Математическая Теория Игр и её Приложения, т.11, в.1, с. 21–38

УДК 519.833.2
ББК 22.18

РАСШИФРОВКА СИГНАЛОВ С ПОМОЩЬЮ КОНЕЧНЫХ АВТОМАТОВ: ПРИМЕНЕНИЕ К ИГРАМ С НЕПОЛНОЙ ИНФОРМАЦИЕЙ*

Михаил Р. Гаврилович
Виктория Л. Крепс
Институт проблем региональной экономики РАН
190013, Санкт-Петербург, ул. Серпуховская, 38
НИУ Высшая школа Экономики
194100, Санкт-Петербург, ул. Кантемировская, 3
e-mail: mishap@sdf.org, vita_kreps@mail.ru

Рассматриваются матричные игры с неполной информацией у обеих сторон и публичным сигналом о состоянии игры, представленным бинарным кодом фиксированной длины. Доступные игрокам стратегии ограничены возможностями конечных автоматов разных размеров: m для Игрока 1 и n для Игрока 2, причем $m \gg n$. Получены оценки размеров m (нижняя граница) и n (верхняя граница), при которых исходная игра с неполной информацией у обеих сторон может превратиться в игру с неполной информацией у Игрока 2.

Ключевые слова: матричная игра, неполная информация, асимметрия, бинарный код, конечные автоматы.

Поступила в редакцию: 15.09.18 *После доработки*: 24.01.19 *Принята к публикации*: 20.03.19

---

* Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ в 2018 году и Программы фундаментальных научных исследований государственных академий наук на 2013-2020 годы, ИПРЭ РАН, пункт 169, а также при частичной поддержке РФФИ, проект 16-01-00124-а. Авторы благодарны анонимному рецензенту за ценные замечания и советы.

1. Введение

В работах по повторяющимся играм с неполной информацией обычно предполагается, что игроки имеют неограниченный вычислительный потенциал. Поскольку на практике это предположение не выполняется, представляет интерес изучение того, как отсутствие этого предположения сказывается на теоретических выводах.

Мы рассматриваем матричные игры с неполной информацией у обоих игроков. Такая игра задается двумя квадратными матрицами выигрышей одинакового размера. Перед началом игры случайный ход выбирает одно из двух возможных «состояний природы» и тем самым матрицу выигрышей. Оба игрока не знают результат случайного хода и, тем самым не знают, какая игра разыгрывается. Они знают лишь вероятность выбора состояния (см. [1]).

О состоянии игры поступает публичный сигнал, который полностью определяет состояние игры. Сигнал представлен бинарным (двоичным) кодом, то есть строкой из нулей и единиц. Отметим, что такая кодировка используется практически во всех современных компьютерах и прочих вычислительных электронных устройствах.

Мы предполагаем, что игроки обладают ограниченными вычислительными ресурсами, причем вычислительный ресурс Игрока 1 мощнее вычислительного ресурса Игрока 2. Рассматриваемая нами модель ограниченных вычислительных ресурсов аналогична модели Неймана [6], [7]: доступные игрокам стратегии ограничены возможностями детерминированных конечных автоматов разных размеров. Размер конечного автомата – это число вершин соответствующего графа.

Интуитивно ясно, что благодаря преимуществу в вычислительных ресурсах, при некоторых размерах доступных игрокам автоматов Игрок 1 может декодировать сигнал и узнать состояние игры, в то время, как Игрок 2 не в состоянии получить этой информации. И таким образом, игра, в которой изначально игроки обладали симметричной неполной информацией, может превратиться в игру с неполной информацией у Игрока 2.

В работе [2] мы рассмотрели класс случайных сигналов с фиксированной длиной L исходящих бинарных строк. В упомянутой работе дана оценка снизу размера доступных Игроку 1 автоматов, позволя-

ющего ему безошибочно декодировать любой сигнал из этого класса и узнать состояние игры. Здесь мы даем существенно лучшую оценку для этого размера. Например, при равновероятных состояниях и большем трех числе символов в строке новая оценка снизу размера такого автомата приблизительно в $L/2$ раз меньше предыдущей оценки.

Также в настоящей работе мы даем оценку сверху для размера доступных Игроку 2 автоматов, при котором Игрок 2 не может безошибочно декодировать любой сигнал из рассматриваемого класса: найдется такой сигнал, что любой конечный автомат данного размера не может безошибочно расшифровать этот сигнал.

Таким образом, если размер доступного Игроку 1 автомата превышает найденную нижнюю границу для безошибочного декодирования, а размер доступного Игроку 2 автомата меньше найденной оценки, гарантирующей наличие сигнала, не подлежащего расшифровке, то найдется публичный сигнал из рассматриваемого класса, при котором исходная игра с неполной информацией у обеих сторон превратится в игру с неполной информацией у Игрока 2.

Полученные результаты показывают, что состояние игры может быть обнаружено одним из игроков не только благодаря его приватной информации, но также как результат публичного сигнала и асимметричных вычислительных ресурсов игроков.

2. Модель

Поскольку нас интересует лишь обнаружение информации до момента начала игры, суть игры и, в частности, число шагов игры не существенно. В наших рассмотрениях мы ориентируемся на классические модели одношаговой игры с неполной информацией у обеих сторон и одношаговой игры с неполной информацией у одной из сторон (см. [3] и [1]).

Обозначим $\mathcal{A}(p)$ одношаговую матричную игру с неполной информацией у обеих сторон. Игра задается двумя квадратными матрицами выигрыша A_1 и A_2. одинакового размера. Перед началом игры случайный ход определяет «состояние природы» $k \in K = \{1, 2\}$ и тем самым матрицу выигрышей A_k: с вероятностью p разыгрывается матричная игра A_1 и с вероятностью $1 - p$ разыгрывается матрич-

ная игра A_2. Оба игрока знают вероятность p и не знают результат случайного хода.

Рассмотрим игру $\mathcal{A}_f^{m,n}(p)$, которая является модификацией игры $\mathcal{A}(p)$. Здесь f – публичный сигнал о состоянии игры $\mathcal{A}(p)$, m – максимальный размер конечных автоматов, доступных Игроку 1, а n – максимальный размер конечных автоматов, доступных Игроку 2, причем $m \gg n$.

Сигнал f – функция от состояния игры (от случайной переменной), $f(k)$, $k = 1, 2$. Область значений функции f – некоторое множество бинарных строк (строк, состоящих из символов 0 и 1).

Функция f известна обоим игрокам. Используя это знание, каждый игрок выбирает конечный автомат. Игрок 1 выбирает произвольный автомат (Автомат 1) размера, не превышающего m, а Игрок 2 выбирает произвольный автомат (Автомат 2) размера, не превышающего n. Оба игрока знают размер автомата противника.

При выборе автомата игрок может использовать следующий алгоритм полного перебора. Каждому автомату соответствующего размера игрок задает на входе функцию $f(k)$, $k = 1, 2$. Если находится автомат, который на выходе дает k, то игрок выбирает этот автомат. В противном случае игрок выбирает автомат, у которого вероятность получить на выходе k при входе $f(k)$, $k = 1, 2$ максимальна. Тем самым игрок выбирает автомат, который наилучшим образом расшифровывает сигнал.

После того, как игроки сделали выбор, игра посылает публичный сигнал $f(k)$, $k = 1, 2$, получив который, выбранные автоматы «вычисляют» свои ответы на этот сигнал.

Ответ Автомата i интерпретируется Игроком i как указание на состояние игры $\mathcal{A}_f^{m,n}(p)$.

Подробное описание конечных автоматов и чтения их диаграмм см. [9] и [4]. Автомат задается с помощью связного направленного графа с конечным множеством вершин.

- Одна из вершин v_0 является *начальной* вершиной.
- Каждая вершина помечена либо единицей, либо двойкой.
- Из каждой вершины выходит ровно две дуги, одна из них помечена нулем, а другая единицей.

- Нет ограничений на число дуг, входящих в вершину.
- Разрешены петли, то есть дуги, которые входят в ту же вершину, из которой они вышли.

Вычисление автоматом происходит следующим образом: автомат получает от игры сигнал – строку $s_1 \dots s_l$, состоящую из нулей и единиц. Автомат читает символы строки последовательно, один за другим. Он начинает с начальной вершины v_0 и, прочитав символ s_1, двигается к вершине v_1 по единственной дуге, выходящей из v_0 и помеченной символом s_1. Затем, прочитав символ s_2, двигается к вершине v_2 по единственной дуге, выходящей из v_1 и помеченной символом s_2 и так далее...

Таким образом, существует единственный начинающийся в начальной вершине v_0 путь по дугам

$$v_0 \xrightarrow{s_1} v_1 \xrightarrow{s_2} v_2 \xrightarrow{s_3} \dots \xrightarrow{s_{l-1}} v_{l-1} \xrightarrow{s_l} v_l$$

такой, что переход от вершины v_{i-1} к вершине v_i помечен символом s_i, $1 \le i \le l$. Ответ автомата – метка конечной вершины v_l этого пути, которая в нашем контексте интерпретируется как состояние игры.

Лемма 2.1. *Для любого m количество конечных автоматов размера не больше m не превосходит*

$$\frac{2^m m^{2m}}{(m-1)!}.$$

Доказательство. Расширим множество графов, соответствующих конечным автоматам размера m, добавив размеченные ориентированные графы с общим числом вершин m, в которых допустимы недостижимые вершины. Легко видеть, что число конечных автоматов размера, не превосходящего m, не превосходит число таких графов.

Подсчитаем точное количество таких графов. Сначала занумеруем m вершин графа, присвоив, как и прежде, начальной вершине номер 0. Есть $(m-1)!$ способов это сделать.

Для каждой из m вершин есть m^2 способов добавить исходящие из этой вершины два ребра. Так как они могут быть помечены 0 или 1, это дает m^{2m} вариантов выбора ребер. Отметим, что при этом могут возникнуть недостижимые вершины.

Каждая из m вершин помечена либо 1, либо 2. Это дает 2^m вариантов разметки вершин. В результате получаем $2^m m^{2m}$ графов.

Далее отметим, что каждый такой граф мы посчитали $(m-1)!$ раз, так как число различных способов занумеровать вершины равно $(m-1)!$. Таким образом, мы получаем, что число таких графов равно $\frac{2^m m^{2m}}{(m-1)!}$, что доказывает утверждение леммы. □

3. Сигналы с фиксированной длиной строк

Далее рассматривается класс сигналов f с фиксированной длиной L исходящих строк. Таким образом, $f : \{1,2\} \to S$, где $S = \{0,1\}^L$ состоит из 2^L элементов.

Сигнал $f(p)$ определяется разбиением множества S на два непустых подмножества $S_1(p)$ и $S_2(p)$

$$S = S_1(p) \cup S_2(p),\ S_1(p) \cap S_2(p) = \emptyset$$

(число таких разбиений равно 2^{2^L}) и вероятностными распределениями на $S_k(p)$, $k = 1,2$, согласно которым сигнал $f(p)$ выдает строку $s \in S_k(p)$, $k = 1,2$. Непустота множеств $S_k(p)$ означает, что мы не рассматриваем крайние случаи, когда $p = 0$ или $p = 1$, которые соответствуют отсутствию неопределенности о состоянии игры.

В работе [2] в предположении, что сигнал $f(p)$ использует равномерные распределения на множествах $S_k(p)$, $k = 1,2$, при малом размере автомата мы оценили долю сигналов рассматриваемого класса, с помощью которых игрок, не имея возможности узнать состояние игры, все же может существенно переоценить априорную вероятность состояния игры.

Для поставленной в данной работе задачи полного определения сигнала мы от распределений на $S_1(p)$ и $S_2(p)$ лишь требуем, чтобы вероятность каждого элемента множеств $S_1(p)$ и $S_2(p)$ была положительна. Отметим, что результаты данной работы (оценки в Теоремах 1 и 2) не зависят от выбранных распределений такого вида. Если предположить, что значительное число элементов множеств $S_1(p)$ и $S_2(p)$ имеют нулевую вероятность, то оценки изменятся. В вырожденном случае, когда в каждом из множеств $S_1(p)$ и $S_2(p)$ имеется лишь по одному элементу с ненулевой вероятностью, то для расшифровки всех таких сигналов достаточен автомат размера L, в то время как

в рассматриваемом нами случае размер автомата экспоненциально зависит от длины строки L.

Естественно полагать, что при разбиении множества S на подмножества $S_1(p)$ и $S_2(p)$, соответствующие состояниям 1 и 2, число элементов этих подмножеств пропорционально вероятностям состояний 1 и 2, то есть $card(S_1(p)) = p2^L$ и $card(S_2(p)) = (1-p)2^L$. Для упрощения расчетов мы рассматриваем случай, когда $p2^L$ целое число. Таким образом, $p = a/2^k$, где $a/2^k < 1$ — несократимая дробь и $k \leq L$. Следовательно, для вероятности p состояния 1 выполняется неравенство $min(p, 1-p) \geq 1/2^L$. Имеется $\binom{p2^L}{2^L}$ различных разбиений такого вида (различных сигналов).

Обозначим $f^{S_1(p),S_2(p)}$ сигнал, соответствующий разбиению множества S на подмножества $S_1(p)$ и $S_2(p)$.

Множество сигналов f вида $f^{S_1(p),S_2(p)}$ обозначим $\mathcal{F}(p)$.

Вот пример такого сигнала при $p = 1/2$ и нечетном L. Сигнал определяется следующим образом: $f(1)$ принимает значения случайно и равномерно из множества таких строк длины L, в которых число единиц больше половины или, что то же самое, число нулей меньше половины; $f(2)$ принимает значения случайно и равномерно из множества таких строк длины L, в которых число единиц меньше половины или, что то же самое, число нулей больше половины. Рассмотрим конечный автомат с $(L+1)/2+1$ вершинами $v_0, v_1, \ldots, v_{(L+1)/2}$. Дуга с меткой 1, выходящая из вершин v_i входит в вершину v_{i+1}, а дуга с меткой 0, выходящая из вершин v_i, образуя петлю, входит в ту же вершину v_i. Здесь $i = 0, 1, \ldots, (L-1)/2$. Оба ребра, выходящие из вершины $v_{(L+1)/2}$, являются петлями (входят в ту же вершину $v_{(L+1)/2}$). В вершине $v_{(L+1)/2}$ стоит метка 2, во всех остальных вершинах – метка 1. Таким образом, если чтение сигнальной строки приводит в вершину $v_{(L+1)/2}$, то это указывает на состояние 2, в противном случае – на состояние 1. Такой автомат безошибочно распознает приведенный сигнал, и не существует конечного автомата меньшего размера, который способен безошибочно распознавать этот сигнал.

4. Нижняя граница размера автомата, декодирующего все сигналы

В работе [2] дана следующая оценка снизу такого размера доступных Игроку 1 автоматов, который позволяет ему безошибочно

расшифровать любой сигнал из класса $\mathcal{F}(p)$.

Утверждение. *Пусть вероятность $p \in (0,1)$ фиксирована. Если для размера m доступных Игроку 1 автоматов выполняется неравенство $m \geq m(p) = min(p, 1-p)L2^L$, то для любого сигнала $f \in \mathcal{F}(p)$ Игрок 1 может выбрать конечный автомат, который безошибочно расшифровывает этот сигнал.*

Отметим, что при $p = 1/2^k$ справедливо $m(1/2^k) = L2^{L-k}$, и в случае наибольшей неопределенности $p = 1/2$ имеет место равенство $m(1/2) = L \cdot 2^{L-1}$.

Здесь мы даем существенно лучшую оценку для этого размера.

Теорема 4.1. *Фиксируем число $L \geq 3$ – длину случайной строки и вероятность p, $min(p, 1-p) \geq 1/2^L$. Если размер m автоматов, доступных Игроку 1, больше или равен $\tilde{m}(p)$, где*

$$\tilde{m}(p) = min(p,1-p)Ent(-log_2(min(p,1-p)))2^L + 2^{L-Ent(-log_2 min(p,1-p))} + 1, \quad (1)$$

то для любого сигнала $f \in \mathcal{F}(p)$ в распоряжении Игрока 1 есть автомат, который безошибочно различает этот сигнал. Здесь $Ent(x)$ целая часть числа x.

Замечание 1. При $p = 1/2^k$, $k \leq L$ формула (1) приобретает вид

$$\tilde{m}(1/2^k) = (k+1)2^{L-k} + 1.$$

и, в частности, при $p = 1/2$ имеем $\tilde{m}(1/2) = 2^L + 1$, в то время как оценка, полученная в [2], дает $m(1/2) = L \cdot 2^{L-1}$, что приблизительно в $L/2$ раз больше. Например, при $L = 6$ и $p = 1/2$ результат Теоремы 1 гарантирует расшифровку любого сигнала при размере доступных Игроку автоматов, превышающем 65, в то время, как оценка, полученная в [2], дает такую гарантию лишь, если размер доступных Игроку автоматов больше 192.

Доказательство. Сигналу f поставим в соответствие сигнальную функцию $f^{-1} : \{0,1\}^L \to \{1,2\}$, такую что для $s \in S_k$ справедливо $f^{-1}(s) = k$. Обозначим $g_A : \{0,1\}^L \to \{1,2\}$ функцию, вычисляемую конечным автоматом A.

Фиксируем произвольный сигнал $f \in \mathcal{F}(p)$ и в явном виде построим конечный автомат размера $\tilde{m}(p)$, использование которого позволяет Игроку 1 безошибочно определять состояние игры $\mathcal{A}_f^{m,n}(p)$. А именно, мы построим автомат A, для которого $g_A(s) = f^{-1}(s)$ для любого $s \in S$.

Мы начнем с построения конечного автомата большего размера, а именно размера $2^{L+1} - 1$, обладающего требуемым свойством. Построение проводим следующим образом. Направленный граф автомата это — направленное дерево высоты L. Возьмем произвольное слово $s = (s_1, \ldots, s_L) \in S = \{0,1\}^L$ и, начиная с начальной вершины, построим путь из L дуг и L вершин, в котором дуги последовательно помечены также, как и соответствующие биты слова s. Конечную вершину (уровень L) пометим символом $f^{-1}(s)$.

Добавим дугу, выходящую из вершины уровня $L-1$, то есть вершины, предшествовавшей конечной. Пометим новую дугу как $s'_L = s_L + 1(mod 2)$ и новую конечную вершину пометим символом $f^{-1}(s')$, где $s' = (s_1, \ldots, s_{L-1}, s'_L)$. Поднимемся на уровень $L-2$ и добавим дугу, выходящую из вершины уровня $L-2$, пометив ее символом $s'_{L-1} = s_{L-1} + 1(mod 2)$. Из полученной новой вершины уровня $L-1$ выведем две дуги, одну пометим символом 0, а другую символом 1. Образовавшиеся две новые конечны вершины пометим, соответственно, символами $f^{-1}(s_1, \ldots, s_{L-2}, s'_{L-1}, 0)$ и $f^{-1}(s_1, \ldots, s_{L-2}, s'_{L-1}, 1)$. И так далее, переходя к вершинам уровня с меньшим номером, получим автомат размера

$$1 + 2 + 2^2 + \ldots + 2^L = 2^{L+1} - 1,$$

безошибочно различающий сигнал f. Отметим, что при таком построении метки на вершинах, соответствующих более коротким строкам $s \in \{0,1\}^l$, $l < L$, не существенны, так как все исходящие строки сигнала имеют фиксированную длину L.

Из построенного автомата (графа) мы можем удалить некоторые вершины с сохранением свойства безошибочного различения сигнала f. Начинаем с анализа конечных вершин — вершин уровня L. Если две конечные вершины, соответствующие дугам, выходящим из одной вершины уровня $L-1$, помечены одним и тем же символом, то мы можем удалить обе конечные вершины, пометив этим символом вершину уровня $L-1$, которая стала конечной. После удаления

всех таких пар конечных вершин перейдем к уровню $L-1$. Среди конечных вершин уровня $L-1$, снова могут найтись две вершины с одинаковой меткой, которые соответствуют дугам, выходящим из одной вершины уровня $L-2$. Удалив все такие пары и пометив новые конечные вершины уровня $L-2$ меткой удаленной пары, перейдем к уровню $L-2$. И так далее ...

Когда не найдется пригодных для удаления пар, посмотрим на финальное множество конечных вершин. Склеим в одну вершину все конечные вершины, помеченные единицей и аналогично поступим с конечными вершинами, помеченными двойкой.

Для сигналов рассматриваемой формы $f \in \mathcal{F}(p)$, в которых число конечных вершин (вершин уровня L) с меткой 1 равно $p2^L = a2^{L-k}$, где $k \le L$, $a < 2^k$, можно вычислить число оставшихся при такой процедуре вершин.

Ради простоты проведем подсчет для случая $p = 1/2^k$, $k \le L$. В этом случае на уровне L среди 2^L конечных вершин имеется 2^{L-k} вершин с меткой 1 и большее количество, а именно, $(2^k-1)2^{L-k}$ конечных вершин с меткой 2.

Вариант, при котором мы можем удалить наименьшее количество конечных вершин, это когда каждая конечная вершина с меткой 1 «находится в паре» с конечной вершиной, помеченной символом 2 (приводящие к ним дуги исходят из одной вершины уровня $L-1$). Максимальное число таких пар равно 2^{L-k} (числу конечных вершин с пометкой 1) и, соответственно, число вершин, входящих в такие пары и не подлежащих удалению, равно 2^{L-k+1}. В этом случае оставшиеся конечные вершины с меткой 2 ($(2^{k-1}-1)2^{L-k+1}$ штук) мы можем удалить, пометив символом 2 вершины уровня $L-1$, соответствующие удаленным вершинам.

Кроме этих вершин уровня $L-1$ ($(2^{k-1}-1)2^{L-k}$ штук), которые теперь стали конечными, на уровне $L-1$ имеется еще 2^{L-k} вершин. В худшем для уменьшения вершин случае, каждая из этих 2^{L-k} вершин "находится в паре" с одной из новых конечных вершин, имеющих метку 2. Таким образом, мы можем удалить

$$2^{L-k+1}(2^{k-2}-1)$$

вершин с меткой 2, пометив символом 2 вершины уровня $L-2$

($2^{L-k}(2^{k-2}-1)$ штук), соответствующие удаленным вершинам. При этом на уровне $L-1$ останется 2^{L-k} конечных вершин.

И так далее до тех пор, пока на некотором уровне после удаления вершин на уровне с большим номером число новых конечных вершин окажется меньше, чем 2^{L-k}. Последним уровнем, на котором возможно удаление, будет уровень $L-(k-2)$, на котором будет удалено 2^{L-k+1} вершин и, соответственно, на уровне $L-(k-1)$ появится 2^{L-k} новых конечных вершин с меткой 2. Начиная с этого уровня, описанная процедура удаления становится невозможной. Таким образом, суммарное количество удаленных вершин равно

$$2^{L-k+1}[2^k-k-1] = 2^{L+1} - (k+1)2^{L-k+1},$$

и после вычитания числа всех удаленных вершин из общего количества вершин, равного $2^{L+1}-1$, число оставшихся в графе вершин равно

$$(k+1)2^{L-k+1} - 1.$$

Перейдем к последнему этапу уменьшения вершин в графе. Подсчитаем количество конечных вершин в графе, оставшемся после удалений: на уровне L осталось 2^{L-k+1} конечных вершин и на каждом из $(k-1)$ уровней $L-1,\ldots,L-(k-1)$ появилось 2^{L-k} новых конечных вершин. В сумме получим $2^{L-k}(k+1)$ конечных вершин. Склеим в одну вершину все конечные вершины, помеченные единицей и аналогично поступим с конечными вершинами, помеченными двойкой. При этом количество вершин в графе уменьшится на $2^{L-k}(k+1)-2$, и в итоге мы получим

$$(k+1)2^{L-k+1} - 1 - 2^{L-k}(k+1) + 2 = (k+1)2^{L-k} + 1,$$

что и требовалось доказать. □

Замечание 2. Как и следовало ожидать, максимум $\tilde{m}(p)$ достигается при $p = 1/2$ (точка максимальной неопределенности). Функция $m(p)$ симметрична относительно $p = 1/2$ и монотонна на интервалах $[0, 1/2]$, $[1/2, 1]$.

Следствие 4.1. *Рассмотрим игру $\mathcal{A}_f^{m,n}(p)$. Если $m \geq \tilde{m}$, то для любого сигнала $f \in \mathcal{F}(p)$ Игрок 1 может выбрать конечный автомат, с помощью которого он безошибочно узнает состояние игры и становится информированным игроком.*

Отметим, что для $L > 3$ оценка $\tilde{m}(p)$ может быть улучшена с помощью продолжения процесса склеивания. При доказательстве Теоремы 1 мы остановились после склеивания в одну вершину всех одинаково помеченных конечных вершины. Далее можно рассмотреть конечные поддеревья высотой единица. Пусть $p < 1/2$, то есть число помеченных 1 вершин базового графа было меньше числа вершин, помеченных 2, и в результате проведенных удалений начальные вершины таких поддеревьев делятся на 3 типа:

- обе исходящие дуги ведут к конечным вершинам, помеченным 2;
- дуга с меткой 0 ведет к вершине, помеченной 1, а дуга с меткой 1 ведет к вершине, помеченной 2;
- и наоборот, дуга с меткой 0 ведет к вершине, помеченной 2, а дуга с меткой 1 ведет к вершине, помеченной 1.

Однотипные поддеревья мы можем склеить и затем продолжать этот процесс, рассматривая поддеревья высоты два и так далее, до тех пор, пока количество типов будет меньше числа вершин рассматриваемого уровня.

В результате можно получить оценку числа вершин в графе приблизительно вдвое меньшую оценки, полученной в Теореме 1. Ввиду громоздкости получающихся в результате формул (в частности, появляется двойной логарифм), мы решили не приводить соответствующих вычислений и ограничиться оценкой Теоремы 1.

5. Верхняя граница размера автомата, недекодирующего все сигналы

В этом разделе мы даем верхнюю границу доступного Игроку 2 размера автомата, который не позволяет ему «вычислить» состояние игры для любого сигнала $f \in \mathcal{F}(p)$.

Пусть $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ обозначает энтропию распределения p.

Теорема 5.1. *Пусть длина сигнальной строки $L \geq 8$. Если размер n доступного Игроку 2 автомата меньше или равен $n(p)$, где*

$$n(p) = \frac{h(p)2^L}{L},$$

то существует сигнал $f \in \mathcal{F}(p)$, который не может быть безошибочно прочитан с помощью автомата размера n.

Доказательство. Каждый автомат безошибочно различает ровно один сигнал. Поэтому для проверки утверждения достаточно убедиться в том, что число автоматов размера, не превышающего $n(p)$ меньше, чем число сигналов $f \in \mathcal{F}(p)$ при $min(p, (1-p)) \geq 1/2^L$.

Отметим, что число сигналов $f \in \mathcal{F}(p)$ (число разбиений множества $S = \{0,1\}^L$), равное $\binom{p2^L}{2^L}$, как функция от p симметрична относительно $p = 1/2$. С другой стороны, ввиду симметричности энтропии $h(p)$ относительно $p = 1/2$, как размер $n(p)$, так и число автоматов размера, не превышающего $n(p)$, также симметричны относительно $p = 1/2$. Следовательно, результат достаточно проверить на интервале $1/2^L \leq p \leq 1/2$.

Сначала оценим число автоматов размера, не превышающего произвольное n. Используя результат Леммы 1 и известную аппроксимацию Стирлинга для факториала [8]

$$n! \geq \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n},$$

получаем, что число автоматов размера не больше n не превосходит

$$\frac{2^n n^{2n}}{(n-1)!} = \frac{2^n n^{2n+1}}{n!} \leq \frac{2^{n+(2n+1)\log_2 n}}{\sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n}}.$$

Преобразуя правую часть этого неравенства, получаем оценку сверху числа автоматов размера не больше n

$$2^{(n+0.5)\log_2 n + n(1+\log_2 e) - \log_2 \sqrt{2\pi}}. \tag{2}$$

Теперь оценим снизу число сигналов $f \in \mathcal{F}(p)$ (число разбиений множества $S = \{0,1\}^L$), которое равно $\binom{p2^L}{2^L}$.

Согласно известной и довольно точной оценке числа сочетаний, см. [5] Глава 10, Лемма 7,

$$\binom{p2^L}{2^L} \geq \sqrt{\frac{2^L}{8p(1-p)2^{2L}}} 2^{h(p)2^L}.$$

Здесь $h(p)$ определенная выше энтропия распределения p. Переписывая правую часть как степень двойки, получаем выражение

$$2^{h(p)2^L-\frac{L}{2}-\frac{1}{2}(\log_2 p+\log_2(1-p))-\frac{3}{2}}, \tag{3}$$

являющееся оценкой снизу числа сигналов $f \in \mathcal{F}(p)$.

Покажем, что при $L \geq 8$ разность между нижней оценкой числа сигналов, приведенной в формуле (3), и верхней оценкой числа автоматов размера $n(p)$, которая получается при подстановке $n(p) = \frac{h(p)2^L}{L}$ в формулу (2), положительна.

Подставив размер $n(p)$ в формулу оценки сверху числа автоматов (2), получаем

$$2^{(\frac{2^L}{L/h(p)}+0.5)(L-\log_2(L/h(p)))+(1+\log_2 e)\frac{2^L}{L/h(p)}-\log_2\sqrt{2\pi}} =$$

$$2^{h(p)2^L+\frac{L}{2}-\frac{log_2(L/h(p))2^L}{L/h(p)}-0.5\log_2 L/h(p)+(1+\log_2 e)\frac{2^L}{L/h(p)}-\log_2\sqrt{2\pi}}. \tag{4}$$

Для того, чтобы показать что величина (3) больше, чем величина (4), достаточно доказать неравенство для соответствующих степеней

$$h(p)2^L+\frac{L}{2}-\frac{log_2(L/h(p))2^L}{L/h(p)}-0.5\log_2(L/h(p))+(1+\log_2 e)\frac{2^L}{L/h(p)}-$$

$$-\log_2\sqrt{2\pi} < h(p)2^L-\frac{L}{2}-\frac{1}{2}(\log_2 p+\log_2(1-p))-\frac{3}{2}.$$

Сокращая члены $h(p)2^L$ и перенося слагаемые, получаем эквивалентное неравенство

$$L+\log_2(2e)h(p)\frac{2^L}{L} < \log_2(L/h(p))(h(p)\frac{2^L}{L}+\frac{1}{2})-\log_2 p(1-p)+\log_2\sqrt{\frac{\pi}{4}}. \tag{5}$$

Сначала проверим, что неравенство (5) справедливо при минимальной возможной вероятности $p = 1/2^L$. Заметим, что энтропия $h(p)$ монотонно возрастает на отрезке $p \in [0, 1/2]$ от нуля до единицы, а при $p = 1/2^L$ имеет место неравенство

$$h = h(p) = -p\log_2 p-(1-p)\log_2(1-p) > L2^{-L}.$$

Таким образом, энтропии, равной $L2^{-L}$, соответствует $p_0 < 2^{-L}$, для которого верно $h(p_0)\frac{2^L}{L} = 1$ и $\log_2(L/h(p_0)) = L$. Подставляя $h(p_0)) = L2^{-L}$ в неравенство (5), получаем неравенство

$$L+\log_2(2e)-\log_2\sqrt{\frac{\pi}{4}} < 3/2L-\log_2 p_0(1-p_0),$$

что равносильно неравенству

$$\log_2 p_0(1-p_0) + \log_2(2e) - \log_2 \sqrt{\frac{\pi}{4}} < 1/2L,$$

которое, как легко проверить, справедливо при $L \geq 8$.

Далее проверим справедливость неравенства (5) сначала на интервале, для которого $p \geq 1/2^L$ и $h(p) < 1/2$, а затем на дополнительном интервале, для которого $p \leq 1/2$ и $h(p) \geq 1/2$.

Введем переменную $h = h(p)$ и возьмем производную по переменной h у левой и правой частей неравенства (5).

Производная по переменной h левой части равна $\log_2(2e)\frac{2^L}{L}$ и не зависит от h. Производная по переменной h правой части равна производной по h выражения

$$(log_2 L - log_2 h)(h\frac{2^L}{L} + 0.5),$$

что то же самое производной по h выражения

$$h\frac{\log_2(L)2^L}{L} + \log_2(L) - h\log_2(h) - 0.5\log_2(h).$$

Эта производная равна разности

$$\frac{\log_2(L)2^L}{L} - (\log_2(h) + \log_2(e) + \frac{\log_2(e)}{2h}), \tag{6}$$

причем уменьшаемое не зависит от h.

Для проверки неравенства (5) при $p \geq 1/2^L$ и $h(p) < 1/2$ достаточно показать, что выражение (6) (производная правой части (5)) больше, чем $\log_2(2e)\frac{2^L}{L}$ (производная левой части (5)).

Возьмем теперь производную от вычитаемого в выражении (6):

$$\frac{\log_2(e)}{h} - \frac{\log_2(e)}{2h^2} = \frac{\log_2(e)}{h}(1 - \frac{1}{2h}).$$

Так как при $0 \leq h < 1/2$ эта производная положительна (и равна нулю при $h = 1/2$), получаем, что для проверки неравенства (5) при $p \geq 1/2^L$ и $h(p) < 1/2$ достаточно проверить, что производная правой части (5) больше, чем производная левой части (5), равная $\log_2(2e)\frac{2^L}{L}$,

при $p_0 < 2^{-L}$, для которого $h(p_0) = L2^{-L}$. А именно, надо проверить неравенство

$$\log_2(2e)\frac{2^L}{L} < \frac{\log_2(L)2^L}{L} - (L - \log_2 L + \log_2(e) + \frac{\log_2(e)}{2}\frac{2^L}{L}),$$

которое эквивалентно неравенству

$$\log_2(2e) + \frac{\log_2(e)}{2} = \log(e^2) < \log_2(L).$$

Легко видеть, что последнее неравенство верно при $L > e^2 < 7,39$, то есть верно при $L \geq 8$. Тем самым мы доказали, что неравенство (5) выполняется при $p \geq 1/2^L$ и $h(p) < 1/2$.

Теперь рассмотрим интервал, для которого $p \leq 1/2$ и $h(p) \geq 1/2$. В этом случае (5) удобно переписать следующим образом

$$L < (\log_2(L/h(p)) - \log_2(2e))(h(p)\frac{2^L}{L} + \frac{1}{2}) - \log_2 p(1-p) + \log_2 \sqrt{\frac{\pi e)}{2}}.$$

Это неравенство справедливо, так как при $L \geq 8$ и $h \geq 1/2$ имеют место соотношения:
$\log_2(L/h) - \log_2(2e) > \log_2(8/(2e)) = \log_2(4/e) \approx 0.56 > 1/2$;
$h\frac{2^L}{L} + \frac{1}{2} > 2L$ и $-\log p(1-p) + \log\sqrt{\frac{\pi e}{2}} > 0$. □

Следствие 5.1. *Если $n \leq n(p)$, то существует сигнал $f \in \mathcal{F}(p)$ такой, что Игрок 2 с помощью доступных ему конечных автоматов не может безошибочно узнать состояние игры $\mathcal{A}_f^{m,n}(p)$.*

Объединяя выводы Следствия 1 и Следствия 2, получаем, что если в игре $\mathcal{A}_f^{m,n}(p)$ размер m доступного Игроку 1 автомата превышает $\tilde{m}(p)$, а размер n доступного Игроку 2 автомата меньше $n(p)$, то найдется публичный сигнал $f \in \mathcal{F}(p)$, при котором исходная игра $f \in \mathcal{F}(p)$ с неполной информацией у обеих сторон превратится в игру с неполной информацией у Игрока 2.

СПИСОК ЛИТЕРАТУРЫ

1. Aumann R., Maschler M. *Repeated Games with Incomplete Information.* The MIT Press: Cambridge, Massachusetts–London, 1995.

2. Gavrilovich M., Kreps V. *Games with symmetric incomplete information and asymmetric computational resources* // Int. Game Theory Review. 2018. Vol. 20. No. 2. P. 17500034

3. Harsanyi J. *Games with Incomplete Information Played by Bayesian Players. Parts I to III*// Management Science. 1967-68. Vol. 14. P. 159–182, 320–334 and 486–502.

4. Kobrinskii N., Trakhtenbrot B. *Introduction to the Theory of Finite Automata.* Amsterdam, North-Holland. 1965.

5. MacWilliams F.J., Sloane N.J.A. *The theory of error-correcting codes.* Amsterdam, North-Holland. 1977.

6. Neyman A. *Cooperation, repetition and automata* // In: Hart, S., Mas-Colell, A. (Eds.), Cooperation: Game-Theoretic Approaches. NATO ASI Series F., Springer-Verlag. 1997. Vol. 155. P. 233-–255.

7. Neyman A. *Finitely repeated games with finite automata* // Math. Oper. Res. 1998. Vol. 23. P. 513-–552.

8. Romik D. *Stirling's Approximation for n!: The Ultimate Short Proof?*// The American Mathematical Monthly. 2000. Vol. 107, No. 6. P. 556–557.

9. Sakarovitch J. *Elements of Automata Theory.* Cambridge University Press. 2009.

SIGNAL DECODING WITH HELP OF FINITE AUTOMATA: APPLICATION TO GAMES WITH INCOMPLETE INFORMATION

Michael R. Gavrilovich, Institute for Problems of Regional Economics RAS, National Research University Higher School of Economics (mishap@sdf.org).
Victoria L. Kreps, Institute for Problems of Regional Economics RAS, National Research University Higher School of Economics, Dr.Sc., professor (vita_kreps@mail.ru).

Abstract: Matrix games with incomplete information on both sides and public signal on the state of game represented by random binary code of fixed length are considered. Players are computationally bounded and are only able to play strategies to finite automata of different sizes: m for Player 1 and n for Player 2 where $m \gg n$. We obtain a lower bound for m and an upper bound for n which may turn the original game with incomplete information for both players into a game with incomplete information for Player 2.

Keywords: matrix game, incomplete information, asymmetry, binary code, finite automata.