

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Образовательная программа «Прикладная математика и информатика»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Исследовательский проект на тему:

**Применение модальной логики для оценки протокола обмена информацией
в играх с неполной информированностью участников**

Выполнил студент:

группы #БПМИ218, 4 курса

Волкова Екатерина Александровна

Принял руководитель ВКР:

Федянин Денис Николаевич

Приглашенный преподаватель

Факультет компьютерных наук НИУ ВШЭ

Содержание

1	Введение	4
2	Обзор литературы	6
2.1	Эпистемическая логика	6
2.2	Задача о мудрецах и шляпах.	6
2.3	Формулировка игры Russian Cards Problem (RCP)	8
2.4	Подходы к расширению семейств протоколов для RCP в литературе	9
2.5	Вероятностное пространство событий (раздач)	11
2.6	Эпистемические отношения знаний	12
2.7	Публичные объявления	12
2.8	Основные условия корректности протокола	12
3	Исследование основных закономерностей игры RCP и ее обобщений	14
3.1	Мини-RCP «4 карты (2-1-1)»	14
3.2	Таблица миров для классической версии игры Russian Cards Problem	16
4	Программный комплекс моделирующий влияние новой информации на знание агентов в реальном мире, действующих индивидуально	18
4.1	Используемые в коде структуры данных	18
4.2	Описание работы алгоритма	19
4.3	Связь с динамической эпистемической логикой	20
4.4	Пример практического применения	21
4.5	Обзор расширенной версии алгоритма для произвольного количества агентов	21
4.6	Модификация алгоритма для произвольного числа агентов	21
5	Расширение на случай произвольной структуры информированности	23
6	Программный комплекс моделирующий влияние новой информации на знание агентов в реальном мире, способных объединяться в группы по два	25
6.1	Метрики и алгоритмы объединения	26
6.2	Сравнительный анализ разбиения агентов на команды по эффективности объединения знаний	26
6.2.1	Метрика эффективности объединения	26
6.2.2	Результаты для различных функций знания	27

6.2.3	Сравнение жадного и случайного разбиения	27
6.2.4	Число возможных миров до и после объединения	28
6.2.5	Распределение эффективности пар	28
7	Заключение	29
8	Приложение	32
8.1	Формальный логический язык	32
8.2	Логическая головоломка «Чумазные дети».	32
8.3	Код	33
8.4	Применение нейросетей и искусственного интеллекта	33

Аннотация

В работе предлагается новый подход к построению защищённого протокола обмена данными через призму динамической эпистемической логики (Dynamic Epistemic Logic, DEL). Поскольку развитие квантовых вычислений ставит под угрозу методы шифрования, основанные на вычислительной сложности, традиционные системы (особенно использующие факторизацию больших чисел или дискретные логарифмы) рискуют потерять надёжность. Мы исследуем, каким образом стратегия, построенная на DEL, может обеспечить высокую защиту, не зависящую исключительно от вычислительной трудности — фактора, который становится всё более уязвимым по мере роста возможностей квантовых компьютеров.

1 Введение

Рост вычислительных возможностей квантовых машин создаёт серьёзный вызов для широко применяемых криптографических стандартов, опирающихся на задачи факторизации больших чисел или вычисления дискретных логарифмов. Протоколы, уязвимые к алгоритмам Шора или Гровера, могут вскоре стать значительно проще для взлома, поставив под сомнение безопасность систем. Чтобы ответить на эту угрозу, усиливается интерес к подходам, не основанным исключительно на вычислительной сложности. В то время как активно развиваются постквантовые методы (например, решетчатая криптография), исследователи также обращаются к логико-теоретическим направлениям. Новая идея состоит в использовании лишь частичной информации агентов вместо сложных вычислений. В данной работе исследуется применение DEL для разработки метода безопасного обмена данными, ограничивающего выводы перехватчика независимо от его ресурсов.

Russian Cards Problem (RCP), сформулированная Henk и Watkins в 1995 г., служит тестовой площадкой для исследований в логике знания, криптографии без ключей и распределённых вычислений. Отсутствие секретного канала при обмене делает задачу актуальной для практики беспарольных протоколов.

Динамическая эпистемическая логика (DEL) — это формальный язык, который использует модальную логику для описания информированности агентов. Для разглашения информации используются публичные объявления. Динамическая эпистемическая логика *одновременно* описывает:

- 1 **Кто что знает** (эпистемическая часть);

2 **Как знание меняется**, когда происходит объявление, сообщение или любое другое событие (динамическая часть).

2 Обзор литературы

2.1 Эпистемическая логика

Эпистемическая (модальная) логика — это расширение классической логики, в которой появляются модальные операторы для выражения таких понятий, как необходимость (обязательно возможно во всех возможных мирах) и возможность (возможно в каком-то из миров). Она предоставляет формальный аппарат для рассуждений о знаниях и убеждениях агентов, которые могут быть как индивидуальными, так и групповыми.

Модальные операторы:

- A — "необходимо A " " A истинно во всех возможных мирах".
- $\Diamond A$ — "возможно A " " A истинно хотя бы в одном возможном мире".

Формулы строятся из пропозициональных переменных, классических связок и модальных операторов знания и веры. Есть некоторая модель, которая состоит из миров W , множества агентов Ag и множества раскрасок на этих мирах V . Также в модели мы задаем один реальный мир w и некоторое количество отношений $R = W \times W$. Модель $\mathcal{M} = \langle W, \{R_a\}_{a \in Ag}, V \rangle$:

- W — множество возможных миров,
- $R_a \subseteq W \times W$ — отношение неразличимости: миры, которые агент a считает возможными,
- Ag — множество агентов,
- V — оценка атомарных пропозиций, то есть множество атомов, истинных в каждом мире. Для простоты можно провести аналогию с раскрасками миров,
- w — реальный мир, принадлежит множеству миров W .

В эпистемической логике знание записывается как $K_a \varphi$.

Ключевые принципы динамической эпистемической логики на примере логической головоломки

2.2 Задача о мудрецах и шляпах.

Есть три мудреца: А, В, С. У каждого из них на голове по шляпе (красная или синяя). Все видят чужие шляпы, но не свою. По очереди (А, В, С) их спрашивают: «Знаешь ли ты,

какого цвета у тебя шляпа?». Если мудрец не знает, какого цвета его шляпа, он отвечает: «Не знаю». Каждый из мудрецов слышит все ответы. Цель — узнать, как после трёх ответов у третьего мудреца (С) может остаться ровно два возможных «мира», и когда он сможет определить цвет своей шляпы.

Всего возможных сочетаний шляп — 8 (по 2 варианта на каждого, $2^3 = 8$).

Разберем пошагово рассуждения мудрецов:

Шаг 1. Первый мудрец (А)

А видит шляпы В и С. Если бы А видел две красные шляпы (К-К), он мог бы сразу сказать: «У меня синяя», если не разрешено всем быть красными. Если есть ограничения, что не все одного цвета, сразу что-то отсекается. В общем случае, если А не может определить, значит, он видит разные цвета или две синие.

Шаг 2. Второй мудрец (В)

В слышит, что А не знает. Это публичная информация: во всех мирах, где А мог бы знать, они невозможны. В видит шляпу С и А. Его рассуждение зависит от их цветов и предыдущего ответа.

Шаг 3. Третий мудрец (С)

С слышит: А не знает, В не знает. Он анализирует: раз оба до него не знают, значит, отсечены ещё некоторые миры. Он смотрит на две шляпы перед собой, слушает все рассуждения — если у него остаётся ровно два возможных мира, и они различаются цветом его шляпы, он делает вывод.

Публичное объявление позволяют динамически отсекаать миры - объявление «не знаю» отсекает все миры, в которых мудрец мог бы знать, значит, их больше нет. Каждый следующий мудрец знает, что предыдущие не знали, и тоже пересматривает возможные миры.

2.3 Формулировка игры Russian Cards Problem (RCP)

Сформулируем правила для базовой версии игры Russian Cards Problem. Эта задача интересна с точки зрения безопасной передачи информации без шифрования, комбинаторного анализа и построения семейств множеств и теории распределённых знаний и логики. Решение этой задачи эквивалентно способу безопасной передачи информации в распределённой среде без использования шифрования. Игроки моделируют участников общения и противника, а принадлежность карт — сообщаемое сообщение. Общепринято, что такая игра обеспечивает безусловную (информационно-теоретическую) безопасность.

Имеется колода, которая состоит из 7 различных публично известных карт, которые случайным образом распределяются между тремя игроками:

- **Агент А - Алиса** получает 3 карты.
- **Агент Б - Боб** получает 3 карты.
- **Агент С - Кэт** (перехватчик) получает 1 карту.

Цель: Алиса и Боб должны передать по одному публичному сообщению, после которого:

- Боб сможет однозначно определить, какие три карты у Алисы, а Алиса может определить карты Боба.
- Перехватчик (Кэт) не сможет определить, какие 3 карты находятся у Алисы, а какие 3 - у Боба.

Ограничения

Агенты Алиса и Боб не должны иметь никаких предварительных соглашений или общих ключей. В игре запрещено использовать шифрование при публичных оъявлениях для передачи информации между агентами. Передаваемые сообщения доступно всем агентам, участвующим в игре, включая перехватчика.

Мысленно агенты считаются идеальными логиками. Каждый выводит всё, что логически следует из услышанных объявлений и собственных карт. Моделью служит много-агентная Крипке-структура, где миры — возможные раздачи ($\times 35$). Отношением «неразличимо игроку i » у нас являются миры, в которых у агента i совпадают карты на руках (то есть совпадает "рука игрока i ").

2.4 Подходы к расширению семейств протоколов для RCP в литературе

В научной литературе описано несколько расширенных семейств протоколов для классической постановки задачи Russian Cards Problem. Построение корректного протокола в этой игре базируется на двух принципах: **информативности** (адресат точно узнаёт руку отправителя) и **безопасности** (перехватчик не может узнать ни одной карты наверняка). Существует несколько способов достижения этих требований; рассмотрим подробно основные из них.

Двухходовые арифметические протоколы

Один из самых известных методов построения протоколов основан на использовании свойств целых чисел по модулю. Его суть заключается в том, что объявления игроков (Алисы и Боба) кодируются с помощью арифметических выражений — обычно это суммы номеров карт по модулю некоторого заранее выбранного простого числа p . Пусть в игре участвует $v = a + b + c$ карт, которые случайно распределяются между Алисой (a), Бобом (b) и Кэт (c), обычно $a = 3$, $b = 3$, $c = 1$.

В ходе протокола Алиса и Боб публично объявляют суммы своих карт:

$$s_A = \sum_{x \in A} x \pmod{p}, \quad s_B = \sum_{y \in B} y \pmod{p},$$

где $p > a + b + 1$.

После такого обмена каждый из них знает сумму чужих карт и свою собственную руку, а Кэт знает обе суммы и свою карту.

Для фиксированной руки Боба и объявленной суммы s_A существует *ровно одна* возможная рука Алисы — это следует из свойств линейных конгруэнций: множество возможных подмножеств карт Алисы определяется однозначно. Аналогично, Алиса может восстановить руку Боба, используя сумму s_B и свою руку. В свою очередь Кэт, даже зная обе суммы и свою карту, не сможет определить ни одной карты Алисы или Боба точно: всегда найдётся по меньшей мере две совместимые руки.

Если одной суммы недостаточно (например, при большем количестве карт у Алисы), протокол может быть обобщён: Алиса публикует не только сумму, но и значения других симметрических многочленов по модулю p , что гарантирует единственность определения её руки для Боба, но всё равно оставляет неопределённость для Кэт.

Геометрические протоколы на основе блок-дизайнов

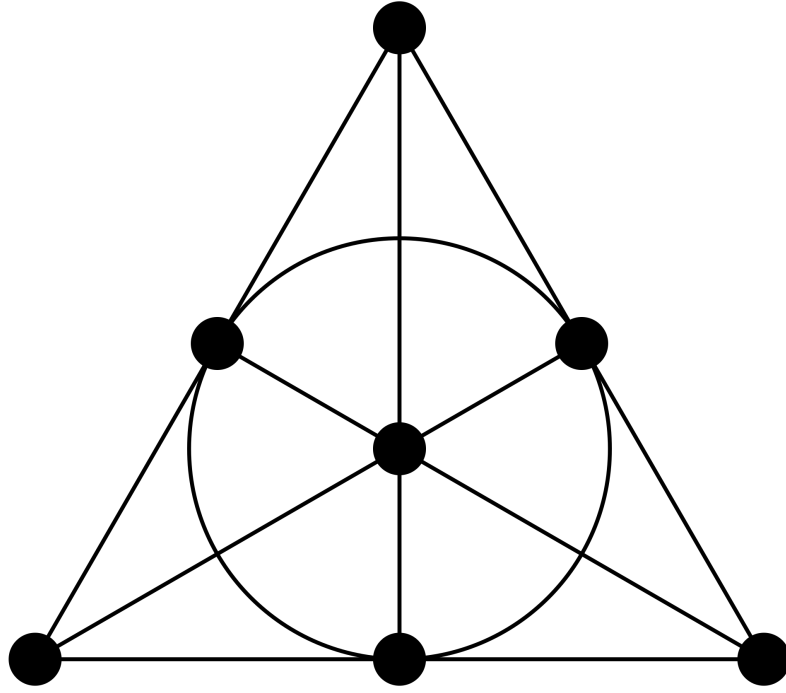


Рис. 2.1: плоскость Фано.

Ещё один подход опирается на конечные геометрические структуры и комбинаторные t -дизайны — например, на проективные плоскости, такие как плоскость Фано. В таких моделях карты интерпретируются как точки конечной геометрии, а руки игроков — как подмножества точек, часто представляющие прямые, плоскости или гиперплоскости. Публичное объявление в этом случае — это выбор некоторого семейства блоков или k -плоскостей, содержащих руку объявляющего игрока.

Классическим примером является использование плоскости Фано, которая состоит из 7 точек (соответствующих 7 картам) и 7 прямых (каждая прямая — это рука Алисы из 3 карт). Когда Алиса объявляет номер своей прямой, Боб по своей руке может однозначно определить, какая из прямых ему подходит, и тем самым узнать карты Алисы. Кэт, однако, не может однозначно восстановить руку Алисы, так как для её знания остаётся несколько подходящих вариантов.

В геометрических протоколах для *perfect 1-security* выполняется вероятностное равенство:

$$\Pr(x \in A \mid \varphi) = \Pr(x \in A) = \frac{a}{a+b}$$

то есть перехватчик не получает никакой вероятностной информации о конкретной карте Алисы.

Многораундовые протоколы с ε -strong security

Третий способ — многораундовые или многошаговые протоколы, допускающие контролируемое смещение вероятностей, то есть неидеальную, но ограниченно нарушаемую безопасность. Их принцип заключается в последовательности публичных объявлений (каждое из которых может быть фейковым или настоящим), после которых не абсолютная невозможность, а ограничение на изменение апостериорных вероятностей служит мерой безопасности.

Для любого мира x требуется выполнение условия:

$$\frac{1}{\varepsilon} \leq \frac{\Pr(x \in A \mid \text{объявления})}{\Pr(x \in A)} \leq \varepsilon$$

где ε — заранее выбранный порог допустимого отклонения вероятности. Перехватчик (Кэт) не сможет гарантированно определить карты Алисы и Боба, даже после всех объявлений — его уверенность ограничивается этим порогом.

Каждая из перечисленных ветвей расширения классического протокола позволяет строить коммуникационные схемы между агентами с разной степенью безопасности, для произвольных параметров игры, с различной длиной и форматом публичных объявлений. Эти методы дают богатый инструментарий для анализа, оптимизации и построения новых защищённых протоколов передачи информации, актуальных для теории распределённых вычислений, информационной безопасности и некриптографических методов обмена.

с).

2.5 Вероятностное пространство событий (раздач)

[Параметрическая раздача] Раздача — это элементарное событие, у нас существуют комбинации элементарных событий как событие. Каждая раздача соответствует некоторому событию. Пусть заданы натуральные $a, b, c \geq 1$ и $v = a + b + c$. Обозначим через $\Omega = \{0, 1, \dots, v - 1\}$ колоду карт. Раздачей называется тройка $w = (A, B, C)$ множеств карт,

$$A \sqcup B \sqcup C = \Omega, \quad |A| = a, \quad |B| = b, \quad |C| = c.$$

Все раздачи образуют конечное множество W ; предполагается равновероятная случайная раздача,

$$|W| = \binom{v}{a} \binom{v-a}{b}. \quad (1)$$

Первым коэффициентом выбираем любые a карт Алисе. Вторым — b карт Бобу из оставшихся $v - a$. То, что останется, уходит Кате, поэтому в формуле c явно не фигурирует.

Таким образом, вероятность каждой конкретной раздачи равна

$$\mathbb{P}(w) = \frac{1}{|W|}. \quad (2)$$

Все раздачи одинаково вероятны, поэтому вероятность любой фиксированной — обратная величине (1).

2.6 Эпистемические отношения знаний

Для игрока X отношение эквивалентности (миров) $\sim_X$ определяется

$$w \sim_X w' \iff \text{рука игрока } X \text{ одинакова в } w \text{ и } w'.$$

Пары $(W, \sim_X)$ задают разбиения, порождая модальную логику $S5$. Знание формулы φ игроком X обозначается $K_X\varphi$.

2.7 Публичные объявления

[Объявление] Формула φ называется *публичным объявлением*, если после её произнесения пространство миров сужается к $W_\varphi = \{w \in W \mid w \models \varphi\}$. Обозначение динамической модальности: $[\varphi]\psi$ — « ψ истинно после объявления φ ».

2.8 Основные условия корректности протокола

Корректность протокола в задаче Russian Cards Problem определяется двумя ключевыми критериями: **информативностью** и **безопасностью**.

Безопасность. Безопасность протокола — это требование, гарантирующее, что после выполнения всей последовательности публичных объявлений $\Phi = (\varphi_1, \dots, \varphi_m)$ перехватчик (например, агент Кэт) не сможет однозначно определить карты других игроков. Формально, после применения всех объявлений к пространству возможных миров W , для любого фиксированного знания Кэт должно оставаться не менее двух вариантов рук Алисы (и/или Боба), согласующихся с её информацией.

По сути, безопасность — это ограничение на совокупность объявлений: протокол должен строиться так, чтобы ни одно сообщение, ни вся их последовательность, не позволяли Кэт однозначно определить настоящую руку других игроков.

Информативность. Информативность протокола — это требование, согласно которому участники обмена (Алиса и Боб) после завершения всех публичных объявлений смогут с уверенностью определить карты друг друга.

Информативность — это необходимое условие того, что каждый из агентов, обладая своей рукой и всеми публичными объявлениями, может однозначно вычислить всю необходимую информацию о реальной раздаче.

В совокупности, оба критерия гарантируют, что протокол одновременно обеспечивает приватность (невозможность перехвата) и полезность (достижение цели коммуникации) — Алиса и Боб узнают всё друг о друге, а Кэт не узнаёт ничего определённого.

Последовательность объявлений $\Phi = (\varphi_1, \dots, \varphi_m)$ решает RCP, если в каждом мире $w \in W$ выполняются

$$[\Phi]K_B(\text{Hand}_A) \quad (\text{информативность}), \quad (3)$$

$$[\Phi]\neg K_C(\text{Hand}_A) \quad (\text{безопасность}). \quad (4)$$

3 Исследование основных закономерностей игры RCP и ее обобщений

3.1 Мини-RCP «4 карты (2-1-1)»

Рассмотрим упрощённый вариант игры russian cards problem с меньшим количеством карт в игре: агент А получает 2 карты, агент В получает одну карту, агенту С достаётся оставшаяся (всего в игре 4 карты). Возможные раздачи — это все перестановки четырех карт между тремя игроками без повторений. В этой версии всего 12 возможных раздач (миров). Каждой паре карт, полученных агентами А и В, соответствует единственная оставшаяся карта для агента С.

- **Классы «Боба».** Фиксируя карту b , Боб различает 3 возможные руки Алисы (например, при $b = 0$: $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$). Чтобы Боб точно определил мир, эти три руки *обязаны* сопровождаться тремя *разными* сообщениями.
- **Классы «Кэт».** Фиксируя свою карту c , Кэт различает три раздачи. Услышав сообщение m , она сужает пространство до

$$\{ (A, B, c) : f(A) = m \}.$$

Чтобы Кэт не вычислила чужую карту $x \neq c$, среди этих раздач должно выполняться

$$|\{ A : x \in A \}| \in \{1, 2\},$$

то есть карта x встречается и «да», и «нет».

Комбинаторный перебор шести возможных рук Алисы показывает, что такую кодировку f не удаётся построить: в любом распределении сообщений, где Бобу хватает информации, остаётся по крайней мере один класс (c, m) , в котором какая-то карта x либо присутствует во всех, либо отсутствует во всех руках Алисы — и Кэт её узнаёт.

Все возможные раздачи карт в этой игре удобно представить в виде таблицы, построенному по следующим принципам:

- Строки — все возможные пары карт, которые может получить Алиса (например, $(1, 2)$, $(1, 3)$, ...).
- Столбцы — возможные карты Боба.

В	А					
	1	1	1	2	2	3
	2	3	4	3	4	4
1				4	3	2
2		4	3			1
3	4		2		1	
4	3	2		1		

Рис. 3.1: в строках перечислены возможные сочетания у Алисы, в столбцах - у Боба, серые клетки обозначают невозможные сочетания, цветом обозначены миры, в которые у Кэт одинаковые карты.

- Ячейки — карта, которая остаётся Кэт (то есть единственная, не попавшая ни к Алисе, ни к Бобу).
- Серые клетки — невозможные раздачи (пересечение рук: комбинации, где А и В получают одну и ту же карту, считаются невозможными и исключаются из таблицы, поскольку каждая карта уникальна в колоде).
- Цветные клетки — миры, в которых Кэт получает одну и ту же карту. Цвета помогают визуально выделить классы эквивалентности по знанию Кэт: все раздачи, где у Кэт одна и та же карта, закрашены одинаково.

Иллюстрация: Например, если Алиса получила (2,3), а Боб — 1, то у Кэт остаётся 4 (см. строку (2,3), столбец 1 — на пересечении написано "4").

Таким образом, каждая допустимая раздача соответствует одной из незакрашенных серым ячейек. Если Кэт знает свою карту, она может посмотреть в этой таблице, в каких мирах она встречается, и, если останется только одна цветная ячейка, она узнаёт всю раскладку.

На основе такой таблицы можно визуализировать весь набор возможных миров и определить, какие из них могут быть исключены в процессе игры. Публичные высказывания агентов А и В не должны пытаться не позволять агенту С точно исключить какие-либо миры, которые он не различал до этого — иначе это приведёт к утечке информации. В игре важно избегать таких объявлений, которые позволяют С однозначно определить карты других агентов или сократить количество возможных миров, в которых он получает одинаковую карту, то есть публичные сообщения агентов должны строиться так, чтобы после любого объявления Кэт не могла исключить все альтернативы, кроме одной.

3.2 Таблица миров для классической версии игры Russian Cards Problem

Аналогично строится таблица и для полной версии: у агентов А и В по три карты, у агента С — одна. Всего в игре используется 7 уникальных карт. Таким образом, при фиксированной руке агентов А и В остаётся ровно одна карта, которую может получить С. Как и в упрощённом варианте, все невозможные миры (где руки игроков пересекаются) исключаются. В процессе игры агенты делают публичные высказывания, и каждый такой акт коммуникации сужает пространство возможных миров, в которых они находятся.

Такие таблицы позволяют визуализировать всю эпистемическую структуру игры: кто что знает, какие ситуации отличимы для игроков. При анализе протоколов эти таблицы позволяют понять, где возможна утечка информации, и как избежать полного раскрытия рук.

		A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	5	
			2	2	2	2	2	3	3	3	3	4	4	4	5	5	6	3	3	3	3	4	4	4	5	5	6	4	4	4	5	5	6	5	5	6	6
B			3	4	5	6	7	4	5	6	7	5	6	7	6	7	7	4	5	6	7	5	6	7	6	7	7	5	6	7	6	7	7	6	7	7	7
1	2	3																																			
1	2	4																																			
1	2	5																																			
1	2	6																																			
1	2	7																																			
1	3	4																																			
1	3	5																																			
1	3	6																																			
1	3	7																																			
1	4	5																																			
1	4	6																																			
1	4	7																																			
1	5	6																																			
1	5	7																																			
1	6	7																																			
2	3	4																																			
2	3	5																																			
2	3	6																																			
2	3	7																																			
2	4	5																																			
2	4	6																																			
2	4	7																																			
2	5	6																																			
2	5	7																																			
2	6	7																																			
3	4	5																																			
3	4	6																																			
3	4	7																																			
3	5	6																																			
3	5	7																																			
3	6	7																																			
4	5	6																																			
4	5	7																																			
4	6	7																																			
5	6	7																																			

Рис. 3.2: в строках перечислены возможные сочетания у Алисы, в столбцах - у Боба, серые клетки обозначают невозможные сочетания, цветом обозначены миры, в которых у Кэт одинаковые карты.

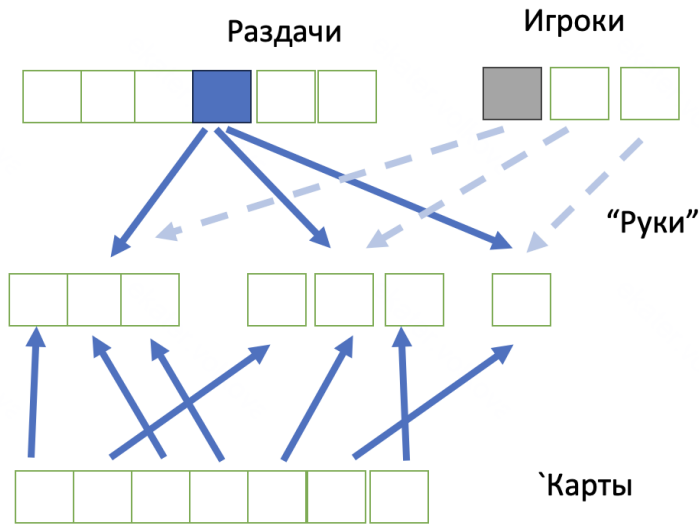


Рис. 3.3: Структуры данных

4 Программный комплекс моделирующий влияние новой информации на знание агентов в реальном мире, действующих индивидуально

Мы хотим уметь понимать, как при заданной информации о мирах изменяются информированность и шансы на победу игроков. Для начала будем рассматривать игроков как отдельные команды из 1 агента, каждый из которых стремится сократить количество своих потенциальных миров до 1.

Рассмотрим скрипт, который строит Крипке-модель возможных раздач и показывает, как публичное объявление “вычёркивает” целый класс миров.

4.1 Используемые в коде структуры данных

В коде используются следующие структуры для хранения данных:

- $cards \in \{0, 1, 2, \dots, n\}$ — какой-то набор карт одного агента (x),
- $worlds \in \{cards_1, cards_2, \dots, cards_n\}$ — миры агента x в раздаче i ,
- $deals \in \{deals_1, deals_2, \dots, deals_i, \dots, deals_m\}$ - множество всех раздач для одного из агентов,
- $hand_j \in \{worlds_0, worlds_1, \dots, worlds_k\}$ — множество возможных рук агента x ,
- $hand \in \{hand_0, hand_1, \dots, hand_i\}$ — множества возможных рук всех агентов.

Рука (карты в руке) агента представляется в виде словаря, где каждому конкретному набору карт сопоставляется множество миров, в которых такая рука возможна. Если для некоторой руки множество возможных миров состоит из одного элемента, это означает, что агент в этом случае точно знает, в каком мире он находится, то есть знает полную конфигурацию игры.

Миры (worlds) — это все возможные состояния (разные раздачи карт). У каждого из агентов есть своя «картина мира» — разбиение множества миров на классы эквивалентности (parts[i]). Два мира попадают в один класс агента i , если он их не различает. Один из агентов публично объявляет номер своего класса. Все миры из этого класса исключаются — стандартная «операция публичного объявления».

В программной реализации игры для описания знаний каждого агента удобно использовать структуры типа «словарь», где каждому потенциальному набору знаний сопоставляется количество возможных миров.

4.2 Описание работы алгоритма

После удаления миров у всех агентов пересчитываются классы (пустые отбрасываем) и стоим новые классы из тех, которые остались непустыми. Далее мы проверяем, кто «выиграл» — тот, у кого остался ровно один возможный мир (то есть он уже точно знает, в какой мир реальный).

- **Генерация всех миров.**

`all_deals()` — функция, которая перебирает все возможные раздачи колоды из 7 карт между тремя игроками: Алиса и Боб получают по 3 карты, Кэт — одну. Каждая раздача представлена кортежем (A, B, C) , где A, B, C — упорядоченные множества карт на руках соответствующих игроков. Итоговое количество миров: 140.

- **Классы эквивалентности по рукам.**

`create(worlds)` — функция, которая для каждого агента строит разбиение всех миров на классы эквивалентности по рукам: в одном классе оказываются все миры, в которых у выбранного агента одна и та же рука. На практике это словарь, где ключ — рука агента (набор карт), а значение — список миров, в которых рука совпадает.

- **Публичное объявление и сужение миров.**

`modify(parts, agent_id, cluster_index)` — функция, моделирующая публичное объявление одного из агентов. Агент с номером `agent_id` объявляет номер своего класса

(например, комбинацию карт на руке), в результате чего все миры, в которых у него такая же рука, вычеркиваются из рассмотрения для всех агентов. После удаления миров обновляются классы эквивалентности для каждого агента, пересчитываются возможные руки.

- **Проверка критерия выигрыша.**

`win(parts, w)` — функция, возвращающая список флагов для каждого агента: 1, если для текущей руки и структуры классов эквивалентности у агента остался ровно один возможный мир (он определил реальную раздачу), иначе 0.

Алгоритм симуляции

- 1 Сначала строится полное пространство миров (`worlds = all_deals()`).
- 2 Для каждого агента создаются классы эквивалентности (`parts = create(worlds)`).
- 3 Один из агентов совершает публичное объявление (например, озвучивает свой класс/руку).
- 4 После объявления для всех агентов обновляются их классы эквивалентности: удаляются миры, несовместимые с объявлением.
- 5 Проверяется, достиг ли кто-то из агентов полного знания: если в его классе эквивалентности остался только один мир, агент может определить реальную раздачу.

4.3 Связь с динамической эпистемической логикой

В терминах динамической эпистемической логики (DEL), каждая итерация функции `modify` реализует операцию публичного объявления: сужает исходную модель (Крипкеструктуру) до подмножества миров, совместимых с объявлением. Каждый агент пересчитывает свою эпистемическую ситуацию: в результате публичной коммуникации возможные для него миры либо остаются, либо исчезают.

Победа агента (точное определение реального мира) соответствует ситуации, когда его эпистемический класс (по руке) состоит из одного мира — знание стало полным.

4.4 Пример практического применения

Такой подход моделирования позволяет программно проверять свойства любых протоколов: можно реализовать объявление по арифметическому, геометрическому или любому другому протоколу и убедиться, что после публичных ходов Боб определяет руку Алисы, а Кэт — нет. Код позволяет изучать процессы сужения миров, анализировать скорость сведения эпистемических классов к единичным и визуализировать эпистемическую динамику.

4.5 Обзор расширенной версии алгоритма для произвольного количества агентов

4.6 Модификация алгоритма для произвольного числа агентов

В предыдущей версии алгоритм был жёстко ориентирован на задачу с тремя агентами (например, Алиса, Боб и Кэт) и фиксированным распределением карт между ними. Структура функций, формирование миров и классов эквивалентности, а также логика публичных объявлений были написаны под конкретный случай Russian Cards Problem 3-3-1.

В новой модификации внесён ряд принципиальных изменений, которые делают алгоритм полностью универсальным и применимым к произвольному числу агентов и любой параметризации раздачи карт:

- **Обобщение параметров раздачи.** Теперь раздача карт задаётся списком `agents_hands` = где h_i — количество карт у i -го агента. Колода формируется автоматически нужной длины как `deck = range(sum(agents_hands))`. Это позволяет моделировать как стандартную RCP 3-3-1, так и задачи с любым количеством агентов и любым распределением карт.
- **Генерация миров.** Функция `all_deals` теперь рекурсивно генерирует все возможные раздачи для заданных размеров рук. Она не ограничена числом агентов и не требует ручного перебора. Множество миров W становится универсальным для любой параметризации.
- **Универсальные классы эквивалентности.** Функция `create(worlds)` строит классы эквивалентности для любого числа агентов: для каждого i формирует разбиение миров по рукам i -го агента. Ранее такое разбиение реализовывалось только для трёх агентов.

- **Гибкое публичное объявление.** Функция `modify(parts, agent_id, cluster_key)` теперь работает для любого $agent_id$, соответствующего номеру объявившего агента, и любого класса (руки) в структуре его знания. Объявления могут совершать любые агенты по очереди или по протоколу, а не только Алиса и Боб.
- **Проверка знания и выигрыша.** Функция `win(parts, real_world)` возвращает вектор знания для всех агентов: 1, если у агента остался ровно один мир с его рукой (он знает полную раздачу), 0 — если не знает. Это позволяет отслеживать эпистемическую динамику для всех участников независимо.

В результате, модифицированный алгоритм обладает высокой универсальностью:

- 1 Позволяет моделировать любые обобщённые протоколы обмена знаниями между произвольным числом агентов.
- 2 Является платформой для анализа новых протоколов в расширенных версиях задачи (например, с командами, с разными ролями агентов, с любыми типами объявлений).
- 3 Упрощает программную проверку критериев информативности и безопасности в широком классе ситуаций.

Таким образом, новый вариант алгоритма существенно расширяет возможности эпистемического моделирования и делает его пригодным для экспериментального анализа любых карточных или абстрактных задач на знание, связанных с Russian Cards Problem.

5 Расширение на случай произвольной структуры информированности

Модель легко масштабируется до перехода от классической карточной реализации, где у каждого агента имеется фиксированное множество потенциальных миров для каждой руки, к более общей модели знаний, мы сталкиваемся с тем, что одному и тому же набору знаний агента может соответствовать различное количество возможных миров. Таким образом, модели с различным распределением знаний среди агентов позволяют формировать более сложные и интересные игровые ситуации.

Например рассмотрим вероятностную модель для произвольного числа агентов, каждый из которых получает информацию о возможных мирах (раздачах карт) — то есть о том, какие распределения карт между игроками допускает его знание. Пусть у нас задан массив вероятностей p , где p_j — вероятность того, что мир j (или состояние) будет *исключён* (удалён) данным агентом после некоторого публичного объявления или их последовательности. Кроме того, задан массив q , в котором для каждого мира i указана вероятность того, что именно этот мир является настоящим (реальным).

Когда игроки совершают публичные объявления, у каждого из них остаётся некоторое количество возможных миров, которые он ещё не исключил. Мы хотим вычислить — с какой вероятностью, исходя из известных массивов p и q , тот или иной агент определит реальный мир (то есть выиграет). Важно: вероятность “победы” агента определяется не только числом отсеянных миров, но и вероятностями того, что удалённый мир был реальным.

Если после объявлений разные агенты удаляют разные множества миров (их классы эквивалентности различаются), итоговое число “доступных” миров у каждого может быть разным. Здесь массив p описывает вероятности исключения миров для каждого агента, а массив q — вероятности их реальности.

Рассмотрим случай когда известно какой из возможных миров будет реальным и известно с какой вероятностью миры будут удаляться, тогда не сложно выписать формулу вычисления *математического ожидания выигрыша* агента. Если мы игнорируем массив q (все миры равновероятны), то ожидание выигрыша есть произведение вероятностей удаления всех альтернативных миров. Если учесть q , формула усложняется: ожидаемый выигрыш агента равен сумме по всем мирам из произведения вероятности реальности мира (q_i), на вероятность того, что все агенты, кроме него, этот мир удалили (то есть выиграть может только он), а также на вероятность, что другой агент не удалил этот мир.

В случае нескольких агентов или команд, вероятность выигрыша команды — это ве-

роятность того, что объединённая информация позволяет однозначно определить реальный мир. Для этого анализируются классы эквивалентности каждого агента $(d_1, d_2, \dots)$, представляющие собой разбиения множества миров по знанию агента.

$$E_u = \sum_i q_i \cdot \prod_{\substack{j \in d_2(w) \\ i \in d_1(w) \\ j \neq i}} p_j \cdot \left(1 - \prod_{\substack{j \in d_2(w) \\ i \in d_1(w) \\ j \neq i}} p_j \right) \quad (5)$$

Здесь:

- E_u — ожидаемый выигрыш (например, вероятность точно определить мир),
- q_i — вероятность, что мир i реален,
- $d_1(w), d_2(w)$ — классы эквивалентности двух агентов для мира w ,
- p_j — вероятность удаления мира j .

Возможности расширения не ограничиваются только изменением структуры знаний. Во-первых, можно существенно увеличить число агентов в игре, что делает анализ стратегий и вероятностей выигрыша значительно богаче. Помимо этого, становится возможным формировать команды из различных агентов. Например, если в базовой игре у нас были команды «Алиса и Боб» против «Кэт», то теперь можно создавать команды из произвольного числа игроков, комбинировать их различными способами и даже реализовывать механизмы перехода агентов из одной команды в другую. При этом передача знаний между командами может существенно влиять на стратегию и исход игры.

Отдельного внимания заслуживает ситуация, когда агенты обмениваются знаниями не полностью открыто, а, например, только внутри своей команды или вообще тайно. Команды могут быть различного размера, а протоколы обмена информацией — различной степени прозрачности. Это позволяет моделировать не только честную, но и скрытую коммуникацию, близкую к реальным когнитивным и социальным сценариям.

Возможны две принципиальные схемы объединения:

- Классическая: команда формируется, но знания остаются индивидуальными, информация передаётся публично и частично.
- Обобщённая: агенты объединяются, и знания становятся общими, что максимально увеличивает информированность команды.

В отличие от абстрактной игры, в моделях реальных агентов можно рассматривать обмен знаниями, в том числе и скрытый: агенты могут делиться информацией только внутри своей команды, не разглашая её остальным. Причём команды могут быть разного размера — от пар до больших объединений. В частности, изучение пар агентов — важный случай: можно промоделировать все возможные пары и посмотреть, насколько эффективно агенты взаимодействуют в дуэтах.

Возникает вопрос: насколько выгодно объединение, и по какому принципу лучше формировать команды? Эффективность можно оценивать с помощью тех же метрик (например, вероятности того, что команда сможет гарантированно определить реальный мир). Для этого можно построить таблицу с вероятностями успешности объединения для каждой пары или группы агентов.

Можно даже использовать методы из машинного обучения, например, reinforcement learning: на старте предполагать некоторые вероятности выгодного объединения, затем проверять по результатам игры, насколько они оправдались, и корректировать стратегии формирования команд. Если пространство миров сужается до одного, объединение считается полностью успешным. Таким образом, каждый агент может стремиться подобрать для себя такую стратегию объединения, которая чаще приводит к выигрышу.

Наконец, эти подходы применимы не только к играм с картами, но и к абстрактным моделям знаний: ведь в примерах с картами у агентов по определению одинаковое число потенциальных миров, а при переходе к моделям знаний это количество может быть произвольным, и анализ сужения пространства возможных миров становится ещё более интересным, открывает широкие перспективы для дальнейших исследований и практических приложений.

6 Программный комплекс моделирующий влияние новой информации на знание агентов в реальном мире, способных объединяться в группы по два

Для двух агентов, скажем, А и Б, их индивидуальные словари можно объединить в общий для команды, что позволяет анализировать комбинации их знаний и возможные состояния мира при совместной игре.

Если у агента А n потенциальных наборов знаний, а у агента Б — m , то совместная команда обладает $n \times m$ возможными комбинациями знаний. При этом каждому сочетанию

может соответствовать своё подмножество миров, и их количество, как правило, меньше или равно таковому для отдельных агентов по отдельности. Таким образом, объединение знаний в команде увеличивает число комбинаций, но уменьшает или сохраняет (но не увеличивает) число возможных миров, делая знания агентов более полными и увеличивая их шансы на победу.

6.1 Метрики и алгоритмы объединения

Для оценки эффективности объединения агентов в команды можно ввести различные метрики. Например, за меру «приближенности к победе» можно взять количество комбинаций знаний, при которых остаётся только один возможный мир, либо рассмотреть долю случаев, в которых объединённое знание сужает пространство возможных миров максимально сильно.

Построив полный граф, где вершины — агенты, а вес рёбер — значение выбранной метрики для соответствующей пары, можно искать оптимальные разбиения на команды. Один из возможных алгоритмов — жадный: поочерёдно выбираем ребро с максимальным весом, объединяем соответствующих агентов в команду и удаляем их из дальнейшего рассмотрения, рекурсивно повторяя процесс. Альтернативой может служить случайный алгоритм объединения или другие эвристики, позволяющие сравнивать эффективность разных стратегий формирования команд.

Расширяя подход на произвольное число агентов, можно анализировать, как увеличение размера команды влияет на вероятность победы, а также обобщать используемые метрики для произвольных групп.

6.2 Сравнительный анализ разбиения агентов на команды по эффективности объединения знаний

6.2.1 Метрика эффективности объединения

В данном анализе эффективность объединения агентов измеряется снижением числа возможных миров — то есть сокращением неопределённости после того, как два агента объединяют свои знания. Каждый агент обладает неполной информацией о состоянии мира, что формализуется как множество допустимых миров согласно знаниям агента. Если два агента образуют команду и обмениваются своими знаниями, их совместное знание соответствует пересечению множеств возможных миров. В качестве метрики эффективности пары исполь-

зудается доля устранённых миров: средний процент уменьшения количества возможных миров для обоих агентов при объединении. Значение метрики, близкое к 1, означает существенное сокращение неопределённости, а значение, близкое к 0, говорит о высокой избыточности знаний в паре.

6.2.2 Результаты для различных функций знания

Были рассмотрены три типа функций знания агентов:

- **Суммирование** (*Summation knowledge*) — каждый агент знает сумму некоторых параметров (например, суммирует значения своей руки).
- **Случайное знание** (*Random knowledge*) — знания агентов формируются случайным образом (разбиение миров на случайные классы).
- **Знание максимума** (*Max knowledge*) — каждый агент знает максимум из своей руки.

Эксперименты проводились для различного числа агентов ($N = 4, 6, 8$) в каждом сценарии. Сравнивались два способа образования команд:

- **Жадное разбиение** — пары формируются итеративно, выбирая на каждом шаге пару с максимальной метрикой.
- **Случайное разбиение** — пары формируются случайным образом без учёта знаний агентов.

6.2.3 Сравнение жадного и случайного разбиения

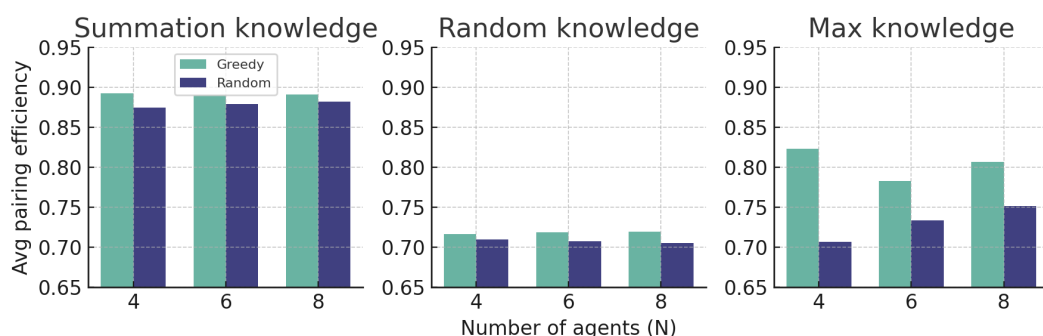


Рис. 6.1: средняя эффективность объединения (по метрике уменьшения миров) для жадного и случайного разбиения. Жадный алгоритм (зелёный) обычно даёт более высокие значения.

На рисунке сравнивается средняя метрика эффективности пар при жадном и случайном объединении. Видно, что жадный алгоритм почти всегда превосходит случайный по

средней эффективности пар. Особенно разница заметна при знании “по максимуму”, где пары агентов могут существенно дополнять друг друга. В сценарии с суммированием знаний разница минимальна, так как любые пары дают почти одинаковый результат.

6.2.4 Число возможных миров до и после объединения

Существенным показателем эффективности команд является сокращение числа возможных миров. На диаграмме ниже для $N = 8$ показано среднее процентное количество миров, остающихся возможными до объединения и после объединения агентов в команды (по жадному и случайному вариантам):

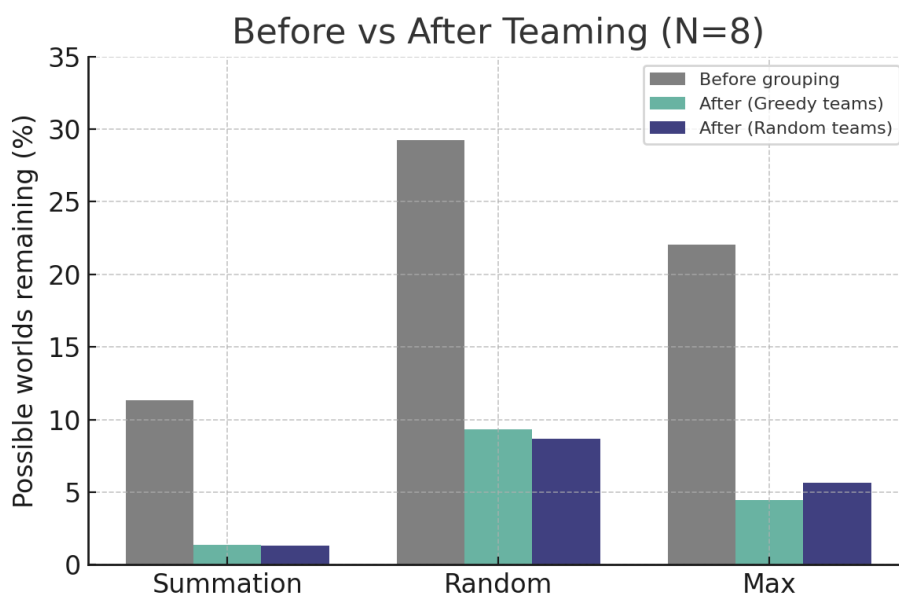


Рис. 6.2: Доля возможных миров: до объединения (серый), после жадного (зелёный) и случайного (синий) объединения.

Видно, что объединение в команды резко уменьшает пространство возможных миров. Жадное разбиение почти всегда даёт лучшее сокращение, хотя разница с случайным небольшая для некоторых сценариев.

6.2.5 Распределение эффективности пар

Рассмотрим распределение метрик эффективности пар для сценария знания “по максимуму” при $N = 8$:

Случайное разбиение часто приводит к умеренным значениям метрики, иногда — к очень низким. Жадное разбиение всегда формирует высокоэффективные пары.

Distribution of pair efficiency (Max knowledge, N=8)

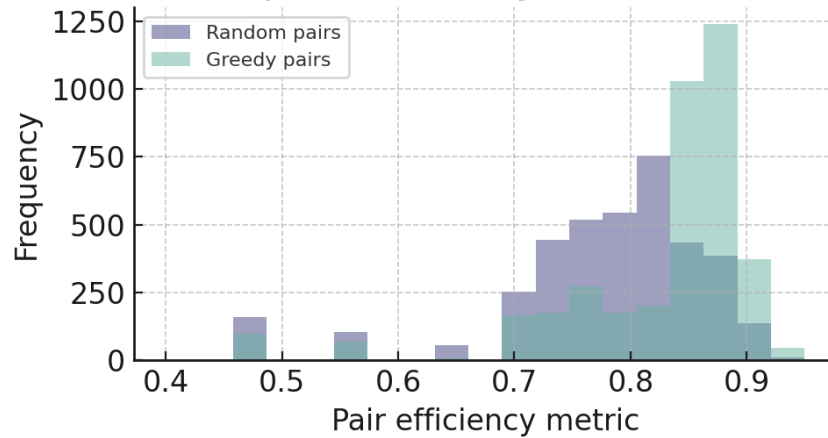


Рис. 6.3: распределение эффективности пар: жадное объединение (зелёный), случайное (фиолетовый). Жадный алгоритм даёт меньше малоэффективных пар.

7 Заключение

В ходе выполненной работы проведено всестороннее исследование задачи Russian Cards Problem и её расширений с применением методов динамической эпистемической логики. Были достигнуты все поставленные цели: сформулирована единая математическая модель RCP, охватывающая классический сценарий и его обобщения на большее число игроков и раундов.

Основным результатом работы является комбинация комбинаторно-логического подхода с динамической логикой знаний для решения RCP. Показано, что методы DEL эффективно описывают и анализируют протоколы обмена: с их помощью формально доказана корректность известных и новых схем, выявлены условия, необходимые для безопасности, а также продемонстрировано, как различные семейства объявлений влияют на знания участников. Разработанные расширенные протоколы расширяют границы применимости классической задачи, позволяя безопасно обмениваться информацией большему числу игроков и в более общих ситуациях.

- Объединение агентов в команды по 2 существенно уменьшает неопределённость (число возможных миров) по сравнению с индивидуальными знаниями.
- Жадный алгоритм разбиения почти всегда превосходит случайный по средней эффективности пар.
- Максимальный выигрыш наблюдается при знаниях типа “максимум”, когда знания агентов хорошо дополняют друг друга.

- Жадный подход избегает неинформативных пар, существенно повышая среднюю информированность команд.

Обсуждая возможные расширения, можно рассмотреть увеличение числа игроков, а также гибкое формирование команд по различным принципам. Игроки могут объединяться для повышения своих шансов, руководствуясь логикой уменьшения числа возможных миров при объединённых знаниях. Для этого важно разработать метрику эффективности объединения, которая может быть основана на вероятности выигрыша или на ожидаемом сужении пространства миров.

Список литературы

- [1] van Ditmarsch, H. (2018). The Russian Cards Problem: A Survey. *Logic Journal of the IGPL*, 26(1), 1–18. • van Ditmarsch, H., van der Hoek, W., Kooi, B. (2007)
- [2] Swift D.A. *A solution to the Russian cards problem using modulus arithmetic*. arXiv:cs/0401012 (2004).
- [3] Conway J. H., Gyles K. Finite packs and projective planes // *J. Combin. Theory, A*. 2012.
- [4] Landerreche C., Fernández-Duque D. Almost-perfect security in the Russian cards problem // *J. Logic Comput.* 23 (2015).
- [5] Taral A. Using block designs in card exchange protocols // *Combinatorial Designs*, 2010.
- [6] Henk M., Watkins J. The Russian Cards Problem // *Discrete Math.* 1995.
- [7] Goldwasser, S., Micali, S. (1984). Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. *Journal of Computer and System Sciences*, 28(2), 270–299.
- [8] Nielsen, M. A., Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th Anniversary ed.). Cambridge University Press.
- [9] Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Proceedings of EUROCRYPT '99* (pp. 223–238). Springer.
- [10] van Benthem, J. (2011). *Logical Dynamics of Information and Interaction*. Cambridge University Press.

- [11] Kirkman, T. P. (1847). On a problem in combinations. *Cambridge and Dublin Mathematical Journal*, **2**, 191–204.
- [12] Albert, M. H., Aldred, R. E. L., Atkinson, M.D., vanDitmarsch, H., Handley, C. C. (2005). Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, **33**, 33–46.
- [13] Cerdón-Franco, A., van Ditmarsch, H., Fernández-Duque, D., Soler-Toscano, F. (2013). A colouring protocol for the generalized Russian cards problem. *Theoretical Computer Science*, **495**, 81–95.
- [14] Swanson, C. M., Stinson, D. R. (2014). Combinatorial solutions providing improved security for the generalized Russian cards problem. *Designs, Codes and Cryptography*, **72**(2), 345–367.
- [15] Plaza, J.A. (1989). Logics of public communications. In *Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems (ISMIS'89)*, Oak Ridge National Laboratory, pp. 201–216.
- [16] Hintikka, J. (1962). *Knowledge and Belief: An Introduction to the Logic of the Two Notions*. Ithaca, NY: Cornell University Press.

8 Приложение

8.1 Формальный логический язык

В работе используется формальный логический язык для описания знаний позволяет записывать и анализировать утверждения вида «агент Алиса знает, чья карта 2» или «после объявления агент Боб узнаёт полный расклад». Язык $\mathcal{L}_{P,N}$ строится по правилам:

- $p \in P \Rightarrow p \in \mathcal{L}_{P,N}$;
- $\varphi, \psi \in \mathcal{L}_{P,N} \Rightarrow \neg\varphi, (\varphi \wedge \psi) \in \mathcal{L}_{P,N}$;
- $a \in N, \varphi \in \mathcal{L}_{P,N} \Rightarrow K_a\varphi \in \mathcal{L}_{P,N}$.

Формула $K_a\varphi$ читается «агент a знает φ ».

8.2 Логическая головоломка «Чумазые дети».

На лужайке играет n детей. У ровно k из них, где $0 < k \leq n$, лицо вымазано грязью. Каждый ребёнок видит грязь на других, но не на себе. **Публичное объявление.**

Папа сообщает:

«Я вижу, что по крайней мере один ребёнок испачкался».

Происходит несколько раундов вопросов и ответов. Каждую минуту папа спрашивает всех одновременно:

«Знает ли кто-нибудь, что он грязный?»

Любой ребёнок, который *достоверно* знает, что его лицо грязное, обязан сделать шаг вперёд (или поднять руку).

Правила и ограничения

Дети идеально логичны. Каждый знает, что все остальные тоже логичны (и что все это знают и т.д. — «общезнание»). Объявление папы услышали все, и это тоже общезнание.

DEL описывает, как каждое публичное объявление («кто-то грязный») и каждая минута коллективного молчания «обрезают» пространство возможных миров, пока у каждого грязного не остаётся ни одной *чистой* альтернативы. Модель: миры — это все распределения грязи; отношение доступности R_i соединяет миры, которые ребёнок i не умеет различать. Публичный акт — это операция *restriction*: $M \upharpoonright \varphi$ удаляет миры, где φ ложно.

8.3 Код

Репозиторий с кодом: https://github.com/CatherineVolkova/RCP_code

8.4 Применение нейросетей и искусственного интеллекта

При написании работы был использован Chatgpt 4-о для оптимизации кода и поиска лучших формулировок некоторых фраз, исследования литературы.