the author expresses his gratitude and great appreciation to the research advisor Vasin A. A. for support, assistance, discussion of the results and scientific guidance. The author also thanks Morozov V. V. for active participation in the work on proofs of theorems and the authors of the template *Russian-Phd-LaTeX-Dissertation-Template* for their contribution in preparing the dissertation layout.

## Glossary

**correlation space** : An additional parameter of the correlated extension of normal form games, characterizing the players' a priori knowledge about events that do not directly affect the outcome of the conflict

**conspiracy space** : Correlation space of a special structure with a simple finite description as a family of player groups called conspiracies

**conspiracy** : A subset of players united by the ability to observe a common secret correlation mechanism whose signals are unpredictable to outsiders

## Bibliography


1. *Aumann, R. J.* Subjectivity and correlation in randomized strategies [Text] / R. J. Aumann // Journal of Mathematical Economics. — 1974. — Mar. — Vol. 1, no. 1. — P. 67—96.
2. *Nikolenko, S.* Theory of economic mechanisms: textbook [In Russian] / S. Nikolenko. — Moscow: Internet University of Information Technologies BINOM. Knowledge Laboratory, 2009. — (Fundamentals of Economics and Management).
3. *Fudenberg, D.* The Folk Theorem in Repeated Games with Discounting or with Incomplete Information [Text] / D. Fudenberg, E. Maskin // Econometrica. — 1986. — Vol. 54, no. 3. — P. 533—554.
4. *Savchenko, M. A.* Partially correlated equilibria in competition game models [In Russian] / M. A. Savchenko, A. A. Vasin // Lomonosov Readings 2017. — 2017.
5. *Savchenko, M. A.* Influence of additional information asymmetry on game solutions [In Russian] / M. A. Savchenko // Lomonosov Readings 2021. — 2021.
6. *Savchenko, M. A.* Axiomatic approach to conspiracy theory [Text] / M. A. Savchenko // IX Moscow International Conference on Operations Research (ORM2018): Moscow, October 22–27, 2018: Proceedings. — 2018.
7. *Savchenko, M. A.* Computational complexity of strategies in repeated games sensitive to additional information asymmetry [Text] / M. A. Savchenko // Conference of Young Scientists on Mathematical Economics and Economic Theory. — 2021.
8. *Savchenko, M. A.* Normative conspiracy theory [In Russian] / M. A. Savchenko // Mathematical Game Theory and its Applications. — 2020. — V. 12, No. 1. — S. 33—59.
9. *Savchenko, M. A.* Card game "Tesseract" [In Russian] / M. A. Savchenko // Mathematical Game Theory and its Applications. — 2021. — T. 13, No. 3. — P. 58—74.

10. *Savchenko, M. A.* Task scheduling with nonmonotonic returns [In Russian] / M. A. Savchenko // Mathematical Game Theory and its Applications. — 2022. — T. 14, No. 1. — P. 85—101.

11. *Savchenko, M. A.* Normative Conspiracy Theory [Text] / M. A. Savchenko // Automation and Remote Control. — 2021. — Vol. 82, no. 4. — P. 706—721.

12. *Kolmogorov, A.* Basic concepts of probability theory [In Russian] / A. Kolmogorov. — 2nd ed. — M.: Nauka, 1974.

13. *Bogachev, V.* Fundamentals of measure theory [In Russian]. T. 1 / V. Bogachev. — Moscow-Izhevsk: Research Center "Regular and Chaotic Dynamics", 2003.

14. *Koutsoupias, E.* Worst-Case Equilibria [Text] / E. Koutsoupias, C. Papadimitriou // STACS 99. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1999. — P. 404—413.

15. *Agussurja, L.* The Price of Stability in Selfish Scheduling Games [Text] / L. Agussurja, H. Lau //. Vol. 7. — 12/2007. — P. 305—311.

16. *Aumann, R. J.* Acceptable points in general cooperative *n*-person games [Text] / R. J. Aumann // Annals of Mathematics Studies. — 1959. — Vol. 40. — P. 287—324.

17. *Bernheim, B.* Coalition-Proof Nash Equilibria I. Concepts [Text] / B. Bernheim, B. Peleg, M. D. Whinston // Journal of Economic Theory. — 1987. — Vol. 42, no. 1. — P. 1—12.

18. *Vasin, A.* The Folk theorem for dominance solutions [Text] / A. Vasin // International Journal of Game Theory. — 1999. — Vol. 28, no. 1. — P. 15—24.

19. *Boyd, C.* Protocols for Authentication and Key Establishment [Text] / C. Boyd, A. Mathuria. — Springer, 2003. — (Information Security and Cryptography).

20. *Gutmann, P. C.* Software Generation of Practically Strong Random Numbers [Text] / P. C. Gutmann // USENIX Security Symposium. — 1998.

21. *Bernstein, D. J.* Curve25519: New Diffie-Hellman Speed Records [Text] / D. J. Bernstein // Public Key Cryptography – PKC 2006. — Berlin, Heidelberg : Springer, 2006. — P. 207—228.

22. *Hoang, V. T.* Security Analysis of NIST CTR-DRBG [Text] / V. T. Hoang, Y. Shen // Advances in Cryptology – CRYPTO 2020 / ed. by D. Micciancio, T. Ristenpart. — Cham : Springer International Publishing, 2020. — P. 218—247.

23. *Myerson, R. B.* Optimal coordination mechanisms in generalized principal–agent problems [Text] / R. B. Myerson // Journal of Mathematical Economics. — 1982. — Vol. 10, no. 1. — P. 67—81.

24. *Myerson, R. B.* Multistage Games with Communication [Text] / R. B. Myerson // Econometrica. — 1986. — Vol. 54, no. 2. — P. 323—358.

25. *Aumann, R. J.* Correlated Equilibrium as an Expression of Bayesian Rationality [Text] / R. J. Aumann // Econometrica. — 1987. — Vol. 55, no. 1. — P. 1—18.

26. *Dhillon, A.* The Folk Theorem in Repeated Games with Discounting or with Incomplete Information [Text] / A. Dhillon, J. F. Mertens // Journal of Economic Theory. — 1996. — Vol. 68, no. 2. — P. 279—302.

27. *Hart, S.* A Simple Adaptive Procedure Leading to Correlated Equilibrium [Text] / S. Hart, A. Mas-Colell // Econometrica. — 2000. — Vol. 68, no. 5. — P. 1127—1150.

28. *Engelking, R.* General topology [In Russian] / R. Engelking. — M.: Mir, 1986.

## List of Figures

# Appendix A

## A brief review of the literature on the correlated extension of normal form games

The concept of correlated extension has become an important tool commonly used in many areas of game theory, and in particular the famous mechanism design relies on it. In this regard, one cannot fail to mention the article by Roger Myerson «Optimal coordination mechanisms in generalized principal-agent problems» [23]. In it, a generalized principal-agent problem is formulated, in which agents have both secret information and the ability to make decisions beyond the control of the principal. It is shown that the principal can be limited to incentive-compatible direct coordination mechanisms, in which agents report their information to the principal, who recommends in response strategies that form a correlated equilibrium. In the finite case, optimal coordination mechanisms can be found using linear programming. In addition, the problems of systems with many principals in which a non-cooperative equilibrium may not exist are discussed, so that a definition of a quasi-equilibrium is introduced and its existence is demonstrated.

Correlated extension has found its place also in relation to the study of expanded form games. Another article by Roger Myerson «Multistage Games with Communication» [24] deals with multi-stage games with a communication mechanism that operates on the principle of a centralized intermediary. In a communication equilibrium, no player should be able to single-handedly increase their payoff by manipulating their reports or actions. Sequential communication equilibrium is a communication equilibrium with a system of conditional probabilities under which no player can benefit from such manipulations, even if events of zero probability occur. Codominated actions are defined in such a way that any communication equilibrium is sequential if and only if no one uses codominated actions. The prevailing communication equilibrium is defined as the result of the successive exclusion of codominated actions, and its existence is demonstrated.

Another important milestone was the article «Correlated equilibrium as an expression of Bayesian rationality» [25], in which Aumann showed that the formalism of correlated equilibrium removes the contradiction between «Bayesian» and «game-theoretical» world-view. From a Bayesian perspective, probabilities can be assigned to anything, even the chance for a player to choose some strategy in a certain

game. From the viewpoint of game theory itself, on the contrary, it is traditionally believed that one cannot talk about the probabilities of events occurring at the will of rational agents, so one must instead use the concept of equilibrium (or other game-theoretic constructs). The proposed formalism combines these two stances — correlated equilibrium can be viewed as a consequence of Bayesian rationality, since the equilibrium condition is a simple profit maximization by each of the players, taking into account the information known to them. This approach does not require explicit randomization in the actions of the players. Even if a player chooses a specific pure strategy without an element of chance, the probabilistic nature of the strategies reflects the uncertainty of other players in his choice, which is shown in the examples.

Questions of compatibility of correlated equilibria with more stringent principles of optimality were raised in the article «Perfect Correlated Equilibria» [26] by Amrita Dhillon and Jean Francois Mertens. It introduces the notion of $(\varepsilon)$-perfect correlated equilibria (PCE) resulting from $(\varepsilon)$-perfect equilibrium of some correlation device. It is shown that the «revealing principle» for this concept is no longer valid — the direct mechanism may not provide perfect equilibrium. The so-called approximately perfect correlated equilibria (APCE) turn out to be the limits of $\varepsilon$-PCE, and the authors reach for them for a complete characterization. In the course of reasoning about APCE «acceptability» in a certain sense, however, illustrated arguments are given in favor of PCE seeming to be «good» among them.

The dynamic aspect of the correlated extension formalism also did not go unnoticed by researchers. Many procedures have been proposed for playing iterative games that ensure convergence to correlated equilibria. Among the many works on this topic, the article by Sergiu Hart and Andreu Mas-Colella «A simple adaptive procedure leading to correlated equilibrium» [27] stands out, in which the authors proposed the so-called regret-matching procedure. Applying it, the players each time deviate from their current strategies in proportion to the extent of the damage they suffered on previous moves from not using other strategies. It is shown that such an adaptive procedure guarantees in any game the convergence with probability 1 of the empirical distribution of play to the set of correlated equilibria.

## Appendix Б

### Proof of the theorem on the isomorphism of correlation spaces[1]

To prove the theorem on isomorphic spaces, we have to introduce additional tools.

**Definition Б.0.1.** A refinement of a set $X = X^1 \times \ldots \times X^m$ of outcomes to a finite set $Y = Y^1 \times \ldots \times Y^m$ of outcomes is any mapping $\rho = (\rho^1, \ldots, \rho^m)$, where each component $\rho^a$ takes $Y^a$ to $X^a$.

Using refinements, one can specify connections between partitions with different codomains. If partitions $f : \Omega \to X$ and $g : \Omega \to Y$ are such that $f = \rho \circ g$, then $f^{-1}(x) = \bigcup_{y \in \rho^{-1}(x)} g^{-1}(y), \forall x \in X$. In this case, $f$ is said to be refinable to $g$.

Partitions of one and the same space can be combined. For example, of the partitions $g_i : \Omega \to Y_i = Y_i^1 \times \ldots \times Y_i^m, i = \overline{1,n}$, one can construct their combination $g_1 \diamond \ldots \diamond g_n : \Omega \to Y_{(n)}$, where $Y^a_{(n)} = Y_1^a \times \ldots \times Y_n^a$ and $(g_1 \diamond \ldots \diamond g_n)^a(\omega) = (g_1^a(\omega), \ldots, g_n^a(\omega)), \forall \omega \in \Omega, a = \overline{1,m}$. This combination of partitions is related to its components via refinement-projections: $g_i = \pi_i \circ (g_1 \diamond \ldots \diamond g_n), \pi_i^a(x_1^a, \ldots, x_n^a) = x_i^a$.

Refinements with a common codomain can be combined in a similar way. For example, from the refinements $\rho_i : Y_i \to X, i = \overline{1,n}$, one can construct a combination $\rho_1 \wr \ldots \wr \rho_n : Y_{[n]} \to X$, where $Y^a_{[n]} = \{(y_1^a, \ldots, y_n^a) \in Y^a_{(n)} \mid \rho_1^a(y_1^a) = \ldots = \rho_n^a(y_n^a)\}, a = \overline{1,m}$, and $\rho_1 \wr \ldots \wr \rho_n$ coincides on the domain of itself with all $\rho_i \circ \pi_i$. Note that

$$f = \rho_i \circ g_i, i = \overline{1,n} \;\Leftrightarrow\; f = (\rho_1 \wr \ldots \wr \rho_n) \circ (g_1 \diamond \ldots \diamond g_n).$$

**Definition Б.0.2.** In a correlation space $\Phi = \langle A, \Omega, \mathfrak{I}^a, \mathbb{P}, a \in A \rangle$, the structure of partition $f : \Omega \to X$ generated by a refinement $\rho : Y \to X$ is the set $H_{\Phi,\rho}(f) = \{\mathbb{P} \circ g^{-1} \mid g \models \Phi, f = \rho \circ g\}$ consisting of the measures $\mu : Y \to \mathbb{R}_{\geqslant 0}$. We also set $H^{-1}_{\Phi,\rho}(\mu) = \{f \models \Phi \mid \mu \in H_{\Phi,\rho}(f)\}$.

**Lemma Б.0.1.** *For all $\rho : Y \to X$ and $\mu : Y \to \mathbb{R}_{\geqslant 0}$, the set $H^{-1}_{\Phi,\rho}(\mu) \subseteq X^\Omega$ is compact in the semimetric*

$$\operatorname{dis}(f_1, f_2) = \frac{1}{2} \sum_{x \in X} \left| \mathbb{P}(f_1^{-1}(x)) - \mathbb{P}(f_2^{-1}(x)) \right|.$$

[1] Quoted from the article [11].

*Доказательство.* Let us restate $H^{-1}_{\Phi,\rho}(\mu) = \rho \circ H^{-1}_{\Phi}(\mu)$ by defining $H^{-1}_{\Phi}(\mu) = \{g \models \Phi \mid \mathbb{P} \circ g^{-1} = \mu\}$. First, we prove the compactness of $H^{-1}_{\Phi}(\mu)$ by introducing $\mathrm{dis}(g_1, g_2)$ by analogy with $\mathrm{dis}(f_1, f_2)$. The semimetric $\mathrm{dis}$ is completely bounded, because $\mathrm{dis}(g_1, g_2) = d(\mu_1^Y, \mu_2^Y)$, where $\mu_k^Y = \mathbb{P} \circ g_k^{-1}, k = 1{,}2$, and the space of probability measures is completely bounded on any finite set. The closedness of $H^{-1}_{\Phi}(\mu)$ follows in an obvious way from the equivalence $\mathrm{dis}(g_1, g_2) = 0 \Leftrightarrow \mathbb{P} \circ g_1^{-1} = \mathbb{P} \circ g_2^{-1}$. Thus, $H^{-1}_{\Phi}(\mu)$ is compact in the semimetric $\mathrm{dis}$. Let us prove the continuity of the mapping $\rho \circ : Y^{\Omega} \to X^{\Omega}$ by differently expressing the same semimetric,

$$\mathrm{dis}(f_1, f_2) = 1 - \sum_{x \in X} \min\left[\mathbb{P}(f_1^{-1}(x)), \mathbb{P}(f_2^{-1}(x))\right].$$

Now let $f_1 = \rho \circ g_1$ and $f_2 = \rho \circ g_2$:

$$\begin{aligned}
\mathrm{dis}(\rho \circ g_1, \rho \circ g_2) &= 1 - \sum_{x \in X} \min\left[\mathbb{P}(g_1^{-1}(\rho^{-1}(x))), \mathbb{P}(g_2^{-1}(\rho^{-1}(x)))\right] \\
&= 1 - \sum_{x \in X} \min\left[\sum_{y \in \rho^{-1}(x)} \mathbb{P}(g_1^{-1}(y)), \sum_{y \in \rho^{-1}(x)} \mathbb{P}(g_2^{-1}(y))\right] \\
&\leqslant 1 - \sum_{x \in X} \sum_{y \in \rho^{-1}(x)} \min\left[\mathbb{P}(g_1^{-1}(y)), \mathbb{P}(g_2^{-1}(y))\right] \\
&= 1 - \sum_{y \in Y} \min\left[\mathbb{P}(g_1^{-1}(y)), \mathbb{P}(g_2^{-1}(y))\right] = \mathrm{dis}(g_1, g_2).
\end{aligned}$$

The mapping $\rho \circ$ is continuous, because $\mathrm{dis}(\rho \circ g_1, \rho \circ g_2) \leqslant \mathrm{dis}(g_1, g_2)$. Since continuous mappings preserve compactness[28, с. 199], it follows that $H^{-1}_{\Phi,\rho}(\mu) = \rho \circ H^{-1}_{\Phi}(\mu)$ is compact in the semimetric $\mathrm{dis}$. □

**Definition Б.0.3.** A partition $f_2 \models \Phi_2$ is called an exact image of a partition $f_1 \models \Phi_1$ (hereinafter $f_1 \precsim f_2$) if their codomains coincide ($X_1 = X_2 = X$) and $H_{\Phi_1,\rho}(f_1) \subseteq H_{\Phi_2,\rho}(f_2)$ for all refinements $\rho$ with the same codomain. The set of all exact images will be denoted in the sequel by $\widehat{\Phi}_2(f_1) = \{f_2 \models \Phi_2 \mid f_1 \precsim f_2\}$.

The relation $f_1 \precsim f_2$ can be understood as follows: no matter into what measurable parts we divide the components of the partition $f_1$, the corresponding components in the partition $f_2$ can always be divided into parts equal to them in measure.

**Remark Б.0.1.** Obviously, $f_1 \precsim f_2 \wedge f_2 \precsim f_3 \Rightarrow f_1 \precsim f_3$.

**Lemma Б.0.2.** *Assume that partitions $g_1 : \Omega_1 \to Y$ and $g_2 : \Omega_2 \to Y$ in correlation spaces $\Phi_1$ and $\Phi_2$ are such that $g_1 \precsim g_2$. Then $\rho \circ g_1 \precsim \rho \circ g_2$ for all refinements $\rho : Y \to X$.*

*Доказательство.* Take any $\rho_* : Y_* \to X$ and $\mu \in H_{\Phi_1,\rho_*}(\rho \circ g_1)$. By the definition of the structure of partition, $\exists g_{1*} : \rho_* \circ g_{1*} = \rho \circ g_1, \mathbb{P}_1 \circ g_{1*}^{-1} = \mu$, and we need to prove, by the definition of the exact image, that $\exists g_{2*} : \rho_* \circ g_{2*} = \rho \circ g_2, \mathbb{P}_2 \circ g_{2*}^{-1} = \mu$. Consider a combination $g_{1+} = g_1 \diamond g_{1*}$, where $g_1 = \pi \circ g_{1+}$ and $g_{1*} = \pi_* \circ g_{1+}$. Here $g_{1+} : \Omega_1 \to Y_+, Y_+^a = Y^a \times Y_*^a, a = \overline{1,m}$. By the definition of the structure of partition, $\mathbb{P}_1 \circ g_{1+}^{-1} \in H_{\Phi_1,\pi}(g_1)$, and hence, since $g_1 \precsim g_2$, there exists a $g_{2+} : \Omega_2 \to Y_+$ such that $\mathbb{P}_1 \circ g_{1+}^{-1} = \mathbb{P}_2 \circ g_{2+}^{-1} \in H_{\Phi_2,\pi}(g_2)$. This obviously implies that $\mathbb{P}_2 \circ (\pi_* \circ g_{2+})^{-1} = \mathbb{P}_1 \circ (\pi_* \circ g_{1+})^{-1}$ as well, and hence $g_{2*} = \pi_* \circ g_{2+}$ is the desired partition. □

**Lemma Б.0.3.** *Assume that partitions $f_1 : \Omega_1 \to X$ and $f_2 : \Omega_2 \to X$ in correlation spaces $\Phi_1$ and $\Phi_2$ are such that $f_1 \precsim f_2$. Then for each refinement $\rho : Y \to X$ and each partition $g_1 : \Omega_1 \to Y$ such that $f_1 = \rho \circ g_1$ there exists a partition $g_2 : \Omega_2 \to Y$ such that $f_2 = \rho \circ g_2$ and $g_1 \precsim g_2$.*

*Доказательство.* Let us state the desired assertion as $\exists g_2 \in \widehat{\Phi}_2(g_1) : f_2 = \rho \circ g_2$ and express $\widehat{\Phi}_2$ via the structure of partitions as

$$\widehat{\Phi}_2(g_1) = \bigcap_{\forall Z,\xi: Z\to Y, \mu \in H_{\Phi_1,\xi}(g_1)} H^{-1}_{\Phi_2,\xi}(\mu).$$

By Lemma Б.0.1 the set $\widehat{\Phi}_2(g_1)$ is the intersection of a family of compact sets. Consequently, to prove that it contains the element $g_2 : f_2 = \rho \circ g_2$, it suffices to prove that such an element is contained in the intersection of each finite subfamily of the same compact sets,

$$\exists g_{2*} \in \bigcap_{i=1}^{n} H^{-1}_{\Phi_2,\xi_i}(\mu_i) : f_2 = \rho \circ g_{2*},$$

where $\xi_i : Z_i \to Y$ are arbitrary refinements with arbitrary domains $Z_i$ and the $\mu_i \in H_{\Phi_1,\xi_i}(g_1)$ are chosen arbitrarily as well.

By the definition of the structure of partition, $\exists h_{1,i} \models \Phi_1 : g_1 = \xi_i \circ h_{1,i}, \mathbb{P} \circ h_{1,i}^{-1} = \mu_i$. Let us construct their combination $h_1 = h_{1,1} \diamond \ldots \diamond h_{1,n}$, where $h_{1,i} = \pi_i \circ h_1$, and denote $\xi = \xi_1 \wr \ldots \wr \xi_n$. By the definition of the exact mapping, $\exists h_2 \models \Phi_2 : f_2 = \rho \circ \xi \circ h_2, \mathbb{P}_1 \circ h_1^{-1} = \mathbb{P}_2 \circ h_2^{-1}$, and hence we can take $g_{2*} = \xi \circ h_2$. By construction, $f_2 = \rho \circ g_{2*}$ and $\mathbb{P}_1 \circ h_{1,i}^{-1} = \mathbb{P}_1 \circ (\pi_i \circ h_1)^{-1} = \mathbb{P}_2 \circ (\pi_i \circ h_2)^{-1} = \mathbb{P}_2 \circ h_{2,i}^{-1}$; consequently, $g_{2*}$ is the desired partition. □

**Corollary Б.0.1.** *If correlation spaces satisfy $\Phi_1 \precsim \Phi_2$, then for each partition $f_1 \models \Phi_1$ there exists an $f_2 \models \Phi_2$ such that $f_1 \precsim f_2$.*

**Corollary Б.0.2.** *Lemmas Б.0.2 and Б.0.3 and Corollary Б.0.1 remain valid for the strict relation $f_1 \prec f_2 \equiv f_1 \precsim f_2 \cap \neg(f_1 \succsim f_2)$.*

**Lemma Б.0.4.** *One has $f_1 \precsim f_2 \Leftrightarrow f_1 \succsim f_2$ for any partitions of one and the same correlation space.*

*Доказательство.* Assume the contrary: there exists an $f_1 \prec f_2$ with the codomain $X$. The trivial refinement $\theta(x) = (0, \ldots, 0), \forall x \in X$ obviously yields $\theta \circ f_1 = \theta \circ f_2$. This contradicts $\theta \circ f_1 \prec \theta \circ f_2$, which follows from Lemma Б.0.2. □

**Corollary Б.0.3.** *One has $f_1 \precsim f_2 \Leftrightarrow f_1 \succsim f_2$ for any partitions of isomorphic correlation spaces.*

*Proof of the theorem on isomorphic spaces.* Take an arbitrary profile $\mathrm{s}_1$ of strategies in the game $\Gamma|\Phi_1$. Obviously, this profile is a partition of the correlation space $\Phi_1$. By Corollary Б.0.1, there exists a partition $\mathrm{s}_2$ of the correlation space $\Phi_2$ such that $\mathrm{s}_1 \precsim \mathrm{s}_2$, and in a similar way, $\mathrm{s}_2$ is also a profile of strategies in the game $\Gamma|\Phi_2$. Let us prove the embeddings in both directions: (1) $U^{A_*}_{\Gamma|\Phi_1}(\mathrm{s}_1) \subseteq U^{A_*}_{\Gamma|\Phi_2}(\mathrm{s}_2)$ and (2) $U^{A_*}_{\Gamma|\Phi_1}(\mathrm{s}_1) \supseteq U^{A_*}_{\Gamma|\Phi_2}(\mathrm{s}_2)$ for each cabal $A_*$ of players:

1. Consider an arbitrary profile $\mathrm{s}_{1*} \models \Phi_1$ different from $\mathrm{s}_1$ by the strategies of the cabal $A_*$. Denote $\mathrm{s}_{1+} = \mathrm{s}_1 \diamond \mathrm{s}_{1*}$, where $\mathrm{s}_1 = \pi \circ \mathrm{s}_{1+}$ and $\mathrm{s}_{1*} = \pi_* \circ \mathrm{s}_{1+}$. By the definition of exact image, we have $H_{\Phi_1,\pi}(\mathrm{s}_1) \subseteq H_{\Phi_2,\pi}(\mathrm{s}_2)$; i.e., $\exists \mathrm{s}_{2+} \models \Phi_2 : \mathbb{P}_1 \circ \mathrm{s}_{1+} = \mathbb{P}_2 \circ \mathrm{s}_{2+}, \mathrm{s}_2 = \pi \circ \mathrm{s}_{2+}$. By construction, $\mathrm{s}_{2*} = \pi_* \circ \mathrm{s}_{2+}$ is different from $\mathrm{s}_2$ by the moves of the same players that distinguish $\mathrm{s}_{1*}$ from $\mathrm{s}_1$, and $\mathbb{P}_1 \circ \mathrm{s}^{-1}_{1*} = \mathbb{P}_2 \circ \mathrm{s}^{-1}_{2*}$, and hence, in a similar way, $u^a(\mathrm{s}_{1*}) = u^a(\mathrm{s}_{2*})$. By virtue of arbitrariness of the choice of $\mathrm{s}_{1*}$, this implies that $U^{A_*}_{\Gamma|\Phi_1}(\mathrm{s}_1) \subseteq U^{A_*}_{\Gamma|\Phi_2}(\mathrm{s}_2)$.
2. Since $\mathrm{s}_1 \succsim \mathrm{s}_2$ by Corollary Б.0.3, the reasoning in the previous item is applicable in both forward and backward directions.

□

# Appendix B

## Proof of the theorem on the conspiracy spaces of the same structure[1]

To prove the theorem on the isomorphism of conspiracy spaces, we need several lemmas.

**Lemma B.0.1.** *For each countable family $\mathfrak{F}$ of sets, there exists a chain $\mathfrak{T}$ of sets such that $\sigma(\mathfrak{F}) = \sigma(\mathfrak{T})$.*

*Доказательство.* Let $\mathfrak{F} = \{F_1, F_2, \ldots\}$. Let us construct by induction a sequence of chains $(\mathfrak{T}_i)$ where each next chain incorporates the previous one and $\sigma(\mathfrak{T}_i) = \sigma(\{F_1, \ldots, F_i\})$. For the base case we take $\mathfrak{T}_1 = \{F_1\}$. The induction step is as follows: let $\mathfrak{T}_{i-1} = \{T_1, \ldots, T_n\}, T_1 \subset \ldots \subset T_n$, and $\sigma(\mathfrak{T}_{i-1}) = \sigma(\{F_1, \ldots, F_{i-1}\})$. We decompose the next element $\mathfrak{F}$ into disjoint disjunctions, $F_i = (F_i \cap T_1) \cup (F_i \cap T_2 \setminus T_1) \cup \ldots \cup (F_i \cap T_n \setminus T_{n-1}) \cup (F_i \setminus T_n)$. In this notation, the $j$-th disjunction is embedded in the corresponding difference $T_j \setminus T_{j-1}$ of neighboring chain elements. Consequently, to generate it, it suffices to augment $\mathfrak{T}_{i-1}$ with the set $T_{j-} = F_i \cap T_j \cup T_{j-1}$, which preserves the chain structure, because $T_{j-1} \subseteq T_{j-} \subseteq T_j$. Thus, to produce the entire $F_i$, we set

$$\mathfrak{T}_i = \mathfrak{T}_{i-1} \cup \left\{ \begin{array}{l} F_i \cap T_1, \\ F_i \cap T_2 \cup T_1, \\ \ldots \\ F_i \cap T_n \cup T_{n-1}, \\ F_i \cup T_n \end{array} \right\}$$

Let us show that the limit of the sequence $(\mathfrak{T}_i)$ is the desired chain. Indeed, each element of $\sigma(\mathfrak{F})$ is a countable union of finite intersections of the sets $F_i$. Therefore,

$$\sigma(\mathfrak{F}) = \bigcup_{i=1}^{\infty} \sigma(\{F_1, \ldots, F_i\}) = \bigcup_{i=1}^{\infty} \sigma(\mathfrak{T}_i) = \sigma(\mathfrak{T}).$$

□

**Lemma B.0.2.** *The maximum chain of measurable sets in an atomless space generates an atomless σ-algebra.*

[1] Quoted from the article [11].

*Доказательство.* Let the maximum chain $\mathfrak{T}$ of measurable sets of the atomless space $\langle\Omega,\mathfrak{B},\mathbb{P}\rangle$ generate an algebra $\sigma(\mathfrak{T})$. Let us prove that for each $B\in\sigma(\mathfrak{T})$ of measure $\mathbb{P}(B)>0$ there exists a $B'\in\sigma(\mathfrak{T})$ such that $B'\subset B$ and $\mathbb{P}(B)>\mathbb{P}(B')>0$. To this end, obviously, it suffices to prove that in the chain $\mathfrak{T}$ there exists a set $T$ such that $0<\mathbb{P}(T\cap B)<\mathbb{P}(B)$. Consider the sets

$$\underline{T}=\bigcup_{T_-\in\mathfrak{T}:\mathbb{P}(T_-\cap B)=0}T_-\quad\text{и}\quad\overline{T}=\bigcap_{T_+\in\mathfrak{T}:\mathbb{P}(T_+\cap B)=\mathbb{P}(B)}T_+,$$

which are nested $\underline{T}\subset\overline{T}$ by construction, so that $\mathbb{P}(\overline{T})-\mathbb{P}(\underline{T})\geqslant\mathbb{P}(B)$. Since the chain $\mathfrak{T}$ is maximal in the atomless space, it follows that there exists a $T_0\in\mathfrak{T}$ such that $\underline{T}\subset T_0\subset\overline{T}$. Since $\underline{T}\subset T_0\Rightarrow\mathbb{P}(T_0\cap B)>0$ and $T_0\subset\overline{T}\Rightarrow\mathbb{P}(T_0\cap B)<\mathbb{P}(B)$, we conclude that $T_0$ is the desired set. □

**Definition B.0.1.** For any families of measurable sets $\mathfrak{T}\subseteq 2^\Omega$ and measures $\mathbb{P}:\mathfrak{T}\to\mathbb{R}_{\geqslant 0}$, we define a mapping $\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle:\Omega\to\mathbb{R}_{\geqslant 0}$ referred to as the least measure of inclusion and calculated by the formula $\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle(\omega)=\inf\{\mathbb{P}(T)\mid\omega\in T\in\mathfrak{T}\}$.

**Lemma B.0.3.** *If $\mathfrak{T}\subset 2^\Omega$ is a chain of sets that generates an atomless σ-algebra, then $\mathbb{P}\circ\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle^{-1}$ coincides with the Lebesgue measure on the interval $[0,\mathbb{P}(\Omega)]$.*

*Доказательство.* Since $\mathfrak{T}$ is a chain, we have $\omega\in T\Leftrightarrow\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle(\omega)\leqslant\mathbb{P}(T),\forall\omega\in\Omega,T\in\mathfrak{T}$. Since, in addition, $\mathfrak{T}$ generates an atomless σ-algebra, we conclude that for each $0<t<\mathbb{P}(\Omega)$ there exists a $T\in\mathfrak{T}$ such that $\mathbb{P}(T)=t$. Consequently, the function $\operatorname{mim}\langle\mathfrak{T},\mathbb{P}\rangle$ maps the sets $T\in\mathfrak{T}$ onto the intervals $[0,\mathbb{P}(T)]$, which obviously implies the desired assertion. □

**Lemma B.0.4.** *Let $\langle\Omega,\mathfrak{B},\mathbb{P}\rangle$ atomless probability space with a σ-algebra decomposable into $n$ atomless components $\mathfrak{B}=\sigma(\mathfrak{B}_1\cup\ldots\cup\mathfrak{B}_n)$ such that all events from different components are jointly independent; i.e., $\mathbb{P}(B_1\cap\ldots\cap B_n)=\mathbb{P}(B_1)\ldots\mathbb{P}(B_n)$ for any $B_i\in\mathfrak{B}_i,i=\overline{1,n}$. Then any measurable function $f:\Omega\to X$ with a finite codomain is representable in the form $f=\varphi\circ\mathfrak{r}$, where $\mathfrak{r}:\Omega\to[0,1]^n$ is such that $\mathbb{P}\circ\mathfrak{r}^{-1}$ coincides with the Lebesgue measure and $\varphi:[0,1]^n\to X$ is a Borel function.*

*Доказательство.* Consider the inverse function $f^{-1}:X\to\mathfrak{B}$. By virtue of the decomposability of $\mathfrak{B}$, it can be represented as the limit of a sequence of conjunctions,

$$f^{-1}(x)=\bigcup_{j=1}^{\infty}F_1^j(x)\cap\ldots\cap F_n^j(x),\ F_i^j:X\to\mathfrak{B}_i.$$

Consider the families $\mathfrak{F}_i = \{F_i^j(x) \mid j \in \mathbb{N}, x \in X\}$ of sets and note that $f$ is measurable according to $\sigma(\mathfrak{F}_1 \cup \ldots \cup \mathfrak{F}_n)$. By Lemma B.0.1, there exist chains of sets $\mathfrak{T}_i \subset \mathfrak{B}_i$ such that $\sigma(\mathfrak{F}_i) = \sigma(\mathfrak{T}_i)$. According to the Hausdorff maximum principle, each such chain is embedded in a maximal chain $\overline{\mathfrak{T}}_i \subset \mathfrak{B}_i$ generating an atomless σ-algebra by Lemma B.0.2. Let us construct the desired $\mathfrak{r} = (\mathrm{mim}\langle\overline{\mathfrak{T}}_1, \mathbb{P}\rangle, \ldots, \mathrm{mim}\langle\overline{\mathfrak{T}}_n, \mathbb{P}\rangle)$ and $\varphi = f \circ \mathfrak{r}^{-1}$. The necessary properties are observed by construction. □

*Proof of theorem 1.3.1.* Let us apply the previous lemma to an arbitrary conspiracy space $\Phi_1$ of the structure $\mathfrak{A} = \{A_1, \ldots, A_n\}$ using the secrets of the cabals of conspirators for the respective components of the decomposition $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$ of the σ-algebra. This yields a decomposition $f_1 = \varphi \circ \mathfrak{r}$ for each partition $f_1 \models \Phi_1$. In any other conspiracy space $\Phi_2$ of the same structure $\mathfrak{A}$, the relevant partition $f_2 \models \Phi_2$ is constructed in a similar fashion as $f_2 = \varphi \circ \mathfrak{u}$. Here $\varphi$ is the same, and $\mathfrak{u} = (\mathrm{mim}\langle\mathfrak{W}_1, \mathbb{P}_2\rangle, \ldots, \mathrm{mim}\langle\mathfrak{W}_n, \mathbb{P}_2\rangle)$, where the $\mathfrak{W}_i$ are arbitrary maximal chains embedded in the σ-algebra of the corresponding secrets of the conspiracy space $\Phi_2$. Since both $\mathbb{P}_1 \circ \mathfrak{r}^{-1}$ and $\mathbb{P}_2 \circ \mathfrak{u}^{-1}$ coincide with the Lebesgue measure, we conclude that $\mathbb{P}_1 \circ f_1^{-1} = \mathbb{P}_2 \circ f_2^{-1}$ as well, and this completes the proof of the theorem. □

# Appendix Г

# Card game «Tesseract»

## Г.1 Rules[1]

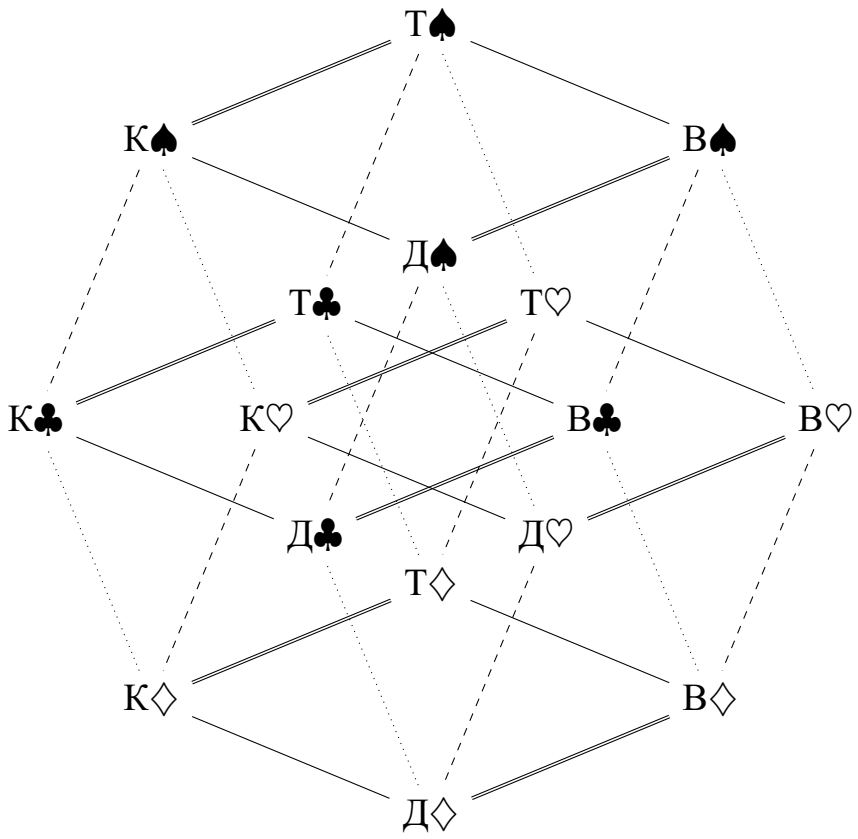


Figure Г.1 — Tesseract of matching cards

To play Tesseract you need:

– 4 player;
– preference deck (4 suit with values from seven to ace, total 32 cards);
– chips or other method of scoring;
– for players just getting to know the game, a printout of the diagram in fig. Г.1 may be helpful at first.

The game consists of any (pre-negotiated and/or upon reaching the win/loss limit) number of independent dealings. The result of one dealing may be the redistribution

[1] The section refines and elaborates the materials of the [9] article.

among the players (with zero sum) of a certain number of fixed bets. No player can lose or win more than 3 bets per dealing.

The dealing begins by dividing the deck into court (В, Д, К, Т) and minor (7, 8, 9, 10) cards.[2] The court deck is shuffled and dealt to the players openly (face up), 4 cards each. The minor deck is dealt without mixing (here the suits and ranks do not matter), also 4 cards per player. After everyone has seen the spread, each player picks up the court and minor cards dealt to him, combining them in a closed hand. After that, the playout begins, consisting of four rounds.

During each round of turns, players must perform two actions in no particular order: a) play one card in front of them face down and b) discard one card into the common discard pile face down. After everyone has finished, the played (but not discarded) cards are revealed. At the end of all four rounds, the players have no cards left in their hands, 4 cards played face up in front of each, and the dealing result is summed up. Each player must count the upturned unpaired cards and, accordingly, his penalty.

From the each player's point of view, 16 court cards are divided into 8 pairs in their own way. The splitting method is determined depending on its position number at the table:

1. matching jacks and queens of the same suit, matching kings and aces of the same suit;
2. matching clubs and spades of the same rank, matching hearts and diamonds of the same rank;
3. matching spades and hearts of the same rank, matching diamonds and clubs of the same rank;
4. matching jacks and aces of the same suit, matching queens and kings of the same suit.

On fig. Г.1 the pairing of cards for different players is indicated by lines of different hatching. Notably, it is easy to see that 16 court cards can be assigned to the vertices of a four-dimensional hypercube (hence the name «Tesseract») in such a way that for each player the pairing relation corresponds to its own set of parallel edges.

[2] You can shuffle and deal the entire deck without dividing it, 8 cards face up per player, however in this case, it won't be uncommon for hands to significantly favor some players at the expense of others. For example, if a hand of only minor cards is dealt to someone, then he will effectively turn into a dummy who does not have the ability to influence the outcome of the game at all. A player with one court card in his hand, while having the opportunity to influence the game situation once per play, will not be able to make meaningful moves in secret from other players, which will make his strategy more predictable, etc. However, if the participants are ready to put up with an increase in the element of chance through the game, then such a «lazy» way of dealing is not forbidden.

In the context of calculating penalties, an unpaired card for a player is the upturned court card that, according to his rules, does not form a pair with other upturned cards. The player's penalty is calculated according to the formula $|2l - 8|$, where $l$ is the number of unpaired cards from his point of view. A player who wants to avoid a penalty should play in such a way that exactly $4$ unpaired cards has been played by the end of the dealing for him, since each card of deviation up or down increases his penalty by $2$. The average penalty is defined as the arithmetic average of the penalties of all players. At the final settlement, players whose penalty is greater than the average deposit chips into the bank equal to the difference between their penalty and the average. On the contrary, the players whose penalty is less than the average take the difference between the average and their penalties from the bank.

## Г.2 Dealing example[3]

Since minor cards are not used in calculating penalties, the initial hands are determined by the layout of court cards (table 2). The further process of playing can be recorded as it is shown in the table 3.

Table 2 — Dealing A

| Player | Hand | | | |
|---|---|---|---|---|
| 1 | В♢ | Д♣ | К♣ | Т♣ |
| 2 | К♠ | К♡ | К♢ | В♣ |
| 3 | Д♠ | В♡ | Д♡ | Д♢ |
| 4 | В♠ | Т♠ | Т♡ | Т♢ |

Table 3 — Playout A1 of dealing A

| Player | Rounds | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | | 2 | | 3 | | 4 | |
| 1 | Д♣ | Т♣ | | | | К♣ | | В♢ |
| 2 | К♠ | | | В♣ | | К♡ | К♢ | |
| 3 | В♡ | | Д♢ | | | Д♡ | Д♠ | |
| 4 | Т♡ | | Т♢ | | Т♠ | | | В♠ |

[3]The section refines and elaborates the materials of the [9] article.

Here, again, the minor cards are not shown due to their indistinguishability by the rules, the played court cards are shown on the white background, and the discarded ones are shown on the gray. For example, the first player on the first round played the queen of clubs and discarded the ace clubs, on the second round played and discarded the minor cards, etc.. Let's count the unpaired cards from the each player's point of view, writing in brackets the corresponding discarded paired card:

1. Д♣ (В♣), В♡ (Д♡), Т♡ (К♡), Д♢ (В♢), Д♠ (В♠)
2. К♠ (К♣), В♡ (В♢), Д♢ (Д♡), Т♠ (Т♣), К♢ (К♡)
3. К♠ (К♡), В♡ (В♠), Т♢ (Т♣), К♢ (К♣), Д♠ (Д♡)
4. Д♣ (К♣), Т♢ (В♢), Т♠ (В♠)

The first player has 4 of 9 upturned cards that form pairs: К♢-Т♢ and К♠-Т♠. There are 5 unpaired cards left, which corresponds to $|2 \cdot 5 - 8| = 2$ penalty points. By repeating the same procedure for the rest of the players, you can complete the table with a penalty column.

Table 4 — Penalties of playout A1

| Player | Rounds | | | | | | | | Penalty |
|---|---|---|---|---|---|---|---|---|---|
| | 1 | | 2 | | 3 | | 4 | | |
| 1 | Д♣ | Т♣ | | | | К♣ | | В♢ | 2 |
| 2 | К♠ | | | В♣ | | К♡ | К♢ | | 2 |
| 3 | В♡ | | Д♢ | | | Д♡ | Д♠ | | 2 |
| 4 | Т♡ | | Т♢ | | Т♠ | | | В♠ | 2 |

Penalties of all players are equal, which means no one pays anyone.

### Г.3 Possible outcomes and simplest strategies

It is interesting that at any moment of the game the penalties of each two participants are either equal or differ by 4. This is easily confirmed by enumeration of $2^{16}$ possible playout outcomes, which allows only 4 distinguishable classes of situations in relation with payoffs:

1. the penalties of all players are equal, there are no payments;
2. the penalty of one of the players is 4 more than the other three, he pays each of them 1 chip;

3. the penalties of the two pairs of players differ by 4, each of the losers pays 1 chip to each of the winners;
4. the penalty of one of the players is 4 less than the other three, they pay him 1 chip each.

Since every time a court card is played, the opponents of the player who upturned it reduce their measure of ignorance about the remaining contents of his hand, it is tactically more reasonable to play court cards after the minor ones. In addition, it is easy to verify that to get a representative of any of the above classes as an outcome of the playout, no more than 4 cards played by all players are sufficient. Thus, the following strategy in the «Tesseract» can be called basic — during the first three turns, only minor cards are played, and the only court card is played on the last round. Even if only beginners are sitting at the table, limited to basic strategies, then their playout may end with an outcome belonging to any of the above classes.

In fact, within the framework of basic strategies, a «Tesseract» can be modeled as a normal form game — if each participant knows that the others will not play court cards until the last round, then what happens turns into a classic $5 \times 5 \times 5 \times 5$ matrix game. It may be tempting to subject «Tesseract» in basic strategies to the ordinary Nash equilibria analysis, but in this case we immediately find ourselves in a dead end — the typical dealing has too many solutions even in pure strategies. For example, the dealing from the table 2 has 21 Nash equilibria, and each strategy of each player participates in at least one of them.

In practice, obviously, such a variety of solutions is little better than none at all — the result is not applicable even as a list of possible agreements, since this would require common knowledge among all 4 players about which agreement applies to each of $\sim 63$ millions of possible dealings. If we reject the idea of rational agents with synchronized memory of tens of millions of cells as clearly artificial, it turns out that even in basic strategies «Tesseract» implies the use of heuristics by players that are parameterized not only by the payoff matrix of the layout. That is, based on the players having a certain internal state that affects the choice of strategy in accordance with a certain algorithm, we inevitably find ourselves in the scheme from the figure 3.1, which allows us to hope for the applicability of the «Tesseract» in the study of the «cohesion» phenomenon.

Table 5 — Nash equilibria in the basic strategies of layout A

| $s^1$ $u^1(s)$ | $s^2$ $u^2(s)$ | $s^3$ $u^3(s)$ | $s^4$ $u^4(s)$ |
|---|---|---|---|
| ∅ 0 | ∅ 0 | ∅ 0 | ∅ 0 |
| ∅ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |
| Д♣ -1 | К♠ -1 | Д♠ 3 | В♠ -1 |
| Д♣ -1 | К♠ -1 | Д♠ 3 | Т♠ -1 |
| Д♣ -2 | К♢ -2 | Д♠ 2 | Т♢ 2 |
| Д♣ -2 | К♡ -2 | Д♠ 2 | Т♡ 2 |
| Д♣ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |
| В♢ -2 | К♠ -2 | В♡ 2 | Т♠ 2 |
| Т♣ 2 | В♣ -2 | ∅ 2 | Т♠ -2 |
| Т♣ 2 | В♣ 2 | ∅ -2 | Т♢ -2 |
| Т♣ 2 | В♣ -2 | Д♢ 2 | Т♠ -2 |

| $s^1$ $u^1(s)$ | $s^2$ $u^2(s)$ | $s^3$ $u^3(s)$ | $s^4$ $u^4(s)$ |
|---|---|---|---|
| Т♣ 2 | В♣ -2 | Д♡ 2 | Т♠ -2 |
| Т♣ 2 | В♣ 2 | Д♡ -2 | Т♢ -2 |
| Т♣ -1 | К♠ -1 | Д♠ 3 | Т♠ -1 |
| Т♣ -1 | К♢ 3 | Д♢ -1 | Т♢ -1 |
| Т♣ 2 | К♡ -2 | Д♡ 2 | Т♠ -2 |
| Т♣ 2 | К♡ 2 | Д♡ -2 | Т♢ -2 |
| Т♣ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |
| К♣ -2 | К♢ 2 | Д♠ -2 | В♠ 2 |
| К♣ -1 | К♢ 3 | Д♢ -1 | Т♢ -1 |
| К♣ -2 | К♡ 2 | Д♡ 2 | Т♡ -2 |