

**МАТЕМАТИЧЕСКИЕ
ВОПРОСЫ
КИБЕРНЕТИКИ**

10

Е. А. Окольнішнікова

**О сложности
ветвящихся программ**

Рекомендуемая форма библиографической ссылки:
Окольнішнікова Е. А. О сложности ветвящихся программ // Математические вопросы кибернетики. Вып. 10. – М.: ФИЗМАТЛИТ, 2001. – С. 69–82. URL: <http://library.keldysh.ru/mvk.asp?id=2001-69>

О СЛОЖНОСТИ ВЕТВЯЩИХСЯ ПРОГРАММ *)

Е. А. ОКОЛЬНИШНИКОВА

(НОВОСИБИРСК)

1. Введение

Изучение сложности реализации булевых функций ветвящимися программами является одним из интенсивно развивающихся в последнее время направлений в математической теории сложности. В данной работе будут приведены результаты лишь по некоторым направлениям этих исследований. Это связано с большим количеством публикаций по данной тематике. При подготовке обзора использовались доклады, прочитанные автором на школе-семинаре по синтезу и сложности управляющих систем, проходившей в 1998 г. в ННГУ и НИИ ПМК, г. Нижний Новгород, и доклады, прочитанные на школах молодых ученых, проходящих в рамках программы «Интеграция» в МГУ (г. Москва, 1997 г.) и в ННГУ (г. Нижний Новгород, 1998 г.)

Ветвящаяся (бинарная) программа — математическая модель вычислений, связанная с переработкой информации, в которой на каждом шаге проверяется значение одного бита информации. Этот тип управляющих систем можно рассматривать как модель вычислений, хорошо моделирующих работу компьютерных программ, состоящих из условных операторов.

В начале обзора, в разделе 2, будут даны определения контактно-вентильной схемы, ориентированной и ациклической контактно-вентильной схем, как моделей управляющих систем наиболее близких к ветвящимся программам, затем будут определены недетерминированная и детерминированная ветвящиеся программы; определены меры сложности для этих классов схем. Приведен ряд соотношений для этих мер сложностей, и описано поведение функции Шеннона для этих классов схем.

В разделах 3 и 4 приведены известные нижние оценки сложности для недетерминированных и детерминированных ветвящихся программ соответственно.

Раздел 5 посвящен ветвящимся программам с ограничениями на ширину.

В разделе 6 рассматриваются ветвящиеся k -программы и приведены методы получения нижних оценок для этого класса схем. В конце раздела приведен метод использования нижних оценок сложности ветвящихся k -программ для получения нижних оценок сложности ветвящихся программ без ограничений.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 00-01-00874) и Федеральной целевой программы «Интеграция» (проект АО-110).

мерой сложности $RS(f)$ для ориентированных контактно-вентильных схем и мерой сложности $\tilde{L}_{\text{кв}}(f)$ для контактно-вентильных схем

$$\tilde{L}_{\text{кв}}(f) \leq RS(f) \leq 2\tilde{L}_{\text{кв}}(f).$$

2.3. Ациклическая контактно-вентильная схема. Под *ациклической контактно-вентильной схемой* (switching-and-rectifier network [20, 27], или directed contact network [13, 33]), или contact gating schema [33]) от переменных x_1, \dots, x_n понимается ориентированный ациклический граф с двумя выделенными вершинами (входной и выходной), у которого часть дуг помечена переменными x_1, \dots, x_n или их отрицаниями $\bar{x}_1, \dots, \bar{x}_n$, а оставшаяся часть дуг — *свободные дуги* — не помечена. Функция $f(x_1, \dots, x_n)$, реализуемая ациклической контактно-вентильной схемой, описывает проводимость между входной и выходной вершинами в зависимости от значений переменных x_1, \dots, x_n . Под сложностью ациклической контактно-вентильной схемы понимается число дуг, помеченных переменными или их отрицаниями.

Пример 2. На рис. 2 приведен пример ациклической контактно-вентильной схемы, реализующей булеву функцию $f_2 = xzv \vee xzut \vee yzv \vee yzu(t \vee \bar{x}) \vee y\bar{z}(t \vee \bar{x})$. Сложность RS этой схемы равна 8.

Порядок функции Шеннона для этого класса схем тот же, что и меры сложности $\tilde{L}_{\text{кв}}$ для контактно-вентильных схем, а именно, ($\approx 2^{n/2}$). Все известные нижние оценки для контактно-вентильных схем справедливы и для ациклических контактно-вентильных схем. Кроме того, на этот класс схем можно перенести некоторые нижние оценки, полученные для других классов схем, в частности нижнюю оценку, полученную для характеристических функций некоторых двоичных кодов в классе недетерминированных и детерминированных ветвящихся программ [10, 12].

Известно, что по каждой ориентированной контактно-вентильной схеме G , реализующей булеву функцию f , можно построить ациклическую контактно-вентильную схему без свободных дуг G' , которая реализует ту же функцию f и сложность которой есть полином (степени не выше четырех) от сложности схемы G [36, теор. 2.2].

2.4. Недетерминированные ветвящиеся программы. Частным случаем ациклических контактно-вентильных схем являются недетерминированные ветвящиеся программы (nondeterministic branching programs). *Недетерминированной ветвящейся программой* от переменных x_1, \dots, x_n называется ориентированный граф без циклов с одной входной вершиной и двумя выходными вершинами, одна из которых помечена нулем, другая — единицей. Из каждой вершины, за исключением выходных, выходит ровно две дуги. Все невыходные вершины при этом делятся на два типа:

— вершины, помеченные переменными из множества $\{x_1, \dots, x_n\}$; из вершин этого типа выходит одна дуга, помеченная единицей, и одна дуга, помеченная нулем;

— недетерминированные вершины (guessing nodes, \vee -nodes, existential nodes), из которых выходит ровно две непомеченных дуги.

Функция $f(x_1, \dots, x_n)$, реализуемая недетерминированной ветвящейся программой, описывает проводимость между входной и выходной вершинами в зависимости от значений переменных x_1, \dots, x_n . Сложность булевых функций в этом классе схем — число помеченных вершин*) — будем обо-

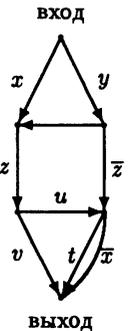


Рис. 2

*) Иногда под сложностью недетерминированной ветвящейся программы понимается число помеченных дуг. Эту меру сложности обычно используют в том случае, когда доказательства утверждений проводятся для ациклических контактно-вентильных схем и распространяются на недетерминированные ветвящиеся программы. В этом случае удобнее под сложностью понимать именно число дуг. Ясно, что эти две меры сложности отличаются ровно в два раза.

значать через $NBP(f)$. Порядок функции Шеннона для этого класса схем тот же, что и для контактно-вентильных схем ($\asymp 2^{n/2}$).

Пример 3. На рис. 3 приведен пример недетерминированной ветвящейся программы (недетерминированная вершина обозначена незаштрихованным кружком), реализующей функцию $f_3 = \bar{x}_5(\bar{x}_6\bar{x}_4(x_2x_1 \vee \bar{x}_3\bar{x}_1) \vee x_4(\bar{x}_2x_1 \vee x_3\bar{x}_1)) \vee x_3(x_4x_2x_1 \vee \bar{x}_2x_1)$. Сложность NBP этой схемы равна 8.

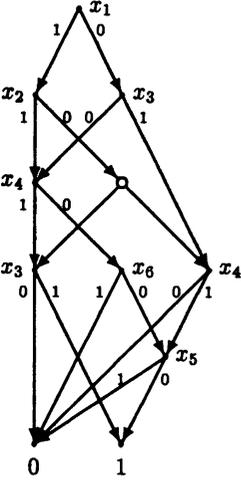


Рис. 3

С точностью до мультипликативной константы, сложность реализации булевой функции недетерминированными ветвящимися программами совпадает со сложностью реализации той же функции ациклическими контактно-вентильными схемами. Но при рассмотрении схем с ограничениями на структуру это соотношение сложностей может измениться.

2.5. Детерминированные ветвящиеся программы. Недетерминированная ветвящаяся программа называется *детерминированной ветвящейся программой*, если в ней нет недетерминированных вершин. В русской литературе используется также термин *бинарная программа* для обозначения детерминированных ветвящихся программ.

Видимо, первой работой, где рассматривался этот класс схем, была работа К. Ли [29]. Сложность реализации булевой функции f в этом классе схем — число невыходных вершин — будем обозначать $BP(f)$. В. А. Кузьминым [5] была получена асимптотика функции Шеннона для этого класса схем ($\sim 2^n/n$) (см. также [1, 4]).

Пример 4. На рис. 4 приведен пример детерминированной ветвящейся программы, реализующей функцию $f_4 = \bar{x}_5(\bar{x}_6\bar{x}_4(x_2x_1 \vee \bar{x}_3\bar{x}_1) \vee x_4(\bar{x}_5\bar{x}_2x_1 \vee x_3\bar{x}_1)) \vee x_3(x_4x_2x_1 \vee x_5x_1\bar{x}_2)$. Сложность BP этой схемы равна 9.

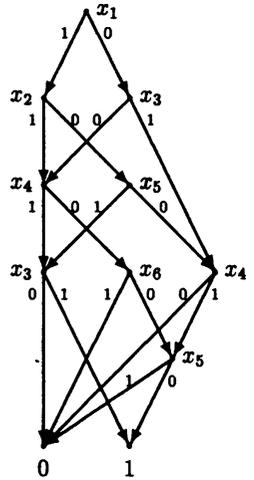


Рис. 4

2.6. Сравнение сложностей реализации булевых функций различными типами управляющих систем. Пусть $S(f)$ обозначает сложность реализации булевой функции f схемами из функциональных элементов, $K(f)$ — сложность реализации булевой функции f контактными схемами, а $L_0(f)$ — сложность реализации булевой функции f формулами в базе $(\&, \vee, \neg)$. Тогда имеют место следующие соотношения сложностей [35, 42] (обозначение $F \preceq Q$ мы будем использовать для обозначения того, что $F = O(Q)$)

$$S^{1/3}(f) \preceq RS(f) \preceq K(f) \preceq BP(f) \preceq L_0(f).$$

Кроме того, А. А. Разборовым [35] было неконструктивно показано, что имеет место следующее соотношение сложностей контактных схем и детерминированных ветвящихся программ

$$K(f) \leq BP(f)^{O(1)}.$$

М. Зауерхофф, И. Вегенер и Р. Верхнер в 1999 г. [37] показали, что имеет место следующее соотношение сложностей:

$$BP(f) = O(L(f)^\beta),$$

где $\beta = \log_4(3 + \sqrt{5}) < 1,194$.

Известно, что последовательности функций, которые могут быть вычислены ветвящимися программами полиномиальной сложности, могут также быть вычислены неуниформной машиной Тьюринга за логарифмическое время и наоборот (см. [24, 34, 42]) Кроме того, о связи ветвящихся программ и машин Тьюринга см. [32, 35, 36].

Существует связь между сложностью ветвящихся программ и пространственной сложностью неуниформных машин Тьюринга.

А. Кобхэм [24] и П. Пудлак [34] доказали следующие утверждения.

Теорема 1. *Если f — булева функция, то*

$$S(f_n) = O(\log(\max\{BP(f_n), n\})),$$

$$BP(f_n) = 2^{O(\max\{S(f_n), \log n\})},$$

где $S(f)$ — пространственная сложность неуниформных машин Тьюринга.

3. Нижние оценки сложности для недетерминированных ветвящихся программ

3.1. Оценка Э. И. Нечипорука. Наилучшей известной нижней оценкой сложности реализации функций недетерминированными ветвящимися программами является оценка $\Omega\left(\frac{n^{3/2}}{\log n}\right)$, полученная П. Пудлаком [33] с помощью метода Нечипорука [8].

3.2. Оценки для симметрических булевых функций. Ясно, что на этот класс схем переносятся все известные оценки для сложности реализации булевых функций контактно-вентильными схемами, в частности оценка $\Omega(n \log \log \log^* n)$ для сложности реализации ряда симметрических булевых функций, включая функцию голосования MAJ_n [13].

3.3. Оценки для характеристических функций двоичных кодов. Е. А. Окольнішниковой [12] были получены нелинейные нижние оценки $\Omega(n \log n / \log \log n)$ для сложности реализации характеристических функций кодов Риды–Маллера в классе недетерминированных ветвящихся программ. Подробнее о способе получения этой оценки будет сказано ниже, в п. 6.4 после введения понятия ветвящейся k -программы.

4. Нижние оценки сложности для детерминированных ветвящихся программ

4.1. Оценка Э. И. Нечипорука. Наилучшей известной нижней оценкой для сложности реализации функций детерминированными ветвящимися программами является оценка $\Omega\left(\frac{n^2}{\log^2 n}\right)$, полученная П. Пудлаком [33] с помощью метода Нечипорука [8].

4.2. Оценки для симметрических булевых функций. Для ряда симметрических булевых функций, в частности для функции голосования, П. Пудлак [32] получил оценку

$$BP(\text{MAJ}_n) \geq \Omega(n \log \log n / \log \log \log n).$$

Впоследствии Л. Бабаи, П. Пудлак, В. Рёдл и М. Семереди [17] улучшили этот результат. Они показали, что

$$BP(\text{MAJ}_n) \geq \Omega(n \log n / \log \log n).$$

Пусть X, Y, Z — множества переменных. И пусть $f(X)$ обозначает тот факт, что функция f зависит только от переменных из множества X ; если X — объединение непересекающихся множеств Y и Z , то будем использовать обозначение $f(Y, Z)$; подстановка — это отображение $\delta: X \rightarrow \{0, 1, *\}$, через f_δ будем обозначать результат применения подстановки δ к функции f .

Пусть заданы непересекающиеся множества Y, Z и функция $f(Y, Z)$. Будем говорить, что функция $f(Y, Z)$ является λ -простой, если существует разбиение A_1, \dots, A_{l_1} множества 2^Y и разбиение B_1, \dots, B_{l_2} множества 2^Z , $l_1, l_2 \leq \lambda$, такие, что функция f постоянна на каждом из множеств $A_i \times B_j$, $1 \leq i \leq l_1, 1 \leq j \leq l_2$.

Теорема 2 [17, теорема 2.4]. *Для любого $\gamma, \gamma \geq 0$, любого натурального n и любой функции $f(X)$, $|X|=2n$, существуют положительные целые числа a и b такие, что если функция $f(X)$ может быть вычислена ветвящейся программой сложности не превосходящей γn , то существуют непересекающиеся множества $Y, Z \subseteq X$ для которых*

$$(1) |Y| = |Z| \geq n/b^\gamma,$$

(2) для подстановки δ , обращающей $X \setminus (Y \cup Z)$ в нуль, функция $f_\delta(Y, Z)$ является $\gamma^{a\gamma}$ -простой.

Эта теорема позволяет получать нетривиальные нижние оценки в случае, когда функция достаточно симметрична. Это позволило получить оценку $\Omega(n \log n)(\log \log n)^{-1}$ для ряда симметрических булевых функций, в том числе для функции голосования MAJ_n и для элементарной симметрической функции $E_{\lfloor n/2 \rfloor}$ (т. е. для функции зависящей от n переменных и принимающих значение 1 на наборах, содержащих $\lfloor n/2 \rfloor$ единиц). Наилучшая известная верхняя оценка для детерминированных ветвящихся программ, реализующих симметрические булевы функции, — это оценка $O(n^2/\log n)$, а для элементарных симметрических функций — оценка $O(n(\log n)^2/\log \log n)$. Эти оценки были получены О. Б. Лупановым для контактных схем [7], но, как замечено в [16], они являются одновременно и оценками для детерминированных ветвящихся программ.

4.3. Оценки для характеристических функций двоичных кодов. Е. А. Окольнишниковой [10] были получены нелинейные нижние оценки сложности реализации характеристических функций двоичных кодов с большим числом кодовых вершин и с растущим (с ростом n) кодовым расстоянием. В частности, получена нижняя оценка $\Omega(n \log n / \log \log n)$ для характеристических функций кодов Боуза–Чоудхури–Хоквингема с кодовым расстоянием $O(\log n / \log \log n)$ в классе детерминированных ветвящихся программ. Впоследствии в [12] аналогичным методом была получена нижняя оценка $\Omega(n \log n / \log \log n)$ для сложности реализации характеристических функций кодов Рида–Маллера в классе недетерминированных ветвящихся программ. Из этой оценки следует такая же оценка в классе детерминированных ветвящихся программ. Подробнее о способах получения этих оценок будет сказано ниже, в п. 6.4, после введения понятия ветвящейся k -программы.

5. Ветвящиеся программы ограниченной ширины

Широкое распространение получили работы по изучению ветвящихся программ с ограничениями на структуру схем. Одним из таких широко исследуемых в конце 80-х, начале 90-х годов ограничений является ограничение на ширину программ (обзор результатов см. в [15, 42], см. также [18]). Говорят, что детерминированная ветвящаяся программа имеет ширину d , если она разбита на уровни и каждый уровень содержит не более d вершин. При этом дуги идут только из вершин меньшего уровня в вершины боль-

шего уровня. Для сложности реализации булевых функций схемами с этим ограничением был получен ряд интересных результатов. В частности для схем ширины d Л. Бабаи, П. Пудлак, Р. Редл и М. Семереди [17] получили нижние оценки $\Omega(n \log n)$ для сложности реализации полностью определенных симметрических булевых функций (в том числе функции голосования MAJ_n). При получении результата для схем ограниченной ширины в [17] использовался тот же принцип доказательства, что и при получении нижних оценок сложности для схем без ограничений.

Используя те же обозначения, что и в п. 4.4, описывающем сложность ветвящихся программ для симметрических булевых функций, имеем для схем ширины, не превосходящей d , следующее утверждение.

Теорема 3 [17, теорема 2.3]. *Для любых натуральных d и n , вещественного γ , $\gamma \geq 0$, и произвольной функции $f(X)$, $|X| = 2n$, существуют положительные целые числа a и b такие, что если функция $f(X)$ может быть вычислена ветвящейся программой ширины d со сложностью, не превосходящей γn , то существуют непересекающиеся множества $Y, Z \subseteq X$ для которых*

$$(1) |Y| = |Z| \geq n/b^\gamma,$$

(2) для подстановки δ , которая фиксирует $X \setminus (Y \cup Z)$, функция $f_\delta(Y, Z)$ является γ^γ -простой.

Эта теорема позволяет, в частности, получить оценку $\Omega(n \log n)$ для функции голосования MAJ_n в классе ветвящихся программ ограниченной ширины.

6. Ветвящиеся k -программы

Другим широко распространенным ограничением на структуру ветвящихся программ является ограничение на число проверок переменных в каждой цепи, когда для любой переменной x_i в любой цепи, идущей от входной вершины к выходной, вершины, помеченные переменной x_i , встречаются не более k раз. Такие программы называются ветвящимися k -программами (read- k -times или read- k -times only branching programs). Сложность реализации булевой функции f недетерминированной (детерминированной) ветвящейся k -программой обозначим через $\text{NBP}_k(f)$ и $\text{BP}_k(f)$ соответственно. Недетерминированная ветвящаяся программа называется *недетерминированной синтаксической* ветвящейся k -программой, если в ней вдоль любого пути от входной вершины к выходной каждая переменная встречается не более k раз. Возможное альтернативное определение k -программы состоит в том, что ограничение на число проверок накладывается не на все пути программы, идущие от входной вершины к выходной, а только на пути, в которых не встречаются одновременно дуги, помеченные некоторой переменной x_i и ее отрицанием (ненулевые пути). Такие ветвящиеся программы называются *несинтаксическими ветвящимися k -программами*. Аналогично можно ввести понятия синтаксических и несинтаксических контактно-вентильных k -схем. С. П. Юкна [27] показал, что для случая $k = 1$ синтаксическая модель для ациклических контактно-вентильных схем в экспоненциальное число раз слабее, чем несинтаксическая модель. Неизвестно ни одной нетривиальной нижней оценки для несинтаксических ветвящихся программ при $k \geq 2$. Более того, не известно ни одной нетривиальной нижней оценки для случая $k = 1$ для несинтаксических ветвящихся ациклических контактно-вентильных схем.

6.1. Нижние оценки сложности для ветвящихся 1-программ.

Имеется большое число работ, которые продолжают появляться до настоящего времени, в которых получены экспоненциальные нижние оценки сложности 1-программ (read-once branching programs или FBDD, т. е. free binary decision diagrams). Среди этих работ одной из первых была работа

С. Жака [46] (см. также [9, 16, 25, 43]). Наилучшими из известных в настоящее время нижних оценок, полученными для 1-программ, являются оценки $2^{n/2000}$ [40], $2^{n - o(n)}$ [38] и $2^{n - O(\log n)^2}$ [14].

6.2. Нижние оценки сложности для ветвящихся k -программ.

Первой работой, в которой была получена оценка экспоненциального типа для детерминированных ветвящихся k -программ при растущих значениях k , была работа Е. А. Окольнишниковой [10]. Оценка была получена для $k = O(\log n / \log \log n)$. Позднее метод получения экспоненциальных нижних оценок из [9] был распространен на случай недетерминированных ветвящихся программ [11, 31]. Отметим, что эта работа была, возможно, первой работой, в которой в явном виде использовались схемы с ограничениями (а именно ветвящиеся k -программы) для получения нижних оценок для схем без ограничений. (Более подробно см. п. 6.4.)

Примерно в это же время и независимо А. Бородиным, А. А. Разборовым и Р. Смоленским [20] были получены экспоненциальные нижние оценки для недетерминированных ветвящихся k -программ для $k \leq c \log n$. Позднее, в 1998 г., метод, предложенный в работе [20], был модифицирован Дж. Тхатхачаром [41].

Можно отметить, что методы, предложенные для получения высоких нижних оценок в [10, 20, 31, 41] схожи. Пусть \mathcal{P} — ветвящаяся программа, реализующая булеву функцию f от N переменных. Каждой единице булевой функции f (т. е. набору, на котором функция равна единице) ставится в соответствие путь в \mathcal{P} . Этот путь делится на «равные» части, и каждому такому пути ставится в соответствие или некоторое подмножество вершин ветвящейся программы [10, 12, 31] или некоторое подмножество дуг ветвящейся программы [20, 41], позволяющее отделить одну часть от другой. Мощности этих множеств зависят только от заранее выбранных параметров и существенно меньше чем длина пути, которому они соответствуют. С каждым таким множеством вершин (или дуг) ассоциируется функция f_i , зависящая только от этого подмножества вершин или дуг программы \mathcal{P} и не зависящая от пути, по которому она строилась. При этом

$$f = \vee f_i, \quad (1)$$

т. е. функции f_i задают покрытие множества единиц функции f . Если число единиц каждой функции f_i не очень большое, а число единиц функции f велико, то, значит, и число различных подмножеств (вершин или дуг), которые ставятся в соответствие единицам булевой функции, велико. Это позволяет оценить снизу мощность множества вершин (или дуг) ветвящейся программы.

В [10, 12, 31] для получения нижних оценок сложности ветвящихся программ используется сопоставление каждой единице ветвящейся программы последовательности вершин ветвящейся программы. Это требует преобразования ветвящейся программы к «однородному» виду, что приводит к некоторому усложнению программы, но позволяет рассматривать обобщенные отрезки пути. Это дает возможность ставить в соответствие каждому пути не все вершины, которые первоначально служили разделителями частей, на которые делился путь ветвящейся программы, а только часть из них. На этом пути в некоторых случаях удается получить лучшие оценки, чем при применении метода из [20], особенно в тех случаях, когда ветвящиеся k -программы используются при получении нижних оценок сложности для ветвящихся программ без ограничений.

При применении метода А. Бородина, А. А. Разборова, Р. Смоленского [20] каждой единице булевой функции ставится в соответствие последовательность дуг ветвящейся программы. Это, с одной стороны, не требует приведения программы к «однородному» виду, но, с другой стороны, не позволяет объединять отрезки пути, т. е. каждому пути необходи-

мо ставить в соответствие все дуги, которые служили разделителями пути программы на части. При получении нижней оценки сложности ветвящейся программы этим методом требуется извлекать корень большой степени из мощности полученного покрытия множества единиц функции из (1).

Остановимся более подробно на особенностях каждого из методов доказательства.

I. Метод Окольниковой. Показано, что каждую ветвящуюся программу, как детерминированную [10], так и недетерминированную [11, 31], можно без существенного увеличения сложности привести к однородному виду, где для любой пары вершин и любой переменной x_i кратность появления вершин, помеченных этой переменной, на пути, ведущем из одной вершины этой пары в другую вершину этой пары, не зависит от пути (для различных переменных эти числа могут быть различными). При этом сложность возрастает незначительно. Зафиксируем некоторые числа p и t , $k \leq p \leq t$. Каждый путь однородной k -программы, реализующей булеву функцию f , разобьем на t отрезков. Показано, что любой единице γ булевой функции можно поставить в соответствие подмножество $\Psi(\gamma)$, состоящее из $2p$ вершин ветвящейся программы, с которым ассоциируется функция *

$$g_{\Psi(\gamma)} = g_{\Psi}^1(\gamma)(X_0 \cup X_1) \cdot g_{\Psi}^2(\gamma)(X_0 \cup X_2),$$

при этом $g_{\Psi(\gamma)}(\gamma) = 1$, множества X_0, X_1, X_2 попарно не пересекаются, $|X_1| \geq n_1(p, t)$, $|X_2| \geq n_2(p, t)$ и $|X_0| \leq n_0 = n - n_1 - n_2$, где величины $n_1(p, t)$ и $n_2(p, t)$, найденные комбинаторными методами, имеют следующий вид:

$$n_1(n; k, p, t) = \left[n \binom{t-k}{p-k} / \binom{t}{p} \right]; \quad (2)$$

$$n_2(n; k, p, t) = n - p \lceil kn/t \rceil + (k-1) \left[n \binom{t-k}{p-k} / \binom{t}{p} \right]; \quad (3)$$

$$n_0(n; k, p, t) = n - n_1 - n_2. \quad (4)$$

Это позволяет оценить число $2p$ -вершинных подмножеств в программе \mathcal{P}_0 и, следовательно, число вершин программы.

Рассмотрим всевозможные представления функции f в виде

$$f(X) = \bigvee_{i=1}^{R(f; k, p, t)} g^1(X_1^i \cup X_0^i) \wedge g^2(X_2^i \cup X_0^i), \quad (5)$$

где $|X| = n$; X_1^i, X_2^i, X_0^i — непересекающиеся множества; $X = X_1^i \cup X_2^i \cup X_0^i$; и при этом $|X_1^i| \geq n_1(n; k, p, t)$, $|X_2^i| \geq n_2(n; k, p, t)$, $|X_0^i| = n - |X_1^i| - |X_2^i|$.

Минимальное число дизъюнктивных членов в представлении (5) обозначим через $R(f; n, k, p, t)$.

Теорема 4. Пусть f — булева функция, существенно зависящая от n переменных, $n \geq 16$; k, p и t , $k \leq p \leq t$, — произвольные натуральные числа такие, что величины $n_1(n; p, k, t)$, $n_2(n; p, k, t)$ и $n_0(n; p, k, t)$, вычисленные по формулам (2)–(4), положительны.

(а) Сложность $\text{NBP}_k(f)$ реализации булевой функции f недетерминированными k -программами удовлетворяет неравенству

$$\text{NBP}_k(f) \geq \max \left\{ n; \frac{1}{4} \sqrt{\frac{2p}{et}} \cdot (R(f; n, k, p, t))^{1/(4p)} \right\}.$$

(б) Сложность $\text{BP}_k(f)$ реализации булевой функции f детерминированными k -программами удовлетворяет неравенству

$$\text{BP}_k(f) \geq \max \left\{ n; \frac{2p}{et} \cdot (R(f; n, k, p, t))^{1/(2p)} \right\}.$$

*) Эта функция состоит из всех конъюнкций, которым соответствуют пути, проходящие через это подмножество вершин.

Обозначим через $H_i(f)$ максимальное число единиц булевой функции f , принадлежащих грани куба размерности i . Легко видеть [12, лемма 5], что величина $R(f; n, k, p, t)$ удовлетворяет неравенству

$$R(f; n, k, p, t) \geq \frac{|f^{-1}(1)|}{2^{n_0} H_{n_1}(f) H_{n_2}(f)}. \quad (6)$$

Другие оценки для величины $R(f; n, k, p, t)$ можно найти в [10]. Это позволяет оценить как общее число вершин однородной ветвящейся программы, так и общее число вершин ветвящейся программы. Этим методом или некоторой модификацией этого метода было получено несколько оценок экспоненциального вида для сложности ветвящихся k -программ, в том числе для характеристических функций графов [10, 31].

II. Метод Бородина, Разборова, Смоленского. В [20] доказательство проводится для ациклических контактно-вентильных схем. При этом каждой единице булевой функции ставится в соответствие подмножество из qk дуг программы, где q — заранее выбранное фиксированное число. С каждым подмножеством ассоциируется функция $f_i = \bigwedge_{j=1}^{kq} f_{i,j}(X_{i,j})$, где ограничения на функции $f_{i,j}$ и множества переменных $(X_{i,j})$ даны в следующей теореме.

Теорема 5. Пусть $f: R^n \rightarrow \{0, 1\}$ — функция от n переменных, k, q — положительные целые числа, и пусть $T = (2 \text{NBP}_k(f))^{2kq}$. Тогда f может быть представлена в виде

$$f = \bigvee_{i=1}^T \bigwedge_{j=1}^{kq} f_{i,j}(X_{i,j}),$$

где $f_{i,j}$ — функция, зависящая только от переменных из $X_{i,j} \subseteq \{x_1, \dots, x_n\}$, $|X_{i,j}| \leq \lfloor n/q \rfloor$, и для любого i каждая переменная принадлежит самое большее k из множеств $\{X_{i,1}, \dots, X_{i,kq}\}$.

Этот метод получил название метода (k, q) -прямоугольников. Он позволил получить нижние оценки экспоненциального вида для сложности реализации ряда функций недетерминированными ветвящимися k -программами при $k \leq \log N$.

С. П. Юкна [27] применил этот метод для характеристических функций кодов, рассмотренных в [10], и получил экспоненциальные оценки для этих функций в классе недетерминированных ветвящихся k -программ.

III. Дж. Тхатхачар [41] модифицировал метод работы [20]. При $q = O(k \cdot 2^k)$ он для каждого i , $1 \leq i \leq T$, разбил множества переменных $X_{i,j}$ из теоремы 5 на два подмножества, что позволило ему сформулировать теорему 3 [20] в виде близком к (5). При этом мощности множеств X_1 и X_2 оцениваются снизу величиной $(2/3)N/2^k$. Оценки снизу на мощности множеств X_1 и X_2 получены с помощью теоретико-вероятностных рассуждений. Число дуг, которые ставятся в соответствие каждой единице булевой функции равно $O(k^2 \cdot 2^k)$. Функции, для которых в [41] были получены экспоненциальные нижние оценки сложности k -программ, будут приведены ниже в п. 6.3, посвященном иерархии ветвящихся k -программ.

Методы [10, 11, 31, 41] позволяют получать высокие нижние оценки сложности реализации булевых функций ветвящимися k -программами функций, обладающих следующим свойством. Пусть $g(Y_1 \cup Y_2)$ — произвольная подфункция функции f , множества Y_1 и Y_2 попарно не пересекаются, и мощности множеств Y_1 и Y_2 достаточно велики и при этом представление функции g в виде

$$\bigvee_i (g_i(Y_1) \wedge g_i(Y_2)) \quad (7)$$

требует большого числа дизъюнктивных членов.

6.3. Иерархия ветвящихся k -программ. В связи с тем, что одну и ту же функцию можно реализовать ветвящимися k -программами с различными значениями k , возникает вопрос о соотношении сложностей реализации одной и той же булевой функции ветвящимися k_1 -и k_2 -программами. В работах [9, 20, 25, 46] показано, что сложность реализации некоторых последовательностей булевых функций ветвящимися 1-программами в экспоненциальное число раз (по числу переменных булевой функции) превышает сложность реализации тех же булевых функций ветвящимися 2-программами.

В [31] было показано, что для любого натурального k , $k \geq 2$, существует последовательность булевых функций такая, что сложность реализации функций из этой последовательности в классе недетерминированных синтаксических ветвящихся k -программ в экспоненциальное число раз (по числу переменных булевой функции) превосходит сложность реализации той же функции в классе недетерминированных синтаксических ветвящихся $(k \ln k / \ln 2 + C)$ -программ, где C — константа, не зависящая от k .

В [41] приведены примеры булевых функций, сложности реализации которых недетерминированными ветвящимися k -и $(k+1)$ -программами отличаются в экспоненциальное число раз. Функция, на которой достигается экспоненциальный разрыв в сложности между k -и $(k+1)$ -программами, определена на k -мерном гиперкубе $[1, n]^k$. Рассматривается n гиперплоскостей перпендикулярных к d -й оси, $d \in [1, k]$, называемых d -плоскостями. Другими словами, i -я d -плоскость, $i \in [1, n]$, — множество $\{v \in [1, n]^k : v_d = i\}$. Пусть X_i^d обозначает множество переменных соответствующих i -й d -плоскости. Пусть через $H_d(X)$ для $d \in [1, k]$ обозначается $\sum_{i \in [1, n]} \prod_{x \in X_i^d} x$ над $GF(q)$. Ясно, что $|X_i^d| = n^{k-1}$. Рассматриваются функции

$$HSP_q^k(X) = true \stackrel{\text{def}}{\iff} \sum_d H_d(X) \equiv 0 \pmod{q},$$

$$CHSP_q^k(X) = true \stackrel{\text{def}}{\iff} \forall d \bigwedge_{d \in [1, k]} H_d(X) \equiv 0 \pmod{q}.$$

Показано, что сложность реализации функций HSP_q^{k+1} и $CHSP_q^{k+1}$ в классе детерминированных $(k+1)$ -программ линейна, а сложность реализации этих функций в классе недетерминированных k -программ — $O(N^{1/(k+1)})$.

6.4. Нижние оценки для схем без ограничений. Перейдем к методу получения нелинейных нижних оценок для ветвящихся программ без ограничений [10, 12, 30]. Пусть \mathcal{P} — произвольная ветвящаяся (детерминированная или недетерминированная) программа, реализующая булеву функцию $f(x_1, x_2, \dots, x_n)$. Если для какой-то переменной x_i число проверок по этой переменной в некоторой цепи (пути) от входной вершины к выходной превышает $k(n)$, то число вершин ветвящейся программы, помеченных переменной x_i , больше чем $k(n)$, где $k(n) \rightarrow \infty$ при $n \rightarrow \infty$. Если число таких переменных не очень мало, то сложность ветвящейся программы \mathcal{P} не может быть малой. Если число таких переменных мало, то можно «забить» эти переменные константами, что позволит от первоначальной схемы перейти к схеме с ограничениями на число проверок каждой переменной в цепи, т. е. рассмотреть реализацию некоторой подфункции функции f ветвящейся k -программой. Этот метод позволяет получать нетривиальные нижние оценки сложности реализации булевых функций ветвящимися программами для функций, обладающих свойством, описанным в конце п. 6.2, т. е. для функций, представление любой из подфункций которых в виде (7) содержит большое число дизъюнктивных членов. Теорема 7 позволяет получать нетривиальные оценки также для функций с множеством единиц, достаточно равномерно распределенных по граням куба.

Пусть $f(x_1, x_2, \dots, x_n)$ — булева функция, $X' = \{x_i, \dots, x_m\}$ — подмножество множества переменных функции f , а $\alpha = \{\alpha_{i_1}, \dots, \alpha_{i_m}\}$ — множество констант. Через $f|_{X'=\alpha}$ обозначим функцию, которая получается из f подстановкой констант из α вместо переменных из X' , а именно, заменой переменной x_{i_j} на константу α_{i_j} , $1 \leq j \leq m$.

Показано ([12, Теорема 1]), что можно получать нижние оценки сложности реализации булевых функций ветвящимися программами без ограничений, используя ветвящиеся k -программы.

Теорема 6. Пусть $g(X)$ — булева функция, и C — константа, $0 < C < 1$. Пусть для любого подмножества переменных X_0 , $X_0 \subseteq X$ и $|X_0| = \lfloor Cn \rfloor$, существует такая подстановка констант из α в X_0 , что сложность реализации функции $g|_{X_0=\alpha}(X \setminus X_0)$ недетерминированными (детерминированными) ветвящимися $k(n)$ -программами не менее чем $n\psi(n)$, где $\psi(n)$ — растущая функция. Тогда сложность реализации функции g недетерминированными (детерминированными) ветвящимися программами без ограничений не меньше $\min\{Cnk(n), n\psi(n)\}$.

Используя теоремы 4 и 6, а также (6), получаем следующее утверждение.

Теорема 7. Пусть заданы последовательность булевых функций $g_n(X)$, $|X| = n$, растущая функция $k(n)$ и константа C , $0 < C < 1$. Если для любого подмножества переменных X_0 , $X_0 \subseteq X$, $|X_0| = \lfloor Cn \rfloor$, существует подстановка констант из α в множество X_0 , и целочисленные $p(n)$, $t(n)$, $k(n) \leq p(n) \leq t(n)$, такие что $n_0(|X \setminus X_0|, k, p, t)$, $n_1(|X \setminus X_0|, k, p, t)$ и $n_2(|X \setminus X_0|, k, p, t)$, вычисленные по формулам (2)–(4), положительны, тогда

$$\text{NBP}(g_n) \geq \min\left\{Cnk(n), 1/4 \cdot \sqrt{2p/(et)} \cdot (R(g_n|_{X_0=\alpha}; k, p, t))^{1/(4p)}\right\}$$

Напомним, что через $H_i(f)$ было обозначено максимальное число единиц булевой функции f , принадлежащих грани куба размерности i .

Теорема 8. Пусть заданы последовательность булевых функций $g_n(X)$, $|X| = n$, растущая функция $k(n)$ и константа C , $0 < C < 1$. Тогда для сложности реализации функции g_n недетерминированными ветвящимися программами без ограничений справедливо соотношение

$$\text{NBP}(g_n) \geq \min\left\{Cnk(n), \frac{1}{4} \sqrt{\frac{2p}{et}} \cdot \left(\frac{|g_n^{-1}(1)|}{2^{n-n_1-n_2} H_{n_1}(g_n) H_{n_2}(g_n)}\right)^{1/(4p)}\right\},$$

где $n_1 = n_1(\lfloor (1-C)n \rfloor, k, p, t)$, $n_2 = n_2(\lfloor (1-C)n \rfloor, k, p, t)$.

Эти результаты позволили получить нелинейные нижние оценки для сложности реализации характеристических функций кодов Боуза–Чоудхури–Хоквингема с кодовым расстоянием $\log n / \log \log n$ в классе детерминированных ветвящихся программ и для характеристических функций кодов Риды–Маллера в классе недетерминированных ветвящихся программ.

6.5. Упорядоченные бинарные деревья решений. Широкое распространение получили исследования по сложности упорядоченных бинарных деревьев решений (OBDD — ordered binary decision diagrams), которые были введены Р. Е. Брайантом (1986) [21]. OBDD — это ветвящаяся 1-программа с предписанным порядком переменных. На каждом пути от входной вершины к выходной, переменные должны проверяться в соответствии с этим порядком. OBDD очень важны для приложений. Этот тип схем часто используется для задания функций. В частности, в теории кодирования

иногда для задания кодов используются именно этот тип программ (trellises) (см. [28]). Этот класс схем исследовался в ряде работ [19, 22, 26]. Обзоры по упорядоченным бинарным деревьям решений см. в [23, 44, 45].

При подготовке данного обзора использовались также обзоры по сложности ветвящихся программ из работ П. Пудлака [33], И. Вегенера [42, 45], И. Вегенера и Д. Зилинга [39], А. А. Разборова [35], диссертации М. Зауэрхоффа [36], а также из ряда работ других авторов.

СПИСОК ЛИТЕРАТУРЫ

1. Грибок С. В. О поведении функции Шеннона для бинарных программ // *Материалы X Межгосударственной школы-семинара «Синтез и сложность управляющих систем»* (Минск, 29 ноября – 3 декабря 1999 г.) — М.: Издательство центра прикладных исследований при механико-математическом факультете МГУ, 2000. — С. 4–7.
2. Гринчук М. И. О сложности реализации симметрических булевых функций контактными схемами // *Диссертация канд. физ.-мат. наук.* — М., 1989.
3. Гринчук М. И. О сложности реализации симметрических булевых функций контактными схемами // *Математические вопросы кибернетики. Вып. 3.* — М.: Наука, 1991. — С. 77–114.
4. Касим-Заде О. М. О сложности реализации функций в одном классе алгоритмов // *Материалы IX Межгосударственной школы-семинара «Синтез и сложность управляющих систем»* — М.: Изд-во механико-математического факультета МГУ, 1999. — С. 25–30.
5. Кузьмин В. А. Оценка сложности реализации функций алгебры логики простейшими видами бинарных программ // *Методы дискретного анализа в теории кодов и схем. Вып. 29.* — Новосибирск, ИМ СО АН СССР, 1976. — С. 11–39.
6. Лупанов О. Б. О вентильных и контактно-вентильных схемах // *Докл. АН СССР.* — 1956. — Т. 111, № 6. — С. 1171–1174.
7. Лупанов О. Б. К вопросу о реализации симметрических функций алгебры логики контактными схемами // *Проблемы кибернетики. Вып. 15.* — М.: Наука, 1965. — С. 85–101.
8. Нечипорук Э. И. Об одной булевой функции // *Докл. АН СССР.* — 1966. — Т. 169, № 4. — С. 765–766.
9. Окольнішнікова Е. А. Об одном соотношении сложностей булевых функций // VIII Всесоюз. конф. по пробл. теор. кибернетики (Горький, 1988). Тез. докл. — Горький: Горьковский университет, 1988. — С. 63.
10. Окольнішнікова Е. А. Нижние оценки сложности реализации характеристических функций двоичных кодов бинарными программами // *Методы дискретного анализа в синтезе реализаций булевых функций. Вып. 51.* — Новосибирск, ИМ СО АН СССР, 1991. — С. 61–83.
11. Окольнішнікова Е. А. О сравнении сложностей недетерминированных ветвящихся k -программ // *Дискретный анализ и исследование операций.* — 1999. — Т. 6, № 1. — С. 65–85.
12. Окольнішнікова Е. А. Об одном методе получения нижних оценок сложности реализации булевых функций ветвящимися программами // *Дискретный анализ и исследование операций.* — 2001. — Т. 8, № 4. — С. 76–102.
13. Разборов А. А. Нижние оценки сложности реализации симметрических булевых функций контактно-вентильными схемами // *Матем. заметки.* — 1990. — Т. 48, № 6. — С. 79–90.
14. Andreev A., Baskakov Ju., Clementi A., Rolim J. Small pseudo-random sets yield hard functions: New tight explicit lower bounds for branching programs // *Proc. of ICALP'99 (Prague, 1999).* — Lect. Notes Comp. Sci. — 1999. — V. 1644. — P. 179–189.
15. Alon N., Maass W. Meanders and their applications in lower bound arguments // *J. Computer and System Sci.* — 1988. — V. 37. — P. 118–129.
16. Babai L., Hajnal P., Szemerédi E., Turán G. A lower bound for read-once-only branching programs // *J. Computer and System Sci.* — 1987. — V. 35, № 2. — P. 153–162.
17. Babai L., Pudlák P., Rödl V., Szemerédi M. Lower bounds to the complexity of symmetric Boolean functions // *Theor. Comp. Sci.* — 1990. — V. 74. — P. 313–324.
18. Barrington D. A. M. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 // *J. Computer and System Sci.* — 1989. — V. 38. — P. 150–164. [Имеется перевод: Баррингтон Д. А. М. Ветвящиеся программы ограниченной ширины, имеющие полиномиальную сложность, распознают в точности языки из NC^1 // *Кибернетик. сб. Новая серия. Вып. 28.* — М.: Мир, 1991. — С. 94–113.]
19. Bollig B., Sauerhoff M., Seiling D., Wegener I. Hierarchy theorems for k OBDDs and k IBDDs // *Theor. Comp. Sci.* — 1998. — V. 205. — P. 45–60.
20. Borodin A., Razborov A., Smolensky R. On lower bounds for read- k -times branching programs // *Computational Complexity.* — 1993. — V. 3, № 1. — P. 1–18.

21. Bryant R. E. Graph-based algorithms for Boolean function manipulation // *IEEE Trans. on Computers.* — 1986. — V. C-35. — P. 677–691.
22. Bryant R. E. On the complexity of VLSI implementation and graph representations of Boolean functions with application to integer multiplication // *IEEE Trans. on Computers.* — 1991. — V. C-40, № 2. — P. 205–213.
23. Bryant R. E. Symbolic Boolean manipulation with ordered binary decision diagrams // *ACM Computing Surveys.* — 1992. — V. 24, № 3. — P. 293–318.
24. Cobham A. The recognition problem for the set of perfect squares // *Proc. of the 7th Symp. on Switching and Automata Theory (SWAT).* — 1966. — P. 78–87.
25. Dunne P. E. Lower bounds on the complexity of 1-time only branching programs (preliminary version) // *Proc. of Fundamentals of Computation Theory.* — *Lect. Notes Comp. Sci.* — 1985. — V. 199. — P. 90–99.
26. Hosaka K., Takenaga Y., Kaneda T., Yajima S. On the size of binary decision diagrams representing threshold function // *Proc. of the 5th Int. Symp. on Algorithms and Computation.* — *Lect. Notes Comp. Sci.* — 1994. — V. 834. — P. 584–592.
27. Jukna S. A note on read- k times branching programs // *RAIRO Inform. Théor. Appl.* — 1995. — V. 29, № 1. — P. 75–83.
28. Lafferty J., Vardy A. Ordered binary decision diagrams and minimal trellises // *IEEE Trans. on Computers.* — 1999. — V. 48, № 9. — P. 971–986.
29. Lee C. Y. Representation of switching circuits by binary-decision programs // *Bell System Technical J.* — 1959. — V. 38. — P. 985–999. [Имеется перевод: Ли К. Представление переключательных схем с помощью программ двоичного решения // *Вопросы теории математических машин.* — М.: Машиностроение, 1964. — С. 219–232.]
30. Okol'nishnikova E. A. Lower bounds on branching programs // *Siberian Adv. Math.* — 1993. — V. 3, № 1. — P. 152–166.
31. Okol'nishnikova E. A. On the hierarchy of nondeterministic branching k -programs // *Fundamentals of computation theory (11th Int. Symp. FCT 97).* — *Lect. Notes Comp. Sci.* — 1997. — V. 1279. — P. 376–387.
32. Pudlák P. A lower bound on complexity of branching programs // *Proc. of the 11th Int. Symp. on Math. Foundations of Comp. Sci. (MFCS).* — *Lect. Notes Comp. Sci.* — 1984. — V. 176. — P. 480–489.
33. Pudlák P. The hierarchy of Boolean circuits // *Comput. Artificial Intelligence.* — 1987. — V. 6, № 5. — P. 449–468.
34. Pudlák P., Žak S. Space complexity of computations // *Univ. Prague / Techn. Rep.* — 1983.
35. Razborov A. A. Lower bounds for deterministic and nondeterministic branching programs // *Fundamentals of Computation Theory (Gosen, 1991).* — *Lect. Notes Comp. Sci.* — 1991. — V. 529. — P. 47–60.
36. Sauerhoff M. Complexity theoretical results for randomized branching programs // *Dissertation zur Erlangung des Grades eines Doktors der Naturwissenschaften der Universität Dortmund am Fachbereich Informatik.* — Dortmund, 1998.
37. Sauerhoff M., Wegener I., Werchner R. Relating branching program size and formula size over the full binary basis // *STACS'99.* — *Lect. Notes Comp. Sci.* — 1999. — V. 1563. — P. 57–67.
38. Savincký P., Žak S. A large lower bound for 1-branching programs // *ECCC, revision 01 of Techn. Rep. 96-036.* — *Electronic Colloquium on Computational Complexity.* — 1996. — available at <http://www.eccc.uni-trier.de/eccc/>.
39. Sieling D., Wegener I. New lower bounds and hierarchy results for restricted branching programs // *Graph-theoretical concepts in computer science. 20th Int. workshop, WG'94 (Herrsching, June 16–18, 1994).* — *Lect. Notes Comp. Sci.* — 1995. — V. 903. — P. 359–370.
40. Simon J., Szegedy M. A new lower bound for read only once branching programs and its applications // *Adv. in computation complexity.* — AMS, 1993. — V. 13. — P. 183–193.
41. Thathachar J. S. On separating the read- k -times program hierarchy // *Proc. of the 30th Ann. ACM Symp. on Theory of Computing (STOC, 1998).* — P. 652–662. (См. также *ECCC, Techn. Rep. TR98-002.* — 1998. — available at <http://www.eccc.uni-trier.de/eccc/>.)
42. Wegener I. The complexity of Boolean functions. — Stuttgart: B. G. Teubner; Chichester: John Wiley & Sons, 1987.
43. Wegener I. On the complexity of branching programs and decision trees for clique functions // *J. of the ACM.* — 1988. — V. 35, № 2. — P. 461–471.
44. Wegener I. Efficient data structures for Boolean functions // *Discrete Math.* — 1994. — V. 136. — P. 347–372.
45. Wegener I. Branching programs and binary decision diagrams. Theory and applications. — Philadelphia, PA: SIAM, 2000.
46. Žak S. An exponential lower bound for one-time-only branching programs // *Proc. of the 11th Int. Symp. on Math. Foundations of Comp. Sci. (MFCS).* — *Lect. Notes Comp. Sci.* — 1984. — V. 176. — P. 562–566.