

УДК 519.7, 519.832

РЕШЕНИЕ НЕКОТОРЫХ КЛАССОВ МАТРИЧНЫХ ИГР

А. Ю. Зубов

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

Получены точные решения матричных игр, определяемых некоторыми классами матриц размеров $N \times N$ и $N \times (N - 1)^N$, где $N \geq 3$ — произвольное натуральное число. Решение матричной игры сводится к вычислению параметров стойкости кода аутентификации.

Ключевые слова: матричная игра, оптимальные смешанные стратегии, код аутентификации, вероятности успеха имитации и подмены.

DOI 10.17223/20710410/34/2

THE SOLUTION OF SOME CLASSES OF MATRIX GAMES

A. Yu. Zubov

*Lomonosov Moscow State University, Moscow, Russia***E-mail:** Zubovanatoly@yandex.ru

The approach of G. Simmons to estimating an authentication code (A-code) security is used for solving matrix games. The approach simulates the behavior of the information sender and receiver and an attacker (opponent) as players in matrix games. The imitation attack is represented by a game, the matrix of which coincides with the incidence matrix of A-code. The step of player 1 is the choice of a matrix line (an encoding rule), the step of player 2 is the choice of a matrix column (the simulated message). The substitution attack is represented by a game in which the step of player 1 is the choice of encoding rule (e), the step of player 2 is the choice of a mapping (φ) without immovable points which maps the set of A-code messages to itself. The element $\sigma(e, \varphi)$ of the game matrix equals the probability that, for given e, φ and randomly selected state of a source s , the message $n = \varphi(m)$ replacing an actual message $m = e(s)$ is taken as an authentic one.

In theorems 1 and 2, it is proven that, for given A-code and probability distribution on the set of encoding rules, the values of the corresponding games are equalled to the least probabilities for success of imitation or substitution. For games corresponding to A-code with two source states, N encoding rules and N messages, $N > 2$, the solutions are obtained with the help of these theorems. In theorems 3 and 5, the values v_1 and v_2 of games with the matrices in sizes $N \times N$ and $N \times (N - 1)^N$ respectively, representing the imitation and substitution attacks, as well as the optimum mixed strategies of players, are obtained. The value v_2 is expressed through the probability of choosing one of two source states and $v_1 = 2/N$. Theorem 4 generalizes the result of theorem 3 for A-code with k states of source, $2 \leq k \leq N$.

Keywords: matrix game, optimal mixed strategy, authentication code, probabilities of success of impersonate and substitute.

Введение

В [1–4] развивается теоретико-игровой подход к исследованию кодов аутентификации (далее — А-кодов), предложенный Г. Симмонсом [5, 6]. Под активными атаками понимаются действия противника, связанные с модификацией (атака подмены), фальсификацией (атака имитации) данных или с комбинированным использованием атак имитации и подмены (комбинированная атака). А-код использует избыточное кодирование данных (аналогичное помехоустойчивому кодированию), что обеспечивает возможность проверки целостности данных и подлинности их источника, т. е. защиту от активных атак. В [5] стойкость А-кода оценивается значением соответствующей матричной игры.

Специфика А-кодов в некоторых случаях позволяет решить соответствующую матричную игру. В [1] такая специфика используется для решения двух игр с матрицами размеров 3×3 и 3×8 . Вычисляются значения игр и оптимальные стратегии в этих играх лишь одного игрока, представляющего сторону защиты. Эти результаты обобщаются в [4] на матрицы размеров $N \times N$ и $N \times (N - 1)^N$, где $N \geq 3$ — произвольное натуральное число. В [2, 3] исследуется вопрос о том, может ли комбинированная атака быть более эффективной, чем атаки имитации и подмены по отдельности. Положительный ответ на этот вопрос получен для класса А-кодов. Попутно найдено значение игры с матрицей размеров 4×85 , которое служит оценкой стойкости А-кода из рассматриваемого класса к комбинированной атаке.

Метод, с помощью которого решаются матричные игры в [1, 4], сводит вычисление значения игры к вычислению параметра стойкости А-кода, определённого без использования теоретико-игрового подхода (теоремы 2 и 3 из [3]). Таким параметром служит вероятность успеха атаки, вычисленная при «лучшей» стратегии защиты. Под стратегией защиты понимается распределение вероятностей на множестве правил кодирования А-кода. «Лучшая» стратегия защиты совпадает с оптимальной стратегией игрока (представляющего сторону защиты) в матричной игре.

Основное внимание в [1–4] уделено обоснованию выбора методики оценки стойкости А-кодов. При этом игра, отвечающая атаке подмены, недостаточно формализована как матричная игра и не указан в явном виде метод её решения. Цели настоящей работы состоят в более чёткой формализации матричных игр, ассоциированных с А-кодами, явном указании метода решения этих игр (теоремы 1 и 2), в том числе вычисления оптимальных стратегий обоих игроков (теоремы 3 и 5), а также в обобщении результата теоремы 3 на более широкий класс матриц (теорема 4).

Интерес к данной тематике объясняется тем, что сегодня известно лишь малое число классов матричных игр (например, игры с кососимметрической матрицей), для которых можно точно указать значение игры и оптимальные стратегии игроков. Предлагаемый метод позволяет получить точное решение для бесконечного класса матричных игр, причём определяемых матрицами, элементы которых зависят от действительного параметра.

1. Необходимые определения и понятия

Пусть $\mathcal{A}$ и $\mathcal{B}$ — пользователи общедоступного канала связи, которые передают друг другу те или иные данные. Будем называть эти данные *состояниями источника*. Ими могут быть текстовые документы, результаты бросания монеты и т. п. Если передаются данные от $\mathcal{A}$ к $\mathcal{B}$, то $\mathcal{A}$ будем называть *отправителем*, а $\mathcal{B}$ — *получателем*. Пусть $\mathcal{C}$ — противник, имеющий доступ к каналу связи и техническую возможность изменять (или целиком заменять) передаваемые между $\mathcal{A}$ и $\mathcal{B}$ сообщения или вводить в канал

связи любые новые сообщения. Отнесём такие действия $\mathcal{C}$ к активным атакам: изменение сообщения — *атака подмены*, а введение нового сообщения — *атака имитации*. Мы рассматриваем лишь атаки, целью которых является попытка навязать получателю любое (отличное от передаваемого) состояние источника.

Для защиты от атак $\mathcal{A}$ и $\mathcal{B}$ используют семейство обратимых преобразований $\mathcal{F} = \{f_\kappa : \kappa \in K\}$ передаваемых данных, параметризованное секретным параметром (ключом κ). Результат применения f_κ к состоянию источника будем называть *сообщением*. Отправитель, используя ключ κ , вычисляет $m = f_\kappa(s)$ и направляет сообщение m получателю. Получатель сообщения проверяет его аутентичность и восстанавливает состояние источника, используя тот же ключ. Преобразование f_κ вносит избыточную информацию в сообщение, которая используется для проверки аутентичности. Обратимость f_κ позволяет восстановить состояние источника.

Противнику известно семейство $\mathcal{F}$ и способ представления информации. Неизвестным является лишь секретный ключ. Противник наблюдает в канале связи цепочку сообщений $m_i = f_{\kappa_i}(s_i)$, $i = 1, 2, \dots$, направляемых в моменты времени t_i , $i = 1, 2, \dots$. В любой момент времени t , $t_1 < t$, стороны $\mathcal{A}$ и $\mathcal{B}$ готовы к передаче (и приёму) следующего сообщения. Это, в частности, означает, что при однократном использовании ключа $\mathcal{A}$ и $\mathcal{B}$ мгновенно меняют использованный ключ после передачи каждого сообщения. В любой момент времени t , $t_i < t < t_{i+1}$, противник может произвести атаку имитации и в любой момент времени t_i , $i = 1, 2, \dots$, — атаку подмены. Атака достигает успеха лишь в случае, когда поддельное сообщение (переданное $\mathcal{C}$) принимается получателем как аутентичное. В данной работе рассматривается лишь случай, когда каждый ключ используется однократно.

Удобной математической моделью описанной системы защиты является код аутентификации.

Пусть S, E, M — конечные множества, называемые соответственно множествами *состояний источника*, *правил кодирования* и *сообщений*. Каждое правило кодирования $e \in E$ — инъективное отображение $e : S \rightarrow M$. Тройка $\mathcal{AC} = (S, E, M)$ называется *кодом аутентификации* (*A-кодом*). Для удобства выбора правил кодирования может вводиться множество K ключей A-кода. При этом полагают, что $E = \{e_\kappa : \kappa \in K\}$ и $e_{\kappa_1} \neq e_{\kappa_2}$ при $\kappa_1 \neq \kappa_2$.

Далее для удобства будем рассматривать элементы $e \in E$ как отображения $e : S \cup \{o\} \rightarrow M$, инъективные на S , где o — произвольный символ, не содержащийся в S . Тогда e^{-1} обозначает обратное к e отображение $e^{-1} : M \rightarrow S \cup \{o\}$, такое, что $e^{-1}(m) = s$, если $e(s) = m$, и $e^{-1}(m) = o$, если $m \notin e(S) = \{e(s) : s \in S\}$. Для практического использования A-кода необходимо, чтобы отображения e и e^{-1} были эффективно реализуемы.

Как используется A-код? Для передачи состояния источника $s \in S$ отправитель и получатель (случайно) выбирают правило кодирования $e \in E$. Отправитель вычисляет $m = e(s)$ и направляет сообщение m получателю. Критерий аутентичности полученного сообщения m' — условие $e^{-1}(m') \neq o$. При его выполнении получатель восстанавливает состояние источника $s' = e^{-1}(m')$. Стойкий A-код должен допускать возможность несовпадения m и m' лишь с очень малой вероятностью, которая и определяет уровень стойкости.

Матрица кодирования A-кода $\mathcal{AC}$ — это $|E| \times |M|$ -матрица $C(\mathcal{AC})$, строки которой пронумерованы элементами $e \in E$, столбцы — элементами $m \in M$; на пересечении строки матрицы с номером e и столбца с номером m расположен элемент $c(e, m) =$

$= e^{-1}(m)$. Матрица инцидентности А-кода $I(\mathcal{AC})$ имеет те же размеры. Её элемент $i(e, m)$ равен 1, если $e^{-1}(m) \neq o$, и 0, если $e^{-1}(m) = o$.

При оценке стойкости А-кода полагают, что состояния источника и правила кодирования выбираются случайно и независимо из множеств S и E в соответствии с известными распределениями вероятностей $\mathcal{P}_S = (p_S(s), s \in S)$, $\mathcal{P}_E = (p_E(e), e \in E)$. Они индуцируют распределение $\mathcal{P}_M = (p_M(m), m \in M)$ на множестве сообщений M по формуле

$$p_M(m) = \sum_{e \in E(m)} p_E(e) p_S(e^{-1}(m)), \quad (1)$$

где $E(m) = \{e \in E : e^{-1}(m) \neq o\}$. Здесь и далее символ p_U указывает на принадлежность к распределению $\mathcal{P}_U$.

Введём параметры стойкости А-кода, $\mathbf{p_I}, \mathbf{p_S}$, к атакам имитации и подмены. В англоязычной литературе по тематике А-кодов эти параметры принято называть соответственно вероятностью успеха имитации и вероятностью успеха подмены — Probability of impersonation ($\mathbf{p_I}$), probability of substitution ($\mathbf{p_S}$).

Пусть $\mathcal{P}_E$ — заданное распределение и $\mathbf{p_I}(m)$ — вероятность события $[m \in e(S)]$ при случайном выборе $e \in E$ в соответствии с распределением $\mathcal{P}_E$, т. е. $\mathbf{p_I}(m)$ — это вероятность того, что сообщение $m \in M$ будет принято как аутентичное. Эта вероятность вычисляется по формуле $\mathbf{p_I}(m) = \sum_{e \in E(m)} p_E(e)$. Тогда $\mathbf{p_I}$ определяется формулой

$$\mathbf{p_I} = \max_{m \in M} \mathbf{p_I}(m). \quad (2)$$

Параметр $\mathbf{p_I}$ оценивает максимальные «шансы на успех» противника в атаке имитации.

Пусть $\mathcal{P}_E$ — заданное распределение на множестве E ; $m, n \in M$ — различные сообщения и $\mathbf{p_S}(n|m)$ — вероятность успеха подмены для случайно выбранной пары (s, e) сообщения m сообщением n . Эта условная вероятность вычисляется по формуле

$$\mathbf{p_S}(n|m) = \frac{1}{p_M(m)} \sum_{e \in E(m, n)} p_E(e) p_S(e^{-1}(m)), \quad (3)$$

где $E(m, n) = E(m) \cap E(n)$, а $p_M(m)$ определяется формулой (1). Пусть $\mathbf{p_S}(m) = \max_{n \neq m} \mathbf{p_S}(n|m)$. Тогда $\mathbf{p_S}$ определяется формулой

$$\mathbf{p_S} = \sum_{m \in M} \mathbf{p_S}(m) p_M(m). \quad (4)$$

Параметр $\mathbf{p_S}$ оценивает средние «шансы на успех» противника в атаке подмены.

Более подробные сведения об А-кодах можно найти в [7].

2. Матричные игры, ассоциированные с А-кодами

Ассоциируем с А-кодом две матричные игры — *игру в имитацию* и *игру в подмену*. В них игрок 1 (отправитель и получатель) защищается, а игрок 2 (противник) нападает. При решении этих игр будем пользоваться общепринятыми в теории игр понятиями *матричной игры*, *ситуации в матричной игре*, *смешанных и оптимальных стратегий* [8].

2.1. Игра в имитацию

В игре в имитацию ход игрока 1 состоит в выборе $e \in E$, а ход игрока 2 — в выборе $m \in M$. Матрица игры совпадает с матрицей инцидентности $I(\mathcal{AC}) = (i(e, m))$ А-кода $\mathcal{AC}$. Если (при многократном повторении игры) игроки выбирают ходы случайно в соответствии с распределениями $\mathcal{P} = \mathcal{P}_E = (p(e), e \in E)$ и $\mathcal{Q} = \mathcal{Q}_M = (q(m), m \in M)$, то говорят о смешанном расширении игры, а $\mathcal{P}$ и $\mathcal{Q}$ называют смешанными стратегиями игроков.

Значение игры $v_I(\mathcal{P}, \mathcal{Q})$ в ситуации $(\mathcal{P}, \mathcal{Q})$ выражается формулой

$$v_I(\mathcal{P}, \mathcal{Q}) = \sum_{e \in E} \sum_{m \in M} p(e) i(e, m) q(m) = \sum_{m \in M} \sum_{e \in E(m)} p(e) q(m). \quad (5)$$

Согласно теореме о минимаксе [8], существуют оптимальные смешанные стратегии $\mathcal{P}^0, \mathcal{Q}^0$, для которых выполняются равенства

$$v_I = v_I(\mathcal{P}^0, \mathcal{Q}^0) = \min_{\mathcal{P}} \max_{\mathcal{Q}} v_I(\mathcal{P}, \mathcal{Q}) = \max_{\mathcal{Q}} \min_{\mathcal{P}} v_I(\mathcal{P}, \mathcal{Q}).$$

При этом величина v_I называется *значением игры в имитацию*. Она оценивает стоимость А-кода к атаке имитации.

Теорема 1. Имеет место равенство $v_I = \min_{\mathcal{P}} \mathbf{r}_I$, где $\mathbf{r}_I$ определяется формулой (2).

Доказательство. Пусть $\mathcal{P}_E = \mathcal{P} = (p(e), e \in E)$ — любая смешанная стратегия игрока 1 и $m_0 = m_0(\mathcal{P})$ — сообщение, для которого выполняется равенство

$$\mathbf{r}_I(m_0) = \max_{m \in M} \mathbf{r}_I(m) = \max_{m \in M} \sum_{e \in E(m)} p(e). \quad (6)$$

Пусть $\bar{\mathcal{Q}}(\mathcal{P}) = (\bar{q}(m), m \in M)$ — такая чистая стратегия игрока 2, что

$$\bar{q}(m) = \begin{cases} 1, & \text{если } m = m_0, \\ 0, & \text{если } m \neq m_0. \end{cases} \quad (7)$$

Заметим, что $\bar{\mathcal{Q}}(\mathcal{P})$ даёт игроку 2 максимальный выигрыш против стратегии $\mathcal{P}$. В самом деле, если $\mathcal{Q}$ — произвольная стратегия игрока 2, то из (5)–(7) следуют соотношения $v_I(\mathcal{P}, \mathcal{Q}) = \sum_{m \in M} q(m) \mathbf{r}_I(m) \leq \sum_{m \in M} q(m) \mathbf{r}_I(m_0) = \mathbf{r}_I(m_0) \sum_{m \in M} q(m) = v_I(\mathcal{P}, \bar{\mathcal{Q}}(\mathcal{P}))$.

Пусть $\mathcal{P}^0, \mathcal{Q}^0$ — оптимальные смешанные стратегии игроков. Тогда, используя полученное свойство стратегии $\bar{\mathcal{Q}}(\mathcal{P})$, получаем соотношения

$$v_I(\mathcal{P}^0, \bar{\mathcal{Q}}(\mathcal{P}^0)) \geq v_I(\mathcal{P}^0, \mathcal{Q}^0) = v_I,$$

из которых следует, что

$$v_I(\mathcal{P}^0, \bar{\mathcal{Q}}(\mathcal{P}^0)) = v_I,$$

так как иначе стратегия $\mathcal{P}^0$ позволяет игроку 2 получить выигрыш, превосходящий v_I , что противоречит условию её оптимальности. Отсюда следует неравенство

$$\min_{\mathcal{P}} v_I(\mathcal{P}, \bar{\mathcal{Q}}(\mathcal{P})) \leq v_I.$$

Предположим, что это неравенство — строгое. Тогда найдётся стратегия $\mathcal{P}'$, такая, что $v_{\mathbf{I}}(\mathcal{P}', \bar{\mathcal{Q}}(\mathcal{P}')) < v_{\mathbf{I}}$. Воспользуемся тем, что стратегия $\mathcal{Q}^0$ гарантирует игроку 2 выигрыш, не меньший, чем значение игры. Это означает, что $v_{\mathbf{I}}(\mathcal{P}', \mathcal{Q}^0) \geq v_{\mathbf{I}}$. Отсюда получаем противоречивую цепочку неравенств

$$v_{\mathbf{I}} \leq v_{\mathbf{I}}(\mathcal{P}', \mathcal{Q}^0) \leq v_{\mathbf{I}}(\mathcal{P}', \bar{\mathcal{Q}}(\mathcal{P}')) < v_{\mathbf{I}}.$$

Следовательно, $v_{\mathbf{I}} = \min_{\mathcal{P}} v_{\mathbf{I}}(\mathcal{P}, \bar{\mathcal{Q}}(\mathcal{P})) = \min_{\mathcal{P}} \mathbf{p}_{\mathbf{I}}(m_0) = \min_{\mathcal{P}} \max_m \mathbf{p}_{\mathbf{I}}(m) = \min_{\mathcal{P}} \mathbf{p}_{\mathbf{I}}$. ■

2.2. Игра в подмену

Ход игрока 1 в игре в подмену — выбор $e \in E$, а ход игрока 2 — выбор $\varphi \in \Psi$, где Ψ — множество всех отображений $\varphi : M \rightarrow M$ без неподвижных точек. Матрица игры $(\sigma(e, \varphi))_{e \in E, \varphi \in \Psi}$ состоит из элементов

$$\sigma(e, \varphi) = \sum_{s \in S: e^{-1}(\varphi(e(s))) \neq o} p_S(s),$$

равных вероятности того, что в ситуации (e, φ) для случайно выбранного $s \in S$ (в соответствии с распределением $\mathcal{P}_S$) сообщение $n = \varphi(m)$, подменяющее $m = e(s)$, будет принято как аутентичное. Смешанные стратегии игроков — это распределения

$$\mathcal{P} = \mathcal{P}_E = (p(e), e \in E), \quad \mathcal{R} = \mathcal{R}_{\Psi} = (r(\varphi), \varphi \in \Psi).$$

В ситуации $(\mathcal{P}, \mathcal{Q})$ значение игры $v_{\mathbf{S}}(\mathcal{P}, \mathcal{Q})$ выражается формулой

$$v_{\mathbf{S}}(\mathcal{P}, \mathcal{Q}) = \sum_{e \in E} \sum_{\varphi \in \Psi} p_E(e) \sigma(e, \varphi) r(\varphi). \quad (8)$$

Для оптимальных стратегий $\mathcal{P}^0, \mathcal{R}^0$ получаем значение $v_{\mathbf{S}}$ игры в подмену:

$$v_{\mathbf{S}} = v_{\mathbf{S}}(\mathcal{P}^0, \mathcal{R}^0).$$

Теорема 2. Для любого А-кода $v_{\mathbf{S}} = \min_{\mathcal{P}} \mathbf{p}_{\mathbf{S}}$, где $\mathbf{p}_{\mathbf{S}}$ определяется формулой (4).

Доказательство. Стратегия $\mathcal{R} = (r(\varphi), \varphi \in \Psi)$ индуцирует совокупность $\mathcal{U} = \mathcal{U}(\mathcal{R}) = (\mathcal{U}_m, m \in M)$ распределений $\mathcal{U}_m = (u_{m,n}, n \in M \setminus \{m\})$, где $u_{m,n}$ — вероятность выбора сообщения n , подменяющего m , вычисляемая по формуле

$$u_{m,n} = \sum_{\varphi \in \Psi: \varphi(m)=n} r(\varphi). \quad (9)$$

С другой стороны, совокупность $\mathcal{U} = \{\mathcal{U}_m, m \in M\}$ распределений $\mathcal{U}_m = (u_{m,n}, n \in M \setminus \{m\})$ индуцирует стратегию $\mathcal{R} = \mathcal{R}(\mathcal{U}) = (r(\varphi), \varphi \in \Psi)$,

$$r(\varphi) = \prod_{m \in M} u_{m, \varphi(m)}. \quad (10)$$

Пусть $\mathcal{P}_E = \mathcal{P}, \mathcal{P}_S$ — распределения вероятностей на множествах E, S А-кода, $\mathcal{V} = (v(e, s), e \in E, s \in S)$ — распределение вероятностей на множестве $E \times S$,

$$v(e, s) = p_E(e) p_S(s), \quad (11)$$

$\mathcal{U} = \{\mathcal{U}_m, m \in M\}$ — совокупность распределений $\mathcal{U}_m$. Пусть для пары $(e, s) \in E \times S$ и $n \in M$

$$y((e, s), n) = \begin{cases} 1, & \text{если } e \in E(n), n \neq e(s), \\ 0 & \text{в противном случае.} \end{cases}$$

При случайном выборе (e, s) в соответствии с распределением $\mathcal{V}$ и $n \neq e(s)$ в соответствии с распределением $\mathcal{U}_{e(s)}$ среднее значение $\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U})$ индикатора $y((e, s), n)$ равно

$$\begin{aligned} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}) &= \sum_{e \in E} \sum_{s \in S} \sum_{n \in M \setminus \{e(s)\}} v(e, s) y((e, s), n) u_{e(s), n} = \\ &= \sum_{e \in E} \sum_{s \in S} \sum_{n \in e(S) \setminus \{e(s)\}} v(e, s) u_{e(s), n} = \sum_{m \in M} \sum_{n \neq m} \sum_{e \in E(m, n)} v(e, e^{-1}(m)) u_{m, n}. \end{aligned} \quad (12)$$

Обозначим через $\hat{\mathcal{V}}, \hat{\mathcal{U}}, \hat{\mathcal{P}}, \hat{\mathcal{R}}$ множества возможных распределений вероятностей $\mathcal{V}, \mathcal{U}, \mathcal{P}, \mathcal{R}$ соответственно.

Величина $\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U})$ совпадает со значением $v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}(\mathcal{U}))$ игры в подмену в ситуации $(\mathcal{P}, \mathcal{R}(\mathcal{U}))$, где $\mathcal{R}(\mathcal{U})$ определяется формулой (10), а распределения $\mathcal{V}$ и $\mathcal{P}$ связаны формулой (11). В самом деле, подставляя выражение $u_{m, n}$ из (9) в (12) и используя (11), получаем

$$\begin{aligned} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}) &= \sum_{m \in M} \sum_{n \neq m} \sum_{e \in E(m, n)} \sum_{\varphi \in \Psi: \varphi(m) = n} p_E(e) p_S(e^{-1}(m)) r(\varphi) = \\ &= \sum_{m \in M} \sum_{\varphi \in \Psi} \sum_{e \in E(m, \varphi(m))} p_E(e) p_S(e^{-1}(m)) r(\varphi) = \sum_{e \in E} \sum_{\varphi \in \Psi} \sum_{s \in S: e^{-1}(\varphi(e(s))) \neq o} p_E(e) p_S(s) r(\varphi) = \\ &= \sum_{e \in E} \sum_{\varphi \in \Psi} p_E(e) r(\varphi) \sum_{s \in S: e^{-1}(\varphi(e(s))) \neq o} p_S(s) = v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}(\mathcal{U})). \end{aligned}$$

Покажем теперь, что значение $v_{\mathbf{S}}(\mathcal{P}, \mathcal{R})$ игры в подмену в ситуации $(\mathcal{P}, \mathcal{R})$ совпадает со значением $\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}(\mathcal{R}))$, определённым формулой (12), где $\mathcal{U}(\mathcal{R})$ определяется формулой (9), а распределения $\mathcal{V}$ и $\mathcal{P}$ связаны формулой (11). В самом деле, подставляя выражение $r(\varphi)$ из (10) в (8), получаем

$$\begin{aligned} v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) &= \sum_{e \in E} \sum_{\varphi \in \Psi} p_E(e) \sigma(e, \varphi) r(\varphi) = \sum_{\varphi \in \Psi} r(\varphi) \sum_{e \in E} \sum_{s \in S: e^{-1}(\varphi(e(s))) \neq o} p_E(e) p_S(s) = \\ &= \sum_{\varphi \in \Psi} \left[r(\varphi) \sum_{m \in M} \sum_{e \in E(m, \varphi(m))} p_E(e) p_S(e^{-1}(m)) \right] = \\ &= \sum_{\varphi \in \Psi} \left[\prod_{m' \in M} u_{m', \varphi(m')} \sum_{m \in M} \sum_{e \in E(m, \varphi(m))} p_E(e) p_S(e^{-1}(m)) \right] = \\ &= \sum_{\substack{(n_1, \dots, n_{|M|-1}) \in M^{|M|-1}, \\ n_i \neq m_i, i=1, \dots, |M|-1}} \left[u_{m_1, n_1} \dots u_{m_{|M|-1}, n_{|M|-1}} \sum_{i \in \{1, \dots, |M|-1\}} u_{m_{|M|}, m_i} \times \right. \\ &\quad \times \sum_{j \in \{1, \dots, |M|-1\}} \sum_{e \in E(m_j, n_j)} p_E(e) p_S(e^{-1}(m_j)) \left. \right] + \dots + \\ &+ \sum_{\substack{(n_1, \dots, n_{t-1}, n_{t+1}, \dots, n_{|M|}) \in M^{|M|-1}, \\ n_i \neq m_i, i \in \{1, \dots, |M|\} \setminus \{t\}}} \left[u_{m_1, n_1} \dots u_{m_{t-1}, n_{t-1}} u_{m_{t+1}, n_{t+1}} \dots u_{m_{|M|}, n_{|M|}} \times \right. \\ &\quad \times \sum_{i \in \{1, \dots, |M|\} \setminus \{t\}} u_{m_t, m_i} \sum_{j \in \{1, \dots, |M|\} \setminus \{t\}} \sum_{e \in E(m_j, n_j)} p_E(e) p_S(e^{-1}(m_j)) \left. \right] + \dots + \\ &+ \sum_{\substack{(n_2, \dots, n_{|M|}) \in M^{|M|-1}, \\ n_i \neq m_i, i=2, \dots, |M|}} \left[u_{m_2, n_2} \dots u_{m_{|M|}, n_{|M|}} \sum_{i \in \{2, \dots, |M|\}} u_{m_1, m_i} \sum_{j \in \{2, \dots, |M|\}} \sum_{e \in E(m_j, n_j)} p_E(e) p_S(e^{-1}(m_j)) \right]. \end{aligned}$$

Замечая теперь, что

$$\sum_{i \in \{1, \dots, |M|-1\}} u_{m_{|M|}, m_i} = \dots = \sum_{i \in \{1, \dots, |M|\} \setminus \{t\}} u_{m_t, m_i} = \dots = \sum_{i \in \{2, \dots, |M|\}} u_{m_1, m_i} = 1,$$

и производя группировку слагаемых, получим равенства

$$v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) = \sum_{m \in M} \sum_{n \neq m} \sum_{e \in E(m, n)} p_E(e) p_S(e^{-1}(m_j)) u_{m, n} = \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}(\mathcal{R})). \quad (13)$$

Функция $\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U})$, определённая на компакте и принимающая значения из $[0, 1]$, является непрерывной, и поэтому существуют экстремумы

$$\min_{\mathcal{V} \in \hat{\mathcal{V}}} \max_{\mathcal{U} \in \hat{\mathcal{U}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}), \quad \max_{\mathcal{U} \in \hat{\mathcal{U}}} \min_{\mathcal{V} \in \hat{\mathcal{V}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}).$$

Покажем, что они равны. Для этого заметим, что

$$\{\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}) : \mathcal{U} \in \hat{\mathcal{U}}\} = \{\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}(\mathcal{R})) : \mathcal{R} \in \hat{\mathcal{R}}\},$$

где $\mathcal{U}$ и $\mathcal{R}$ связаны соотношением (10). В самом деле, включение $\supseteq$ очевидно. Обратное включение следует из равенств $\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}_0) = v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}(\mathcal{U}_0)) = \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}(\mathcal{R}_0))$, где для любого $\mathcal{U}_0 \in \hat{\mathcal{U}}$ через $\mathcal{R}_0$ обозначено распределение $\mathcal{R}(\mathcal{U}_0) \in \hat{\mathcal{R}}$. Из полученного равенства следует

$$\max_{\mathcal{R} \in \hat{\mathcal{R}}} \min_{\mathcal{P} \in \hat{\mathcal{P}}} v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) = \max_{\mathcal{R} \in \hat{\mathcal{R}}} \min_{\mathcal{V} \in \hat{\mathcal{V}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}(\mathcal{R})) = \max_{\mathcal{U} \in \hat{\mathcal{U}}} \min_{\mathcal{V} \in \hat{\mathcal{V}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}).$$

Аналогично

$$\min_{\mathcal{P} \in \hat{\mathcal{P}}} \max_{\mathcal{R} \in \hat{\mathcal{R}}} v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) = \min_{\mathcal{V} \in \hat{\mathcal{V}}} \max_{\mathcal{R} \in \hat{\mathcal{R}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}(\mathcal{R})) = \min_{\mathcal{V} \in \hat{\mathcal{V}}} \max_{\mathcal{U} \in \hat{\mathcal{U}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}).$$

Согласно теореме о минимаксе,

$$\min_{\mathcal{P} \in \hat{\mathcal{P}}} \max_{\mathcal{R} \in \hat{\mathcal{R}}} v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) = \max_{\mathcal{R} \in \hat{\mathcal{R}}} \min_{\mathcal{P} \in \hat{\mathcal{P}}} v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) = v_{\mathbf{S}}.$$

Объединяя предыдущие соотношения, получаем равенства

$$\min_{\mathcal{V} \in \hat{\mathcal{V}}} \max_{\mathcal{U} \in \hat{\mathcal{U}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}) = \max_{\mathcal{U} \in \hat{\mathcal{U}}} \min_{\mathcal{V} \in \hat{\mathcal{V}}} \bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U}) = v_{\mathbf{S}}.$$

Поскольку распределение $\mathcal{V}$ однозначно определяется распределением $\mathcal{P}$, будем вместо $\bar{v}_{\mathbf{S}}(\mathcal{V}, \mathcal{U})$ использовать выражение $\bar{v}_{\mathbf{S}}(\mathcal{P}, \mathcal{U})$. Для оптимальных стратегий $\mathcal{P}^0, \mathcal{U}^0$ получаем значение игры

$$\bar{v}_{\mathbf{S}}(\mathcal{P}^0, \mathcal{U}^0) = v_{\mathbf{S}}. \quad (14)$$

Из (11)–(13) следует равенство

$$\bar{v}_{\mathbf{S}}(\mathcal{P}, \mathcal{U}) = \sum_{m \in M} \sum_{n \neq m} p_M(m) \mathbf{p}_{\mathbf{S}}(n|m) u_{m, n},$$

где вероятность $\mathbf{p}_{\mathbf{S}}(n|m)$ определена формулой (3).

Пусть $\mathcal{P}_E = \mathcal{P}$ — произвольная стратегия защиты и $m^0 = m^0(m, \mathcal{P}) \in M$ — сообщение, определённое для данного $m \in M$ и распределения $\mathcal{P}$ равенством

$$\mathbf{p}_{\mathbf{S}}(m^0|m) = \max_{n \neq m} \mathbf{p}_{\mathbf{S}}(n|m). \quad (15)$$

Пусть $\bar{\mathcal{U}}(\mathcal{P}) = \bar{\mathcal{U}}$ состоит из распределений

$$\bar{\mathcal{U}}_m = (\bar{u}_{m,m^0} = 1, \bar{u}_{m,n} = 0, n \neq m).$$

Нетрудно видеть, что для любого $\mathcal{U}$ справедливо неравенство

$$\bar{v}_S(\mathcal{P}, \mathcal{U}) \leq \bar{v}_S(\mathcal{P}, \bar{\mathcal{U}}(\mathcal{P})).$$

Отсюда и из (14), (15) и (4), точно так же, как в теореме 1, следует, что

$$v_S = \min_{\mathcal{P}} \bar{v}_S(\mathcal{P}, \bar{\mathcal{U}}(\mathcal{P})) = \min_{\mathcal{P}} \mathbf{p}_S.$$

Теорема 2 доказана. ■

3. Решение матричных игр

Пусть $N \geq 3$ — натуральное число. Решим игру G_1 с матрицей $\mathcal{A}_1$ равной

$$\begin{pmatrix} 1 & 1 & 0 & 0 & . & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & . & 0 & 0 & 1 \end{pmatrix}.$$

В этой игре ход первого игрока состоит в выборе строки матрицы, а ход второго игрока — в выборе столбца.

Теорема 3. Значение v_{G_1} игры G_1 равно $2/N$. Оптимальными смешанными стратегиями игроков служат соответственно равномерные распределения на множествах строк и столбцов матрицы $\mathcal{A}_1$.

Доказательство. Заметим, что $\mathcal{A}_1$ является матрицей инцидентности А-кода $\mathcal{AC}_N$ с двумя состояниями источника, которые можно интерпретировать как результаты случайного бросания монеты (орёл и решка — будем их обозначать H и T). Пусть $\mathcal{AC}_N$ определяется множествами $S = \{H, T\}$, $E = \{e_1, \dots, e_N\}$, $M = \{m_1, \dots, m_N\}$ и матрицей кодирования $C(\mathcal{AC}_N)$, которая имеет вид

$$\begin{pmatrix} H & T & o & o & . & o & o & o \\ o & H & T & o & . & o & o & o \\ . & . & . & . & . & . & . & . \\ o & o & o & o & . & o & H & T \\ H & o & o & o & . & o & o & T \end{pmatrix}. \quad (16)$$

Паре (s_j, e_i) А-код $\mathcal{AC}_N$ ставит в соответствие сообщение $m_{\kappa_{i,j}} = e_i(s_j)$, где

$$\kappa_{i,j} = \begin{cases} i + j - 1, & \text{если } i \leq N - 1, \\ 1, & \text{если } i = N, j = 1, \\ N, & \text{если } i = N, j = 2. \end{cases}$$

Будем рассматривать G_1 как игру в имитацию для А-кода $\mathcal{AC}_N$.

Пронумеруем i -ю строку матрицы $C(\mathcal{AC}_N)$ правилом кодирования e_i , а j -й столбец — сообщением m_j , $i, j = 1, \dots, N$. Введём обозначение $p_E(e_i) = x_i$, $i = 1, \dots, N$. Тогда, согласно теореме 1, v_{G_1} совпадает с $v_I = \min \{L(\bar{x}), \bar{x} \in \Omega\}$, где

$$L(\bar{x}) = \max \{x_1 + x_N, x_1 + x_2, \dots, x_{N-1} + x_N\}, \\ \Omega = \{\bar{x} = (x_1, \dots, x_N) : x_1 + \dots + x_N = 1, 0 \leq x_i \leq 1, i = 1, \dots, N\}.$$

Минимальное значение $L(\bar{x})$ достигается лишь в случае, когда все переменные принимают одинаковые значения. В самом деле, пусть без ограничения общности $x_1 \geq x_2 \geq \dots \geq x_N$. Тогда $L(\bar{x}) = x_1 + x_2$. При $x_1 = \dots = x_N = 1/N$ получаем значение $L(\bar{x}) = 2/N$. Отсюда следует, что $\min_{\bar{x} \in \Omega} L(\bar{x}) \leq 2/N$. Предположим, что $L(\bar{x}) < 2/N$ при некотором $\bar{x}$. Поскольку x_1 не может быть меньше $1/N$, пусть $x_1 = 1/N + \varepsilon$, где $\varepsilon > 0$. Тогда по условию $x_i < 1/N - \varepsilon$ для любого $i = 2, \dots, N$. Получаем противоречивое неравенство

$$x_1 + \dots + x_N < 1/N + \varepsilon + (N-1)(1/N - \varepsilon) = 1 - N\varepsilon < 1,$$

из которого следует требуемое равенство $v_{G_1} = 2/N$. Отсюда, в частности, также следует, что равномерное распределение вероятностей на множестве строк матрицы $\mathcal{A}_1$ является единственной оптимальной стратегией первого игрока. Найдём оптимальную стратегию игрока 2.

Используя (5), представим значение игры в имитацию в произвольной ситуации $(\mathcal{P}, \mathcal{Q})$ формулой

$$v_{\mathbf{I}}(\mathcal{P}, \mathcal{Q}) = \sum_{m \in M} \sum_{e \in E(m)} p(e)q(m) = \sum_{e \in E} p(e)q_{\mathbf{I}}(e),$$

где $q_{\mathbf{I}}(e) = \sum_{m \in e(S)} q(m)$. Точно так же, как в теореме 1, можно показать, что

$$v_{G_1} = \max_{\mathcal{Q}} v_{\mathbf{I}}(\bar{\mathcal{P}}(\mathcal{Q}), \mathcal{Q}),$$

где $\bar{\mathcal{P}}(\mathcal{Q})$ — «лучшая» против $\mathcal{Q}$ стратегия игрока 1; $\bar{\mathcal{P}}(\mathcal{Q}) = (\bar{p}(e), e \in E)$ — чистая стратегия, такая, что

$$\bar{p}(e) = \begin{cases} 1, & \text{если } e = e_0, \\ 0, & \text{если } e \neq e_0, \end{cases}$$

а $q_{\mathbf{I}}(e_0) = \max_{e \in E} q_{\mathbf{I}}(e)$. Вычислим $q_{\mathbf{I}}(e_0)$. Пусть $q(m_i) = y_i$, $i = 1, \dots, N$. По матрице $C(\mathcal{A}_N)$ находим

$$q_{\mathbf{I}}(e_1) = y_1 + y_2, q_{\mathbf{I}}(e_2) = y_2 + y_3, \dots, q_{\mathbf{I}}(e_{N-1}) = y_{N-1} + y_N, q_{\mathbf{I}}(e_N) = y_1 + y_N.$$

Тогда $q_{\mathbf{I}}(e_0) = \min \{y_1 + y_2, \dots, y_{N-1} + y_N, y_1 + y_N\}$, где y_i удовлетворяют условиям $y_1 + \dots + y_N = 1$, $0 \leq y_i \leq 1$.

Легко показать, что равенство $q_{\mathbf{I}}(e_0) = 1/N$ достигается лишь в случае, когда $y_1 = \dots = y_N = 1/N$. Отсюда, в частности, следует, что в игре G_1 единственной оптимальной стратегией игрока 2 является равномерное распределение на множестве столбцов матрицы $\mathcal{A}_1$. ■

Нетрудно проверить, что аналог теоремы 3 справедлив и для игры G , матрица выигрышей $\mathcal{A}$ которой представляет собой циркулянт, в первой строке которого имеется k единиц и $N - k$ нулей, где $2 \leq k \leq N - 1$.

Теорема 4. Значение v_G игры G равно k/N . Оптимальными смешанными стратегиями игроков служат соответственно равномерные распределения на множествах строк и столбцов матрицы $\mathcal{A}$.

Рассмотрим теперь игру G_2 , матрица выигрышей которой $\mathcal{A}_2$ определяется следующим образом.

Пусть на множестве S состояний источника А-кода $\mathcal{AC}_N$ задано распределение вероятностей $\mathcal{P}_S = (p_S(H) = p, p_S(T) = 1 - p)$, где $0,5 \leq p < 1$. Пусть Ψ — множество всех отображений множества сообщений А-кода $\mathcal{AC}_N$ в себя без неподвижных точек. Тогда $\mathcal{A}_2$ — матрица размеров $|E| \times |\Psi|$, состоящая из элементов $\sigma(e, \varphi)$, где

$$\sigma(e, \varphi) = \sum_{s \in S: e^{-1}(\varphi(e(s))) \neq o} p_S(s). \quad (17)$$

Строки матрицы $\mathcal{A}_2$ пронумерованы правилами кодирования $e \in E$, а столбцы — отображениями $\varphi \in \Psi$. Можно заметить, что $\mathcal{A}_2$ имеет размеры $N \times (N - 1)^N$ и состоит из элементов $0, 1, p, 1 - p$. При этом $\mathcal{A}_2$ содержит ровно $N(N - 1)^{N-2}$ элементов 1 , $N(N - 2)^2(N - 1)^{N-2}$ элементов 0 , $N(N - 2)(N - 1)^{N-2}$ элементов p и столько же элементов $1 - p$. Например, при $N = 3$ матрица $\mathcal{A}_2$ имеет вид

$$\begin{pmatrix} 1-p & 1-p & 1 & 1 & 0 & 0 & p & p \\ 1-p & 1 & 0 & p & 1-p & 1 & 0 & p \\ p & 0 & p & 0 & 1 & 1-p & 1 & 1-p \end{pmatrix}. \quad (18)$$

Строки матрицы пронумерованы правилами кодирования $e_1, e_2, e_3 \in E$, а столбцы — отображениями $\varphi_i, i = 1, \dots, 8$, соответственно:

$$\begin{aligned} \varphi_1 &= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_2 & m_3 & m_1 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_2 & m_3 & m_2 \end{pmatrix}, \quad \varphi_3 = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_2 & m_1 & m_1 \end{pmatrix}, \\ \varphi_4 &= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_2 & m_1 & m_2 \end{pmatrix}, \quad \varphi_5 = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_3 & m_3 & m_1 \end{pmatrix}, \quad \varphi_6 = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_3 & m_3 & m_2 \end{pmatrix}, \\ \varphi_7 &= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_3 & m_1 & m_1 \end{pmatrix}, \quad \varphi_8 = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_3 & m_1 & m_2 \end{pmatrix}. \end{aligned}$$

В игре G_2 ход игрока 1 состоит в выборе строки матрицы $\mathcal{A}_2$ (т. е. правила кодирования $e \in E$), а ход игрока 2 — в выборе столбца матрицы (т. е. отображения $\varphi \in \Psi$).

Введём следующие обозначения. Пусть $a = (1 - p)/p$, $\Theta = \{1, \dots, N\}$ и для $\varphi \in \Psi$

$$\Theta_\varphi^+ = \{k \in \Theta : \varphi(m_k) = m_{(k+1) \bmod N}\}, \quad \Theta_\varphi^- = \{k \in \Theta : \varphi(m_k) = m_{(k-1) \bmod N}\}.$$

Пусть также $y_{N,1} = 0$, $y_{N,N-1} = 1$ и для $k = 1, \dots, N - 1$

$$y_{k,(k-1) \bmod N} = \frac{(1-a)(1-a^{N-k})}{2-a-a^{N-1}}, \quad y_{k,k+1} = \frac{1+a^{N-k}-a^{N-k+1}-a^{N-1}}{2-a-a^{N-1}}. \quad (19)$$

Теорема 5.

1) Если $p = 0,5$, то $v_{G_2} = 0,5$. Оптимальной смешанной стратегией игрока 1 служит равномерное распределение на множестве строк матрицы $\mathcal{A}_2$. В оптимальной смешанной стратегии игрока 2 столбец с номером $\varphi \in \Psi$ выбирается с вероятностью 0 в том и только в том случае, когда для некоторых $i, j \in \Theta$ выполняются соотношения $\varphi(m_i) = m_j$, $1 < (i - j) \bmod N < N - 1$, и с вероятностью $\alpha^{|\Theta_\varphi^+|}(1 - \alpha)^{|\Theta_\varphi^-|}$ в противном случае, где α — произвольное действительное число из интервала $[0, 1]$.

2) Если $p > 0,5$, то

$$v_{G_2} = \frac{3p - 1 - p^2(1 + a^{N-1})}{3p - 1 - pa^{N-1}}. \quad (20)$$

Оптимальной смешанной стратегией игрока 1 служит распределение вероятностей $\mathcal{P}_E = (p(e), e \in E)$ на множестве номеров строк матрицы $\mathcal{A}_2$, где

$$p(e_k) = \frac{a^{k-1}(2p-1)}{3p-1-pa^{N-1}}, \quad k = 1, \dots, N-1, \quad p(e_N) = \frac{2p-1}{3p-1-pa^{N-1}}. \quad (21)$$

Оптимальной смешанной стратегией игрока 2 служит распределение вероятностей $\mathcal{R}_\Psi = (r(\varphi), \varphi \in \Psi)$ на множестве номеров столбцов матрицы $\mathcal{A}_2$, где

$$r(\varphi) = \prod_{k \in \Theta_\varphi^+} y_{k, (k+1) \bmod N} \cdot \prod_{k \in \Theta_\varphi^-} y_{k, (k-1) \bmod N}, \quad (22)$$

а $y_{i,j}$ определены формулами (19).

Доказательство. Будем рассматривать G_2 как игру в подмену для А-кода $\mathcal{AC}_N$. Согласно теореме 2 и виду матрицы кодирования $C(\mathcal{AC}_N)$,

$$v_{G_2} = v_S = \min \{L_1(\bar{x}), \bar{x} \in \Omega\},$$

где

$$L_1(\bar{x}) = \max \{px_1, px_N\} + \max \{(1-p)x_1, px_2\} + \max \{(1-p)x_2, px_3\} + \dots \\ + \max \{(1-p)x_{N-2}, px_{N-1}\} + \max \{(1-p)x_{N-1}, (1-p)x_N\}. \quad (23)$$

При $p = 0,5$ утверждения теоремы о значении игры и оптимальной стратегии игрока 1 сразу следуют из вида функции $L_1(\bar{x})$. При $p > 0,5$ для нахождения v_{G_2} будем вычислять $\min \{L_1(\bar{x}), \bar{x} \in \Omega\}$ путём раскрытия максимумов в сумме правой части равенства (23) в 2^N случаях, определяемых расстановкой неравенств $\leq$ или $\geq$ вместо знака $\vee$ в системе

$$\begin{cases} px_1 \vee px_N, \\ (1-p)x_1 \vee px_2, \\ \dots \\ (1-p)x_{N-2} \vee px_{N-1}, \\ (1-p)x_{N-1} \vee (1-p)x_N. \end{cases} \quad (24)$$

В каждом таком случае $L_1(\bar{x})$ представляет собой линейную функцию с положительными коэффициентами. Представим для удобства систему (24) в виде

$$\begin{cases} x_1 \vee x_N, \\ ax_1 \vee x_2, \\ \dots \\ ax_{N-2} \vee x_{N-1}, \\ x_{N-1} \vee x_N \end{cases} \quad (25)$$

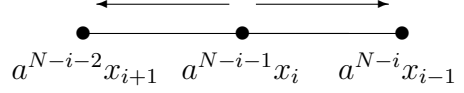
и расположим переменные $x_1, x_N, x_{N-1}, ax_{N-2}, a^2x_{N-3}, \dots, a^{N-2}x_1$ в одну цепочку, которую для наглядности изобразим в виде схемы:

$$\begin{array}{ccccccc} \bullet & \bullet & \bullet & \bullet & \dots & \bullet & \bullet \\ x_1 & x_N & x_{N-1} & ax_{N-2} & \dots & a^{N-3}x_2 & a^{N-2}x_1 \end{array} \quad (26)$$

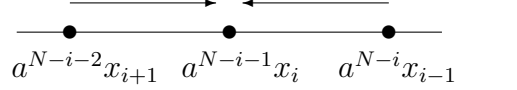
В схеме (26), соответствующей системе (25), нарисует стрелки, указывающие направление возрастания значений переменных:

$$\begin{array}{ccc} \xrightarrow{\hspace{2cm}} & & \xleftarrow{\hspace{2cm}} \\ \bullet & \bullet & \bullet & \bullet \\ a^{N-i-1}x_i & a^{N-i}x_{i-1} & a^{N-i-1}x_i & a^{N-i}x_{i-1} \\ (x_i \leq ax_{i-1}) & & (x_i \geq ax_{i-1}) \end{array}$$

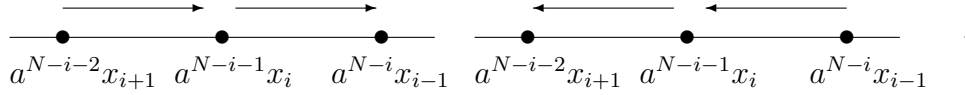
Заметим, что в схеме (26) могут быть точки трёх видов, назовём их соответственно *начальными*, *конечными* и *проходными*. Начальная точка $a^{N-i-1}x_i$ отвечает случаю, когда в системе (25) имеются неравенства $ax_{i-1} \geq x_i$ и $ax_i \leq x_{i+1}$. Ей соответствует фрагмент схемы вида



Конечная точка $a^{N-i-1}x_i$ отвечает случаю, когда в системе (25) имеются неравенства $ax_{i-1} \leq x_i$ и $ax_i \geq x_{i+1}$. Ей соответствует фрагмент схемы вида



Наконец, проходная точка $a^{N-i-1}x_i$ отвечает случаю, когда в системе (25) имеются неравенства $ax_{i-1} \leq x_i$ и $ax_i \leq x_{i+1}$ или неравенства $ax_{i-1} \geq x_i$ и $ax_i \geq x_{i+1}$. Проходной точке соответствует один из фрагментов схемы вида



Нетрудно видеть, что в любом случае, определяемом системой (25), выражение функции $L_1(\bar{x})$ содержит переменную x_i с коэффициентом 1, если точка $a^{N-i-1}x_i$ — конечная, с коэффициентом p или $1-p$, если точка $a^{N-i-1}x_i$ — проходная, и не содержит x_i если точка $a^{N-i-1}x_i$ — начальная.

Рассмотрим сначала два случая, в которых соответствующая схема не содержит начальных и конечных точек:

- 1) ;
- 2) .

Первый случай невозможен, поскольку (в силу того, что $a < 1$) его условия

$$x_1 \leq x_N \leq x_{N-1} \leq ax_{N-2} \leq \dots \leq a^{N-3}x_2 \leq a^{N-2}x_1$$

противоречивы. Второй случай соответствует системе неравенств

$$x_1 \geq x_N \geq x_{N-1} \geq ax_{N-2} \geq \dots \geq a^{N-3}x_2 \geq a^{N-2}x_1. \quad (27)$$

В этом случае $L_1(\bar{x})$ имеет вид

$$L_1(\bar{x}) = p(x_1 + x_2 + \dots + x_{N-1}) + (1-p)x_N = (2p-1)(x_1 + x_2 + \dots + x_{N-1}) + 1-p. \quad (28)$$

Лемма 1. В условиях (27) минимум функции $L_1(\bar{x})$ достигается на наборе переменных, удовлетворяющем условиям

$$x_{N-1} = ax_{N-2} = \dots = a^{N-3}x_2 = a^{N-2}x_1 = a^{N-2}x_N. \quad (29)$$

При этом

$$\min_{(27)} L_1(\bar{x}) = \frac{3p-1-p^2(1+a^{N-1})}{3p-1-pa^{N-1}}. \quad (30)$$

Доказательство. Условия (27) можно представить в следующем виде:

$$x_N \leq \frac{1}{a^0} x_1 \leq \frac{1}{a^1} x_2 \leq \dots \leq \frac{1}{a^{N-2}} x_{N-1}. \quad (31)$$

Пусть $\bar{x}^1$ — вектор аргументов, на котором $L_1(\bar{x})$ достигает минимума в условиях (31). Предположим, что в цепочке неравенств (31) имеет место хотя бы одно строгое неравенство:

$$x_N^1 = \frac{1}{a^0} x_1^1 = \dots = \frac{1}{a^{k-1}} x_k^1 < \frac{1}{a^k} x_{k+1}^1 \leq \dots$$

Рассмотрим тогда вектор $\bar{x}'$ с координатами

$$\begin{aligned} x'_N &= x_N^1 + \varepsilon, \quad x'_1 = x_1^1 + \varepsilon, \dots, x'_k = x_k^1 + \varepsilon, \\ x'_{k+1} &= x_{k+1}^1 - (k+1)\varepsilon, \quad x'_{k+2} = x_{k+2}^1, \dots, x'_{N-1} = x_{N-1}^1. \end{aligned}$$

Очевидно, что ε можно выбрать таким, чтобы сумма координат $\bar{x}'$ оставалась равной единице и выполнялись бы условия (31). Но

$$L_1(\bar{x}') = L_1(\bar{x}^1) - (2p-1)\varepsilon < L_1(\bar{x}^1).$$

Полученное противоречие доказывает, что координаты вектора $\bar{x}$, для которого $L_1(\bar{x})$ достигает минимума в рассматриваемых условиях, удовлетворяют (29). Поскольку сумма координат вектора $\bar{x}$ равна 1, из (28) получаем значения координат вектора $\bar{x}^1$. Они выражаются формулами (21). Учитывая, что в условиях леммы $L_1(\bar{x})$ можно выразить формулой $L_1(\bar{x}) = p - (2p-1)x_N$, из (21) получаем формулу (30). ■

Лемма 2. Пусть $\bar{x}^{(\alpha)}$ — вектор, для которого $\min_{(24)} L_1(\bar{x}) = L_1(\bar{x}^{(\alpha)})$ в условиях случая, определённого произвольной фиксированной совместной системой неравенств (24). Тогда координаты вектора $\bar{x}^{(\alpha)}$ удовлетворяют одному из следующих условий:

$$\begin{aligned} \alpha = 0: \quad & x_N^{(0)} = x_{N-1}^{(0)} = ax_{N-2}^{(0)} = \dots = a^{N-2}x_1^{(0)}; \\ \alpha = 1: \quad & x_{N-1}^{(1)} = ax_{N-2}^{(1)} = \dots = a^{N-2}x_1^{(1)} = a^{N-2}x_N^{(1)}; \\ \alpha = k: \quad & x_{N-k}^{(k)} = ax_{N-k-1}^{(k)} = \dots = a^{N-k-1}x_1^{(k)} = a^{N-k-1}x_N^{(k)} = \\ & = a^{N-k-1}x_{N-1}^{(k)} = a^{N-k}x_{N-2}^{(k)} = \dots = a^{N-3}x_{N-k+1}^{(k)}, \quad 2 \leq k \leq N-1. \end{aligned}$$

Доказательство. Случай, когда схема (26), соответствующая данной системе неравенств, не содержит начальных точек, рассмотрен в лемме 1. При этом $\bar{x}^{(\alpha)}$ удовлетворяет условиям (29), которые совпадают с условиями случая $\alpha = 1$. В других случаях схема имеет хотя бы одну начальную и хотя бы одну конечную точку.

Рассмотрим фрагмент схемы, в котором начальная точка расположена между двумя конечными точками:

$$\begin{array}{ccccccc} \longrightarrow & \longleftarrow & \longrightarrow & \longleftarrow & \longrightarrow & \longleftarrow & \longrightarrow \\ \bullet & \bullet & \bullet & \dots & \bullet & \bullet & \bullet \\ a^{N-m-1}x_m & & & & a^{N-j-1}x_j & & a^{N-k-1}x_k \end{array},$$

причём $r > 1$. Такому фрагменту соответствует система неравенств

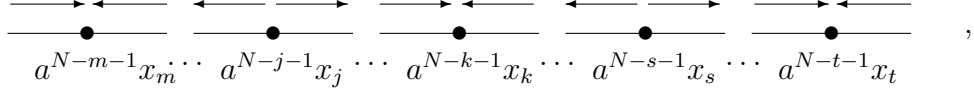
$$\begin{cases} a^{N-j-1}x_j \leq a^{N-j}x_{j-1} \leq \dots \leq a^{N-k-1}x_k, \\ a^{N-j-1}x_j \leq a^{N-j-2}x_{j+1} \leq \dots \leq a^{N-r-1}x_r. \end{cases}$$

Так же как и в лемме 1, можно доказать, что для координат вектора $\bar{x}^{(\alpha)}$ в системе (31) все нестрогие неравенства обязаны быть равенствами. Отсюда следует, что

$$\frac{1}{a^{j-m}} x_m^{(\alpha)} = \dots = \frac{1}{a} x_{j+1}^{(\alpha)} = x_j^{(\alpha)} = ax_{j-1}^{(\alpha)} = \dots = a^{j-1}x_k^{(\alpha)}. \quad (32)$$

Если для вектора $\bar{x}^{(\alpha)}$ выполняется условие (32), то будем говорить, что в схеме (26) на отрезке $[x_m^{(\alpha)}, x_k^{(\alpha)}]$ достигается равенство.

Пусть системе неравенств (24) соответствует схема (26), в которой имеется более одной начальной точки. Рассмотрим тогда фрагмент схемы, содержащий две соседние начальные точки $a^{N-j-1}x_j$ и $a^{N-s-1}x_s$:

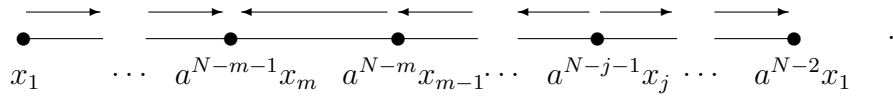


причём $r \neq 1$. Тогда для вектора $\bar{x}^{(\alpha)}$ достигаются равенства на отрезках $[x_r^{(\alpha)}, x_k^{(\alpha)}]$ и $[x_k^{(\alpha)}, x_t^{(\alpha)}]$. А так как эти отрезки пересекаются в точке $a^{N-k-1}x_k$, достигается равенство и на всём отрезке $[x_r^{(\alpha)}, x_t^{(\alpha)}]$. Таким образом, для нахождения вектора $\bar{x}^{(\alpha)}$, минимизирующего $L_1(\bar{x})$ в условиях (24), достаточно рассмотреть случай, когда схема содержит ровно одну начальную точку. При этом и конечная точка должна быть одна, так как иначе в соответствующей схеме



последняя точка $a^{N-2}x_1$ является фактически второй начальной точкой. Осталось рассмотреть возможные случаи расположения начальной и конечной точек в схеме, включая случай, когда конечная точка является первой или последней точкой (при этом $r = 1$).

Рассмотрим случай, когда конечная точка $a^{N-r-1}x_r$ не совпадает с последними двумя точками схемы — $a^{N-3}x_2$ и $a^{N-2}x_1$:



В этом случае имеет место система неравенств

$$\begin{cases} (1/a^{j-1})x_j \leq \dots \leq (1/a)x_2 \leq x_1 \leq x_N \leq \dots \leq a^{N-m-1}x_m, \\ x_j \leq (1/a)x_{j+1} \leq \dots \leq (1/a^{m-j})x_m. \end{cases} \quad (33)$$

Как и в доказательстве леммы 1, легко убедиться в том, что необходимым для вектора $\bar{x}^{(\alpha)}$, минимизирующего $L_1(\bar{x})$, является условие, когда в неравенствах системы (33) достигаются равенства. Исключения составляют последние неравенства цепочек, которые можно записать в виде $ax_{r-1} \leq x_r$ и $x_{r+1} \leq ax_r$. Если бы выполнялись равенства в обоих этих неравенствах, мы получили бы противоречивое равенство $x_1 = a^{N-2}x_1$. Отсюда следует, что для координат вектора $\bar{x}^{(\alpha)}$ справедливо одно из трёх условий:

$$\begin{aligned} (1/a^{r-2})x_{r-1}^{(\alpha)} &= \dots = (1/a^j)x_{j+1}^{(\alpha)} = (1/a^{j-1})x_j^{(\alpha)} = \dots = \\ &= (1/a)x_2^{(\alpha)} = x_1^{(\alpha)} = x_N^{(\alpha)} = \dots = a^{N-m-1}x_m^{(\alpha)}, \end{aligned}$$

$$\begin{aligned} (1/a^{m-1})x_m^{(\alpha)} &= \dots = (1/a^j)x_{j+1}^{(\alpha)} = (1/a^{j-1})x_j^{(\alpha)} = \dots = \\ &= (1/a)x_2^{(\alpha)} = x_1^{(\alpha)} = x_N^{(\alpha)} = \dots = a^{N-r-2}x_{r+1}^{(\alpha)}, \end{aligned}$$

или

$$\begin{aligned} (1/a^{r-2})x_{r-1}^{(\alpha)} &= \dots = (1/a^j)x_{j+1}^{(\alpha)} = \dots = (1/a)x_2^{(\alpha)} = x_1^{(\alpha)} = x_N^{(\alpha)} = \dots = \\ &= a^{N-r-2}x_{r+1}^{(\alpha)} < a^{N-r-1}x_r^{(\alpha)}. \end{aligned}$$

Их можно переписать соответственно в виде

$$\begin{aligned} x_{r-1}^{(\alpha)} &= a x_{r-2}^{(\alpha)} = \dots = a^{r-3} x_2^{(\alpha)} = a^{r-2} x_1^{(\alpha)} = a^{r-2} x_N^{(\alpha)} = a^{r-2} x_{N-1}^{(\alpha)} = \dots = a^{N-3} x_r^{(\alpha)}, \\ x_r^{(\alpha)} &= a x_{r-1}^{(\alpha)} = \dots = a^{r-2} x_2^{(\alpha)} = a^{r-1} x_1^{(\alpha)} = a^{r-1} x_N^{(\alpha)} = a^{r-1} x_{N-1}^{(\alpha)} = \dots = a^{N-3} x_{r+1}^{(\alpha)}, \quad (34) \\ x_{r-1}^{(\alpha)} &= a x_{r-2}^{(\alpha)} = \dots = a^{r-3} x_2^{(\alpha)} = a^{r-2} x_1^{(\alpha)} = a^{r-2} x_N^{(\alpha)} = a^{r-2} x_{N-1}^{(\alpha)} = \dots = a^{N-4} x_{r+1}^{(\alpha)} < a^{N-3} x_r^{(\alpha)}. \end{aligned}$$

Заметим, что последний случай в (34), соответствующий тому, что в (33) последнее неравенство в каждой из двух цепочек строгое, невозможен. Дело в том, что в условиях (33) функция $L_1(\bar{x})$ имеет вид

$$L_1(\bar{x}) = p(x_m + \dots + x_{j+1} + x_N) + (1-p)(x_1 + \dots + x_{j-1} + x_m + \dots + x_{N-1}). \quad (35)$$

Поэтому действует тот же метод, приводящий к противоречию с условием выбора $\bar{x}^{(\alpha)}$, что и в лемме 1, а именно: достаточно рассмотреть вектор $\bar{x}'$, связанный с $\bar{x}^{(\alpha)}$ соотношениями $x'_s = x_s^{(\alpha)} + \varepsilon$ при $s \neq m$, $x'_m = x_m^{(\alpha)} - \varepsilon(N-1)$, выбрать ε таким, чтобы выполнялись условия (34), и сравнить значения $L_1(\bar{x}^{(\alpha)})$ и $L_1(\bar{x}')$, используя (35).

Каждый из двух оставшихся вариантов $\bar{x}^{(\alpha)}$ может быть получен путём разбиения множества точек схемы (26) на два подмножества, соответствующих двум цепочкам в (33), и последующего приравнивания значений точек в каждом подмножестве. Разбиение иллюстрируется схемой, на которой «разорвано» одно звено:

$$\begin{array}{ccccccc} \bullet & \bullet & & \bullet & \bullet & & \bullet \\ x_1 & x_N & \dots & a^{N-m-1} x_m & a^{N-m} x_{m-1} \dots a^{N-3} x_2 & a^{N-2} x_1 & \dots \end{array}$$

Таким «разорванным» звеном может быть любое из N звеньев схемы. Несложно проверить, что множество вариантов $\bar{x}^{(\alpha)}$ совпадает с множеством векторов, приведённых в формулировке леммы. Индекс α указывает номер (по счёту слева) «разрываемого» звена схемы. При этом охватываются и случаи, когда конечной точкой схемы является одна из точек $a^{N-3}x_2$ или $a^{N-2}x_1$. ■

Непосредственно проверяется

Лемма 3. Вектор $\bar{x}^{(\alpha)}$, $0 \leq \alpha \leq N-1$, определяемый условиями леммы 2, имеет следующие координаты:

$$x_1^{(0)} = \frac{2p-1}{p-(2-3p)a^{N-2}}, \dots, x_{N-2}^{(0)} = \frac{a^{N-3}(2p-1)}{p-(2-3p)a^{N-2}}, x_N^{(0)} = x_{N-1}^{(0)} = \frac{a^{N-2}(2p-1)}{p-(2-3p)a^{N-2}};$$

координаты $\bar{x}^{(1)}$ определяются формулами (16); при $2 \leq \alpha = k \leq N-1$

$$x_1^{(k)} = x_N^{(k)} = x_{N-1}^{(k)} = \frac{a^{k-2}(2p-1)}{p(1-a^{N-2}) + 2(2p-1)a^{k-2}}, \dots,$$

$$x_{N-k}^{(k)} = \frac{a^{N-3}(2p-1)}{p(1-a^{N-2}) + 2(2p-1)a^{k-2}},$$

$$x_{N-k+1}^{(k)} = \frac{2p-1}{p(1-a^{N-2}) + 2(2p-1)a^{k-2}}, \dots, x_{N-2}^{(k)} = \frac{a^{k-3}(2p-1)}{p(1-a^{N-2}) + 2(2p-1)a^{k-2}}.$$

Для доказательства теоремы 5 остаётся вычислить $L_1(\bar{x}^{(\alpha)})$ для указанных вариантов векторов $\bar{x}^{(\alpha)}$ и найти среди полученных значений минимальное. Чтобы сделать это, заметим, что координаты всех N векторов $\bar{x}^{(\alpha)}$ удовлетворяют системе неравенств (27).

При этом $L_1(\bar{x}^{(\alpha)}) = p - (2p - 1)x_N^{(\alpha)}$. Поэтому достаточно найти $\max_{0 \leq \alpha \leq N-1} x_N^{(\alpha)} = x_N^{(l)}$ и вычислить $L_1(\bar{x}^{(l)})$. Используя лемму 2, получаем

$$x_N^{(1)} - x_N^{(0)} = \frac{(2p - 1)[p - a^{N-2}(1 - pa^{N-1})]}{(3p - 1 - pa^{N-1})(p - (2 - 3p)a^{N-2})} > 0 \Leftrightarrow p - a^{N-2}(1 - pa^{N-1}) > 0.$$

Пусть $b = a^{N-2}$. Тогда

$$p - a^{N-2}(1 - pa^{N-1}) = (1 - p)b^2 - b + p > 0,$$

поскольку $0 < b < 1$, и корнями квадратного трёхчлена $(1 - p)b^2 - b + p$ являются $b_1 = 1$, $b_2 = 1/a > 1$. Аналогично

$$\begin{aligned} x_N^{(1)} - x_N^{(k)} &= \frac{(2p - 1)[p(1 - a^{N-2}) + 2(2p - 1)a^{k-2} - (3p - 1 - pa^{N-1})a^{k-2}]}{(3p - 1 - pa^{N-1})[p(1 - a^{N-2}) + 2(2p - 1)a^{k-2}]} > 0 \Leftrightarrow \\ &\Leftrightarrow p(1 - a^{N-2}) - a^{k-2}(1 - p - pa^{N-1}) > 0 \Leftrightarrow (1 - b)(p - a^{k-2}(1 - p)) > 0. \end{aligned}$$

Итак, $\max_{0 \leq \alpha \leq N-1} x_N^{(\alpha)} = x_N^{(1)}$ и $L_1(\bar{x}^{(1)})$ выражается формулой (23).

Вычислим оптимальную стратегию игрока 2 в игре G_2 . В ситуации $(\mathcal{P}, \mathcal{R})$ в смешанных стратегиях $\mathcal{P} = \mathcal{P}(E) = (p(e), e \in E)$ и $\mathcal{R} = \mathcal{R}(\Psi) = (r(\varphi), \varphi \in \Psi)$ значение игры выражается формулой

$$v_{G_2}(\mathcal{P}, \mathcal{R}) = \sum_{e \in E} \sum_{\varphi \in \Psi} p(e)\sigma(e, \varphi)r(\varphi),$$

где $\sigma(e, \varphi)$ выражается формулой (17). Для оптимальных стратегий $\mathcal{P}^0, \mathcal{R}^0$ получаем значение v_{G_2} игры: $v_{G_2} = v_{G_2}(\mathcal{P}^0, \mathcal{R}^0)$. Согласно теореме 2,

$$v_{G_2} = v_{\mathbf{S}} = \min_{\mathcal{P}} \sum_{m \in M} \mathbf{p}_{\mathbf{S}}(m)p_M(m),$$

где $p_M(m)$ выражается формулой (1), $\mathbf{p}_{\mathbf{S}}(n|m)$ — формулой (3), а $\mathbf{p}_{\mathbf{S}}(m) = \max_{n \neq m} \mathbf{p}_{\mathbf{S}}(n|m)$.

Напомним, что распределение $\mathcal{R}$ индуцирует совокупность $\mathcal{U} = \mathcal{U}(\mathcal{R}) = \{\mathcal{U}_m : m \in M\}$ распределений $\mathcal{U}_m = (u_{m,n}, n \in M \setminus \{m\})$, где $u_{m,n}$ — вероятность выбора сообщения n , подменяющего m , вычисляемая по формуле (9). В свою очередь, совокупность $\mathcal{U} = \{\mathcal{U}_m : m \in M\}$ распределений $\mathcal{U}_m$ индуцирует стратегию $\mathcal{R} = \mathcal{R}(\mathcal{U}) = (r(\varphi), \varphi \in \Psi)$ по формуле (10).

Согласно (13), $v_{\mathbf{S}}(\mathcal{P}, \mathcal{R}) = \bar{v}_{\mathbf{S}}(\mathcal{P}, \mathcal{U}(\mathcal{R}))$, где

$$\bar{v}_{\mathbf{S}}(\mathcal{P}, \mathcal{U}) = \sum_{m \in M} \sum_{n \neq m} p_M(m)\mathbf{p}_{\mathbf{S}}(n|m)u_{m,n}. \quad (36)$$

Представим (36) в следующем виде:

$$\bar{v}_{\mathbf{S}}(\mathcal{P}, \mathcal{U}) = \sum_{e \in E} p(e)c_e(\mathcal{U}),$$

где $c_e(\mathcal{U}) = \sum_{\substack{m, n \in e(S), \\ n \neq m}} u_{m,n} \cdot p_S(e^{-1}(m))$. Пусть $c_{e_0}(\mathcal{U}) = \min_{e \in E} c_e(\mathcal{U})$. Как и в теореме 2,

можно показать, что

$$v_{\mathbf{S}} = \max_{\mathcal{U}} \bar{v}_{\mathbf{S}}(\bar{\mathcal{P}}(\mathcal{U}), \mathcal{U}) = \max_{\mathcal{U}} c_{e_0}(\mathcal{U}), \quad (37)$$

где $\bar{P}(\mathcal{U}) = (\bar{p}(e), e \in E)$ — чистая стратегия, такая, что

$$\bar{p}(e) = \begin{cases} 1, & \text{если } e = e_0, \\ 0, & \text{если } e \neq e_0. \end{cases}$$

Вычислим максимум (37). Для этого введём обозначения $y_{i,j} = u_{m_i, m_j}$, $i, j = 1, \dots, N$. По матрице кодирования (16) находим

$$\begin{aligned} c_{e_1}(\mathcal{U}) &= y_{1,2}p + y_{2,1}(1-p), \quad c_{e_2}(\mathcal{U}) = y_{2,3}p + y_{3,2}(1-p), \quad \dots, \\ c_{e_{N-1}}(\mathcal{U}) &= y_{N-1,N}p + y_{N,N-1}(1-p), \quad c_{e_N}(\mathcal{U}) = y_{1,N}p + y_{N,1}(1-p). \end{aligned}$$

Таким образом,

$$c_{e_0}(\mathcal{U}) = \min \{y_{1,2}p + y_{2,1}(1-p), \dots, y_{N-1,N}p + y_{N,N-1}(1-p), y_{1,N}p + y_{N,1}(1-p)\},$$

где переменные $y_{i,j}$ удовлетворяют условиям

$$0 \leq y_{i,j} \leq 1, \quad y_{i,i+1} + y_{i,i-1} = 1, \quad i = 1, \dots, N-1, \quad y_{N,1} + y_{N,N-1} = 1. \quad (38)$$

Пусть без ограничения общности $c_{e_1}(\mathcal{U}) \leq c_{e_2}(\mathcal{U}) \leq \dots \leq c_{e_N}(\mathcal{U})$. Тогда $c_{e_0}(\mathcal{U}) = c_{e_1}(\mathcal{U})$. Максимальное значение величина $c_{e_0}(\mathcal{U})$ принимает, когда в неравенствах (38) достигаются равенства. Получаем систему уравнений

$$y_{1,2} + y_{2,1}a = \dots = y_{N-1,N} + y_{N,N-1}a = y_{1,N} + y_{N,1}a. \quad (39)$$

Рассмотрим сначала случай, когда $p > 0,5$. В этом случае $a < 1$. Выразим из системы (39) $y_{k,k-1}$ через $y_{1,2}, y_{2,1}$:

$$y_{k,k-1} = y_{1,2} \frac{1-a^{k-2}}{(1-a)a^{k-2}} + y_{2,1} \frac{1-a^{k-1}}{(1-a)a^{k-2}} - \frac{1-a^{k-2}}{(1-a)a^{k-2}}, \quad k = 3, \dots, N. \quad (40)$$

Из равенств $y_{1,2} + y_{2,1}a = y_{1,N} + y_{N,1}a$ и $y_{N,1} + y_{N,N-1} = 1$ получаем выражение

$$y_{N,N-1} = \frac{a+1}{a} - \frac{2}{a}y_{1,2} - y_{2,1}. \quad (41)$$

Приравнявая выражения $y_{N,N-1}$ из (40), (41), получаем соотношение

$$y_{1,2} = \frac{1+a^{N-3}-a^{N-2}-a^{N-1}}{1+2a^{N-3}-3a^{N-2}} - y_{2,1} \frac{1+a^{N-2}-2a^{N-1}}{1+2a^{N-3}-3a^{N-2}}. \quad (42)$$

Нас интересует величина $c_{e_0}(\mathcal{U}) = p(y_{1,2} + y_{2,1}a)$. Из (42) находим

$$y_{1,2} + y_{2,1}a = \frac{1+a^{N-3}-a^{N-2}-a^{N-1}}{1+2a^{N-3}-3a^{N-2}} - y_{2,1} \frac{1-a-a^{N-2}+a^{N-1}}{1+2a^{N-3}-3a^{N-2}}. \quad (43)$$

Максимум $\max_{\mathcal{U}} c_{e_0}(\mathcal{U})$ совпадает с $\max_{y_{i,j} \in (38)} p(y_{1,2} + y_{2,1}a)$, где переменные $y_{i,j}$ удовлетворяют условиям (38). Поскольку в (43) дроби представляют собой положительные величины (при условии $a < 1$), сумма $y_{1,2} + y_{2,1}a$ принимает максимальное значение при минимально возможном $y_{2,1}$. Найдём такое $y_{2,1}$, исходя из условий (38). Для этого воспользуемся условиями $0 \leq y_{i,j} \leq 1$. Из (42) получаем неравенства

$$0 \leq \frac{1+a^{N-3}-a^{N-2}-a^{N-1}}{1+2a^{N-3}-3a^{N-2}} - y_{2,1} \frac{1+a^{N-2}-2a^{N-1}}{1+2a^{N-3}-3a^{N-2}} \leq 1,$$

откуда следует оценка

$$y_{2,1} \geq \frac{2a^{N-2} - a^{N-3} - a^{N-1}}{1 + a^{N-2} - 2a^{N-1}}. \quad (44)$$

При $a < 1$ величина в правой части (44) отрицательна. Это означает, что в условиях $0 \leq y_{1,2} \leq 1$ минимальное значение $y_{2,1}$ равно нулю.

Аналогично из (40) получаем неравенства

$$y_{2,1} \geq \frac{a^{N-k-1}(1-a)(1-a^{k-2})}{1 + 2a^{N-k-1} - 2a^{N-k} - a^{N-2}}, \quad k = 3, \dots, N. \quad (45)$$

Правая часть в (45) как функция от k монотонно убывает и достигает минимума при $k = N$. Таким образом, в условиях $0 \leq y_{k,k-1} \leq 1$, $k = 3, \dots, N$, минимальное значение $y_{1,2}$ равно

$$\frac{(1-a)(1-a^{N-2})}{2-a-a^{N-1}}. \quad (46)$$

Остаётся рассмотреть ограничение на $y_{1,2}$, которое дают условия $0 \leq y_{1,N} \leq 1$. Из равенств (42), $y_{1,2} + y_{1,N} = 1$ и условий $0 \leq y_{1,N} \leq 1$ получаем неравенства

$$0 \leq y_{2,1} \frac{2-2a+a^2-a^N}{a(1+2a^{N-3}-3a^{N-2})} - \frac{(1-a)^2(1-2a^{N-2})}{a(1+2a^{N-3}-3a^{N-2})} \leq 1,$$

откуда следует оценка

$$y_{2,1} \geq \frac{(1-a)^2(1-2a^{N-2})}{2-2a+a^2-a^N}. \quad (47)$$

Сравнивая полученные оценки, убеждаемся, что оценка (47) слабее оценки (46). Отсюда следует, что минимальное значение $y_{2,1}$ выражается дробью (46), а

$$\max_{y_{i,j} \in (21)} p(y_{1,2} + y_{2,1}a) = \frac{p(1+a-a^2-a^{N-1})}{2-a-a^{N-1}}. \quad (48)$$

Мы получили значение игры v_{G_2} . Нетрудно проверить, что правая часть в (48) совпадает с правой частью в (20). Отсюда получаем и значения переменных $y_{i,j}$, на которых достигается максимум (48). Они приведены в (19).

Заметим, что мы вычислили значение игры двумя независимыми способами (находя минимакс и максимум) и при этом получили одинаковые результаты. Это означает, в частности, что G_2 — это действительно игра с нулевой суммой.

В случае, когда $p = 0,5$, из (39) аналогично получаем соотношения

$$y_{1,N} = y_{2,1} = \dots = y_{N,N-1} = \alpha, \quad y_{N,1} = y_{1,2} = \dots = y_{N-1,N} = 1 - \alpha,$$

где α — произвольное действительное число из $[0, 1]$.

Подставляя полученные значения $y_{i,j}$ в (22), находим оптимальную смешанную стратегию второго игрока в игре G_2 . Эта стратегия приведена в условиях теоремы 5. Это завершает доказательство теоремы. ■

Отметим, что классы рассмотренных в теоремах 3–5 матричных игр, для которых можно вычислить значение игры, можно расширить. Например, хорошо известно [8], что значение матричной игры не изменяется при добавлении к матрице выигрышей строк и столбцов, которые доминируются строками и столбцами матрицы. Например,

при $N = 3$ и $p = 0,6$ добавлением двух строк к матрице (18), которые доминируются первыми двумя строками матрицы (18), получаем матрицу

$$\begin{pmatrix} 0,6 & 0,6 & 1 & 1 & 0 & 0 & 0,4 & 0,4 \\ 0,6 & 0 & 0,6 & 0 & 1 & 0,4 & 1 & 0,4 \\ 0,4 & 1 & 0 & 0,6 & 0,4 & 1 & 0 & 0,6 \\ 0 & 0,5 & 0,3 & 0,2 & 0 & 0 & 0,1 & 0,3 \\ 0,1 & 0 & 0,5 & 0 & 0,8 & 0,4 & 0,9 & 0,1 \end{pmatrix}.$$

Игра с такой матрицей выигрышей имеет то же значение, что и игра с матрицей (18). Согласно теореме 5, это значение выражается формулой (20) и равно $21/40$.

Заключение

Предлагается метод решения матричных игр, ассоциированных с кодами аутентификации. Метод иллюстрируется примерами решений двух частных классов матричных игр. Метод даёт возможность расширить круг «решаемых игр» за счёт аналогичных вычислений для других А-кодов.

ЛИТЕРАТУРА

1. Зубов А. Ю. Может ли комбинация активных атак привести к большему ущербу для системы защиты информации, чем каждая из атак в отдельности? // Лесной вестник. 2008. № 4(61). С. 144–148.
2. Зубов А. Ю. Решение одной матричной игры // Лесной вестник. 2008. № 6(63). С. 173–179.
3. Зубов А. Ю. К теоретико-игровому подходу исследования кодов аутентификации // Дискретная математика. 2009. Т. 21. Вып. 3. С. 45–72.
4. Зубов А. Ю. О выборе оптимальной стратегии защиты для кода аутентификации с двумя состояниями источника // Дискретная математика. 2009. Т. 21. Вып. 4. С. 135–147.
5. Simmons G. J. A game theoretical model of digital message authentication // Congressus Numerantium. 1982. V. 34. P. 413–424.
6. Simmons G. J. Authentication theory / Coding theory // LNCS. 1984. V. 196. P. 411–431.
7. Зубов А. Ю. Математика кодов аутентификации. М.: Гелиос АРВ, 2007.
8. Воробьёв Н. Н. Теория игр. М.: Наука, 1985.

REFERENCES

1. Zubov A. Yu. Mozhet li kombinatsiya aktivnykh atak privesti k bol'shemu ushcherbu dlya sistemy zashchity informatsii, chem kazhdaya iz atak v otdel'nosti? [Can combination of the active attacks to bring about greater damage for system of protection to information, than each of attacks separately?]. Moscow State Forest University Bulletin — Lesnoy Vestnik, 2008, no. 4(61), pp. 144–148. (in Russian)
2. Zubov A. Yu. Reshenie odnoy matrichnoy igry [The decision of one matrix game]. Moscow State Forest University Bulletin — Lesnoy Vestnik, 2008, no. 6(63), pp. 173–179. (in Russian)
3. Zubov A. Yu. K teoretiko-igrovomu podkhodu issledovaniya kodov autentifikatsii [On the game-theoretical approach to the analysis of authentication codes]. Diskr. Mat., 2009, vol. 21, iss. 3, pp. 45–72. (in Russian)
4. Zubov A. Yu. O vybere optimal'noy strategii zashchity dlya koda autentifikatsii s dvumya sostoyaniyami istochnika [On the choice of the defence strategy for an authentication code with two-state source]. Diskr. Mat., 2009, vol. 21, iss. 4, pp. 135–147. (in Russian)
5. Simmons G. J. A game theoretical model of digital message authentication. Congressus Numerantium, 1982, vol. 34, pp. 413–424.
6. Simmons G. J. Authentication theory / Coding theory. LNCS, 1984, vol. 196, pp. 411–431.

7. Zubov A. Yu. Matematika kodov autentifikatsii [Authentication Codes Mathematics]. Moscow, Gelios ARV Publ., 2007. (in Russian)
8. Vorob'ev N. N. Teoriya igr [Game Theory]. Moscow, Nauka Publ., 1985. (in Russian)