АКАДЕМИЯ НАУК СССР

ТЕОРИЯ ВЕРОЯТНОСТЕЙ И ЕЕ ПРИМЕНЕНИЯ

(ОТДЕЛЬНЫЙ ОТТИСК)

3

МОСКВА · 1987

ная проверка закончится. Если обнаруживается несимметричность, то M переходит к новому a_i. Если детерминированная проверка обнаруживает симметричность, то M выдает ответ «принадлежит».

Для оценки времени работы M заметим, что M на симметричных отрезках a_i с вероятностью 1 выдает ответ «симметрично». На несимметричных отрезках a_i с вероятностью $^3/_4$ M' выдает ответ «несимметрично» за время $|a_i| \log_2 |a_i|$. Для любого $\varepsilon > 0$ с вероятностью $1 - \varepsilon$ можно ожидать, что число применений M' к z несимметричным отрезкам не превысит const z и, следовательно, суммарное время работы M не превысит

$$\text{const}\, z\, |a_i| \log_2 |a_i| + |a_i|^2 \leqslant \text{const}'\, n \log_2 n.$$

ЛИТЕРАТУРА

1. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М.: Наука, 1986, 368 с.
2. *Фрейвалд Р. В.* Быстрые вычисления на вероятностных машинах Тьюринга.— Уч. записки Латвийского гос. ун-та, 1975, т. 233, с. 201—205.
3. *Фрейвалд Р. В.* Ускорение распознавания некоторых множеств применением датчика случайных чисел.— В сб.: Проблемы кибернетики, В. 36. М.: Наука, 1979, с. 209—224.
4. *Барздинь Я. М.* Сложность распознавания симметрии на машинах Тьюринга.— В сб.: Проблемы кибернетики, В. 15. М.: Физматгиз, 1965, с. 245—248.
5. *Бухштаб А. А.* Теория чисел. М.: Учпедгиз, 1960, 375 с.

Поступила в редакцию
17.IV.1987

ВЕРОЯТНОСТНЫЕ СТРАТЕГИИ В КОНЕЧНЫХ ИГРАХ С ПОЛНОЙ ИНФОРМАЦИЕЙ

ШЕНЬ А. Х.

Как известно, всякая конечная игра с полной информацией предопределена: для одного из ее участников существует выигрышная стратегия (мы считаем, что ничьи невозможны). Эта теорема, однако, является «теоремой существования»: предлагаемая в ее доказательстве стратегия требует, по существу, перебора всех возможных позиций игры, которых, как правило, очень много, и с практической точки зрения наличием такой стратегии можно пренебречь. Цель заметки — обратить внимание на то, что этому наблюдению можно придать точный смысл. Оказывается, что (в предположении некоторой теоретико-сложностной гипотезы) справедливо следующее утверждение: существуют конечные полиномиальные игры с полной информацией, в которых для каждого из игроков существует вероятностная полиномиальная стратегия, гарантирующая ему близкую к $^1/_2$ вероятность выигрыша при игре против любой полиномиальной вероятностной стратегии. (Слова «полиномиальная» означают, грубо говоря, что правила игры и стратегии достаточно быстро алгоритмически вычислимы; точные формулировки смотри ниже.)

Назовем *игрой* размера k произвольное подмножество A множества $\mathbf{B}^k$ последовательностей длины k из нулей и единиц. (Неформально говоря, игра состоит в том, что Белые и Черные по очереди пишут цифры 0 или 1; после того, как последовательность достигла длины k, игра кончается; кто выиграл, определяется тем, принадлежит ли получившаяся последовательность множеству A.) *Булевской сложностью* игры называется минимальный размер схемы (с k входами и одним выходом) из логических элементов, распознающей принадлежность множеству A. Будем называть последовательность игр $A_0, A_1, \ldots$ *полиномиальной*, если размер и булева сложность игры A_n ограничены полиномом от n.

Определим понятие *вероятностной стратегии* для игр описанного типа. Обычно стратегией называют функцию, сопоставляющую последовательности уже сделанных ходов очередной ход. В случае нашей игры аргументами стратегии будут последовательности длины меньше k из нулей и единиц (четной длины для Белых и нечетной — для Черных), а значениями — нули и единицы. Вероятностная стратегия (называемая также смешанной) имеет еще один аргумент, значениями которого служат последовательности некоторой длины s из нулей и единиц (интерпретируемые как результаты бросаний «честной» монеты). Другими словами, вероятностная стратегия представляет собой набор из 2^s стратегий в обычном (невероятностном) смысле; выбор одной из них производится случайно (каждый элемент набора имеет вероятность 2^{-s}). Имеет смысл говорить о *булевой сложности* вероятностной стратегии (чтобы это сделать, нужно лишь закодировать ее входы последовательностями постоянной длины). Мы будем рассматривать полиномиальные последовательности игр и последовательности вероятностных стратегий для соответствующих игр, в которых булева сложность стратегии ограничена некоторым полиномом от ее номера в последовательности, называя их *полиномиальными последовательностями стратегий*.

Для двух обычных, невероятностных, стратегий — одной для Белых, другой для Черных — в заданной игре можно определить, кто выигрывает, если Белые и Черные руководствуются указанными стратегиями. Для вероятностных стратегий имеет смысл говорить о вероятности выигрыша. (Напомним, что мы считаем все 2^s стратегий, входящий в семейство стратегий, соответствующих данной вероятностной стратегии при одном из 2^s исходов датчика случайных чисел, равновероятными; мы предполагаем также, что датчики случайных чисел Белых и Черных независимы.) Теперь мы можем сформулировать утверждение, о котором шла речь.

Утверждение. *Существует полиномиальная последовательность игр $A_0, A_1, \ldots$ со следующими свойствами: для каждого из игроков (Белых и Черных) существует полиномиальная последовательность стратегий, обеспечивающая ему вероятность выигрыша в игре A_n не менее $1/2 - \varphi(n)$, где $\varphi(n) = o(n^{-d})$, $n \to \infty$, для любого d, при игре против любой полиномиальной последовательности вероятностных стратегий.*

Отметим, что функция φ может зависеть от последовательности стратегий, выбранной противником; в частности, она может быть равна $1/2$ для малых n.

Это утверждение справедливо в предположении некоторой формулируемой ниже теоретико-сложностной гипотезы, заимствованной из [1]. Конструкции игр и стратегий основываются на идеях работы [2].

Теоретико-сложностная гипотеза. *Существуют последовательность чисел $k_0, k_1, \ldots$, последовательность взаимно однозначных отображений $f_0, f_1, \ldots$ (f_n отображает множество $\mathbf{B}^{k_n}$ всех последовательностей длины k_n из нулей и единиц в себя) и предикатов $P_0, P_1, \ldots$ (P_n определено на $\mathbf{B}^{k_n}$), для которых справедливы следующие утверждения:*

1) *числа k_n, булева сложность функций f_n и предикатов P_n ограничены полиномом от n;*

2) *для всякой последовательности Q_n, $n = 0, 1, \ldots$, предикатов на $\mathbf{B}^{k_n}$, булева сложность которых ограничена полиномом от n, доля тех x из $\mathbf{B}^{k_n}$, для которых $Q_n(f_n(x)) = P_n(x)$, отличается от $1/2$ на функцию, убывающую быстрее любой степени n.*

Проведем построение игр A_n в предположении этой гипотезы. Мы опишем игру A_n в неформальных терминах. Вначале Белые называют некоторую последовательность x длины k_n. Черные в ответ называют $z \in \{\text{И}, \text{Л}\}$. Затем Белые называют некоторую последовательность y длины k_n. На этом игра кончается. Белые выигрывают, если $x = f_n(y)$ и $P_n(y) \neq z$. В противоположном случае выигрывают Черные. Другими словами, Белые сообщают Черным $f_n(y)$, не сообщая самого y, затем Черные пытаются отгадать значение $P_n(y)$, зная $f_n(y)$, а затем Белые сообщают y для контроля. (В нашем описании ход в игре состоит не в сообщении одного бита, а сразу многих, но это, очевидно, несущественно: можно считать, например, что ответы Черных на некоторые ходы Белых игнорируются.)

Перейдем к построению стратегий. Стратегия для Черных состоит в случайном выборе между И и Л с вероятностью $^1/_2$. Она обеспечивает им вероятность выигрыша $^1/_2$ при любой (не обязательно полиномиальной) стратегии Белых.

Стратегия для Белых состоит в следующем. Нужно выбрать случайную последовательность y длины k_n из нулей и единиц (считая все такие последовательности равновероятными), затем вычислить $x = f_n(y)$ и сделать ход x. Затем независимо от хода Черных сделать ход y.

Покажем, что стратегии действительно обладают указанными свойствами. Для стратегии Черных это очевидно. Рассмотрим указанную стратегию Белых. Если при этом у Черных есть стратегия, гарантирующая им вероятность выигрыша p, то это означает, что по $f_n(y)$ можно восстановить $P_n(y)$ с вероятностью p. Ссылка на теоретико-сложностную гипотезу почти завершает рассуждение — «почти» потому, что стратегия вероятностная, а предикат Q_n, о котором шла речь в формулировке гипотезы, — нет. Чтобы восполнить этот пробел, необходимо использовать следующий результат.

Лемма. *Пусть числа k_n, функции f_n и предикаты P_n обладают свойствами, указанными выше, R_n — последовательность предикатов на $\mathbf{B}^{k_n} \times \mathbf{B}^{l_n}$, где l_n — некоторая последовательность, ограниченная полиномом от n, и булева сложность R_n ограничена полиномом от n. Тогда вероятность того, что $R_n(f_n(x), y) = P_n(x)$, взятая при равномерном распределении x в $\mathbf{B}^{k_n}$ и независимом равномерном распределении y в $\mathbf{B}^{l_n}$, отличается от $^1/_2$ на функцию, убывающую быстрее любой степени n.*

Доказательство. Обозначим y_n «наилучшее» y — то y, при котором доля таких x, что $R_n(f_n(x), y) = P_n(x)$, максимальна. Применим свойство (2) теоретико-сложностной гипотезы, положив $Q_n(x) = R_n(x, y_n)$. Ясно, что булева сложность Q_n полиномиально ограниченна, и что вероятность равенства $R_n(f_n(x), y) = P_n(x)$ не превосходит доли тех x, при которых $R_n(f_n(x), y_n) = P_n(x)$. Поэтому указанная вероятность не может сильно превосходить $^1/_2$. Аналогично, взяв «наихудшее» y, убеждаемся, что эта вероятность не может быть сильно меньше $^1/_2$. Лемма доказана.

Автор благодарит Г. М. Адельсона-Вельского, неоднократно высказывавшего мысль об осмысленности применения вероятностных понятий к анализу игр с полной информацией (см. [3]), а также всех участников семинара А. Н. Колмогорова по сложности определений и сложности вычислений.

ЛИТЕРАТУРА

1. *Blum M., Micali S.* How to generate cryptographically strong sequences of pseudo-random bits.— SIAM J. Comput., 1984, v. 13, № 4, p. 850—864.
2. *Шамир А., Райвест Р., Адельман Л.* Покер без карт.— В сб.: Математический цветник. М.: Мир, 1983, с. 58—66.
3. *Адельсон-Вельский Г. М., Арлазаров В. Л., Донский М. В.* Программирование игр. М.: Наука, 1978, 255 с.

Поступила в редакцию
17.IV.1987

ОБ ОДНОЙ СХЕМЕ ЧАСТИЧНОГО СУММИРОВАНИЯ

ЧИБИСОВА Е. Д.

Пусть $X_1, X_2, \ldots$ — независимые случайные величины, среди функций распределения (ф.р.) которых не более r различных,

$$S_n = (X_1 + \ldots + X_{k(n)})/B_n - A_n, \quad B_n > 0. \tag{1}$$

Класс предельных распределений для S_n в случае $k(n) = n$ описан в [1]. В [2] показано, что если $k(n) = n$, а ф. р. слагаемых в (1) принадлежат областям притяжения устойчивых законов, то предельное распределение является сверткой этих устойчивых законов; даны также необходимые и достаточные условия существования предельного распределения.