

О СООТНОШЕНИИ ВРЕМЕНИ ВЫЧИСЛЕНИЯ ПРЯМОГО И ОБРАТНОГО ОТОБРАЖЕНИЙ

Э. Ш. Коспанов

Показано, что минимально-возможная глубина схемы из функциональных элементов в базисе $\{\&, \vee, \neg\}$, реализующей отображение множества всех $(0, 1)$ -векторов длины n на себя, может отличаться от минимально-возможной глубины схемы, реализующей обратное отображение (в том же базисе), не менее чем на $2 \log_2 n - 3$, а для «почти всех» отображений эта величина не больше 4.

1. Постановка задачи

Пусть $T = \{0, 1, \dots, 2^n - 1\}$, где n — любое натуральное число, а $\Phi(n)$ — отображение множества T на себя. Таким образом, $\Phi(n)$ — числовая функция, имеющая обратную, и можно говорить о сравнении «сложностей» прямой ($\Phi(n)$) и обратной ($\Phi^{-1}(n)$) функций. Задачи такого рода возникают, например, в криптографии [1, 2], когда требуется найти такую «простую» функцию, обратная к которой была бы «сложной». Под сложностью функции в этом случае обычно понимают сложность алгоритма, вычисляющего эту функцию. В [3] изучается задача, близкая к рассматриваемой здесь, но под сложностью функции понимается число элементов в схеме, реализующей эту функцию.

В настоящей работе под сложностью функции мы будем понимать глубину схемы из функциональных элементов в базисе $\{\&, \vee, \neg\}$, реализующей эту функцию. Глубина схемы, или длина максимальной цепи в ней, выбрана в качестве меры сложности по той причине, что с помощью этого параметра можно характеризовать быстродействие схемы. Это следует из результатов В. М. Храпченко [4, 5], где показано, что глубина формулы (значит, и глубина функции) совпадает с задержкой (временем срабатывания схемы), хотя существуют минимальные (по числу элементов) схемы, в которых эти величины — глубина и быстродействие — сильно разнятся.

ЗАМЕЧАНИЕ. Такие понятия, как базис, схема, глубина схемы, глубина формулы, которыми мы пользуемся, но не определяем, широко известны; их можно найти, например, в [6–9].

Уточним теперь постановку задачи.

Пусть $A(n)$ есть $(0,1)$ -матрица с n столбцами и 2^n попарно различными строками, а $\Phi(n)$ — отображение множества строк из $A(n)$ на себя. Результат такого отображения есть матрица $A'(n)$ с количеством строк и столбцов, как у матрицы $A(n)$.

Припишем булевы переменные x_1, x_2, \dots, x_n столбцам матрицы $A(n)$, а булевы переменные y_1, y_2, \dots, y_n столбцам матрицы $A'(n)$. Поскольку в матрицах $A(n)$ и $A'(n)$ нет одинаковых строк, можно говорить, что любой столбец y_i матрицы $A'(n)$ есть булева функция f_i от переменных x_1, x_2, \dots, x_n , и наоборот, каждый столбец x_i матрицы $A(n)$ есть булева функция g_i от переменных y_1, y_2, \dots, y_n ($i = 1, 2, \dots, n$).

Итак, имеется две системы булевых функций, определяемые отображением $\Phi(n)$:

$$F = \{f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n)\},$$

$$F^{-1} = \{g_1(y_1, y_2, \dots, y_n), g_2(y_1, y_2, \dots, y_n), \dots, g_n(y_1, y_2, \dots, y_n)\}.$$

Пусть $S(F)$ — схема из функциональных элементов в базисе $\{\&, \vee, \neg\}$, реализующая систему функций F , а $D(S)$ — глубина этой схемы. Рассмотрим величину $D(F) = \min D(S)$, где минимум берется по всем схемам, реализующим систему F над базисом $\{\&, \vee, \neg\}$. Аналогичным образом определяется величина $D(F^{-1})$ для системы F^{-1} . Введем величины $d(\Phi) = |D(F) - D(F^{-1})|$ и $d(n) = \max d(\Phi)$, где максимум берется по всем рассматриваемым отображениям.

Задача, исследуемая в данной статье, состоит в оценке величины $d(n)$. В разд. 2 описывается поведение $d(\Phi)$ в «типичном» случае, в разд. 3 приводится пример отображения с «ощутимым» различием глубины, а в разд. 4 — класс таких отображений $\{\Phi\}$, что $d(\Phi) = 0$.

2. «Типичный» случай

Пусть P_4 есть класс таких отображений $\Phi(n)$, что для любого отображения Φ из P_4 верно неравенство $d(\Phi) \leq 4$.

Теорема 1. При $n \rightarrow \infty$

$$|P_4|/2^n! \rightarrow 1.$$

Доказательство. Для установления справедливости теоремы нам потребуются следующие известные факты.

Утверждение 1 [8]. Если имеется схема глубины D в базисе $\{\&, \vee, \neg\}$, реализующая булеву функцию f , то имеется и формула глубины D в этом же базисе, реализующая функцию f .

Утверждение 2 [9]. Если число вхождений переменных в формуле, реализующей булеву функцию в базисе $\{\&, \vee, \neg\}$, не меньше k , то глубина этой формулы не меньше $\log_2 k$.

Утверждение 3 [6]. Число булевых функций, которые зависят не более чем от n переменных и которые могут быть реализованы формулами в базисе $\{\&, \vee, \neg\}$, содержащими не более k вхождений переменных, не превосходит $(cn)^k$, где c — некоторая константа.

Утверждение 4 [9]. В базисе $\{\&, \vee, \neg\}$ любая булева функция от n переменных может быть реализована схемой глубины не более чем $n - \log_2 n + 3$.

Число всех отображений, равное $2^n!$, может быть подсчитано следующим способом. Матрица A' , задаваемая отображением Φ , получается из матрицы A перестановкой ее строк. Поэтому в любом столбце из A' число нулей равно числу единиц, любая пара столбцов есть матрица, в которой число строк типа (i, j) равно числу строк типа (k, l) для любых i, j, k, l из $\{0, 1\}$, и т. д. Поэтому верно следующее равенство:

$$2^n! = \binom{2^n}{2^{n-1}} \binom{2^{n-1}}{2^{n-2}}^2 \binom{2^{n-2}}{2^{n-3}}^4 \dots 2^{2^{n-1}}. \quad (1)$$

Обозначив произведение всех сомножителей, кроме первого, в правой части равенства (1) через M_n , получаем следующее равенство:

$$2^n! = M_n \binom{2^n}{2^{n-1}}. \quad (2)$$

Теперь рассмотрим такие отображения, в которых любая функция из системы F может быть реализована формулой, содержащей не более $2^{n-1}/\log_2 n$ вхождений переменных x_1, x_2, \dots, x_n . Из утверждения 3 следует, что число таких функций не превосходит величины

$$(cn)^{2^{n-1}-\log_2 \log_2 n} \stackrel{\text{def}}{=} m_n.$$

Число отображений таких, что система функций F для каждого из них состоит лишь из функций, допускающих реализацию формулами сложности не выше $2^{n-1}/\log_2 n$, может быть оценено сверху с помощью (2). Так как первый столбец матрицы A' может быть лишь такой функцией, которая допускает реализацию формулой сложности не более $2^{n-1}/\log_2 n$, то он может быть выбран не более чем m_n способами. Теперь, заменяя в правой части равенства (2) второй сомножитель на m_n , получаем верхнюю оценку для числа искомых отображений, которая равна $m_n M_n$. С учетом (2) и неравенства $\binom{2^n}{2^{n-1}} > 2^{2^n-n}$ убеждаемся в том, что при $n \rightarrow \infty$

$$\frac{m_n M_n}{2^n!} \rightarrow 0. \quad (3)$$

Соотношение (3) показывает, что доля тех отображений, которые не могут быть реализованы формулами, содержащими менее $2^{n-1}/\log_2 n$

вхождений переменных, стремится к 1 при $n \rightarrow \infty$. Иными словами, «почти все» прямые отображения не могут быть реализованы формулами, содержащими менее $2^{n-1}/\log_2 n$ вхождений переменных. Используя утверждения 1 и 2, мы можем заключить, что глубина схем, реализующих такие отображения, не меньше $n - \log_2 \log_2 n - 1$.

Множество этих отображений обозначим через P_0 . Каждому отображению Φ из множества P_0 соответствуют матрицы $A(n)$ и $A'(n)$.

Выше, зафиксировав матрицу $A(n)$, мы отобрали подходящее множество матриц $\{A'(n)\}$. Теперь же, упорядочив в естественном порядке строки каждой матрицы из $\{A'(n)\}$ для всех отображений из множества P_0 , мы получим множество матриц $\{A(n)\}$. Проведя аналогичные рассуждения относительно множества $\{A(n)\}$, приходим к заключению, что «почти все» отображения из множества P_0 таковы, что глубина схем, реализующих как прямое, так и обратное отображение, для них не меньше величины $n - \log_2 \log_2 n - 1$.

Полученное множество отображений, которое мы обозначим через P'_4 , таково, что любые прямое и обратное отображения не могут быть реализованы схемой глубины менее чем $n - \log_2 \log_2 n - 1$. Поскольку любую булеву функцию от n переменных можно реализовать схемой, глубина которой не превосходит $n - \log_2 \log_2 n + 3$ (утверждение 4), то «почти все» отображения таковы, что глубины любого как прямого, так и обратного отображения различаются не более чем на 4. Итак, множество P'_4 обладает требуемыми свойствами. Множество P_4 , указанное в формулировке теоремы 1, содержит множество P'_4 , поэтому теорема 1 доказана.

Оценку $d(\Phi) \leq 4$ можно несколько усилить, если утверждение 4 заменить более точным, содержащимся в работе С. А. Ложкина [10], что, впрочем, не меняет качественной картины в «типичном» случае.

3. Нижняя оценка для $d(n)$

Пусть, как и прежде, $A(n)$ есть $(0,1)$ -матрица с 2^n строками и n столбцами, а x_1, x_2, \dots, x_n — булевы переменные, приписанные ее столбцам. Рассмотрим следующие n булевых функций:

$$y_1 = x_1, y_2 = x_1 \oplus x_2, \dots, y_n = x_1 \oplus x_2 \oplus \dots \oplus x_n \quad (4)$$

(символ \oplus обозначает операцию сложения по mod 2). Равенства (4) задают отображение множества строк матрицы $A(n)$ на себя, которое мы обозначим через Φ_0 .

Обратимость Φ_0 устанавливается следующим образом. Рассматривая равенства (4) как систему уравнений, разрешим ее относительно

переменных x_1, x_2, \dots, x_n . Легко видеть, что решения этой системы таковы:

$$x_1 = y_1, x_2 = y_1 \oplus y_2, x_3 = y_2 \oplus y_3, \dots, x_n = y_{n-1} \oplus y_n. \quad (5)$$

Разрешимость системы (4) показывает обратимость Φ_0 , а равенства (5) задают систему функций, порождающих обратное отображение Φ_0^{-1} . Система (4) состоит из линейных функций. Сложность реализации линейной функции в базисе $\{\&, \vee, \neg\}$ хорошо изучена. В частности, В. М. Храпченко [4] показал, что линейная булева функция, существенно зависящая от n переменных, не может быть реализована формулой, содержащей менее n^2 вхождений переменных. Поэтому, используя утверждения 1 и 2 предыдущего раздела, мы можем заключить, что глубина схемы, реализующей эту функцию, не может быть меньше $2 \log_2 n$. Функция y_n из (4) является линейной функцией, существенно зависящей от n переменных. Поэтому минимально-возможная глубина схемы, реализующей систему функций (4), равна $2 \log_2 n$. Но система (5) состоит из линейных функций, зависящих не более чем от двух переменных, и, как легко увидеть, существует схема глубины 3, реализующая эту систему. Поэтому для отображения Φ_0 , задаваемого системой функций F_0 , справедливо соотношение $d(\Phi_0) = 2 \log_2 n - 3$, иначе говоря, справедлива

Теорема 2. При любом $n \geq 1$

$$d(n) \geq 2 \log_2 n - 3.$$

4. «Правильные» отображения

В разд. 1 мы отмечали, что каждому отображению можно поставить в соответствие систему функций

$$F = \{f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n)\}, \quad (6)$$

а обратному отображению — систему функций

$$F^{-1} = \{g_1(y_1, y_2, \dots, y_n), g_2(y_1, y_2, \dots, y_n), \dots, g_n(y_1, y_2, \dots, y_n)\}. \quad (7)$$

Теперь укажем класс отображений, для которых множества F и F^{-1} совпадают. Такие отображения назовем «*правильными*».

Пусть Φ — некоторое отображение, а A и A' , как и прежде, матрицы, связанные с этим отображением. Если строки этих матриц считать двоичными записями чисел из множества $\{0, 1, \dots, 2^n - 1\}$, то Φ можно рассматривать как перестановку этого множества.

Рассмотрим перестановки, состоящие лишь из циклов длины 2. Пусть Φ — такая перестановка. Рассмотрим любой ее цикл. Пусть число α переходит в число β , а β переходит в число α . Тогда строке

матрицы A , являющейся двоичной записью числа α , отображение Φ ставит в соответствие строку матрицы A' , являющуюся двоичной записью числа β , и наоборот, строке матрицы A , являющейся двоичной записью числа β , отображение Φ ставит в соответствие строку матрицы A' , являющуюся двоичной записью числа α . Нетрудно видеть, что такое же соответствие устанавливает и обратное отображение Φ^{-1} . А это означает, что на одинаковых наборах значений переменных значения систем функций (6) и (7) совпадают.

Число рассматриваемых перестановок равно числу различных разбиений множества $\{0, 1, \dots, 2^n - 1\}$ на пары. Нетрудно видеть, что это число равно $2^n! / 2^{n-1}! 2^{2^{n-1}} = 2^{n2^{n-1}(1-o(1))}$. Это и есть нижняя оценка для числа правильных отображений.

Характерная особенность правильных отображений состоит в том, что шифровка сообщения, или построение системы F , и дешифровка, т. е. построение системы F^{-1} , производятся одной и той же схемой, которая может быть построена методом О. Б. Лупанова [11]. Число элементов такой схемы есть величина порядка $2^n/n$, глубина схемы не больше n , и в то же время «несанкционированная» дешифровка приводит к необходимости перебора $2^{n2^{n-1}(1-o(1))}$ вариантов.

ЛИТЕРАТУРА

1. Massey J. L. An introduction to contemporary criptology // Proc. IEEE. 1988. V. 76, N 5. P. 533-549.
2. Schneier B. Applied Criptography: Protokols, Algorithms and Source Codes in Criptography. New York: John Wiley & Sons, 1996.
3. Hiltgen A. P. L. Constructions of feebly-one-way families of permutations // Advances in Cryptology. AUSCRYPT'92. Berlin: Springer-Verl., 1993. P. 422-434. (Lecture Notes in Comput. Sci.; V. 718).
4. Храпченко В.М. . Различие и сходство между задержкой и глубиной // Проблемы кибернетики. М.: Наука. 1979. Вып. 35. С. 141-168.
5. Храпченко В. М. Новые соотношения между глубиной и задержкой // Дискрет. математика. 1995. Т. 7, вып. 4. С. 77-85.
6. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. М.: Наука, 1963. Вып. 10. С. 63-98.
7. Храпченко В. М. О сложности реализации линейной функции в классе π -схем // Мат. заметки. 1971. Т. 9, № 1. С. 35-40.
8. Храпченко В. М. Некоторые оценки времени умножения // Проблемы кибернетики. М.: Наука, 1978. Вып. 33. С. 221-228.

9. **Гашков С. Б.** О глубине булевых функций // Проблемы кибернетики. М.: Наука, 1978. Вып. 34. С. 265–268.
10. **Ложкин С. А.** О глубине функций алгебры логики в некоторых базисах // Ann. Univ. Sci. Budapest. Eötvös Sect. Comput. 1983. Т. 4. Р. 115–125.
11. **Лупанов О. Б.** Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. М.: Наука, 1965. Вып. 14. С. 31–111.

Адрес автора:

Россия,
630090 Новосибирск,
Университетский пр., 4,
Институт математики
им. С. Л. Соболева СО РАН

Статья поступила

5 июня 1996 г.