УДК 519.6

В.А. Орлов

О РЕАЛИЗАЦИИ КОНЕЧНОЗНАЧНЫХ ОТОБРАЖЕНИЙ

Рассмотрены вопросы реализации конечнозначных функций схемами из функциональных элементов. Предложено семейство k-значных базисов и показана их полнота. Для этих базисов построены методы синтеза схем из функциональных элементов, обеспечивающие асимптотически наилучшие оценки.

Email: orlovaldr@mail.ru

Ключевые слова: *схемы из функциональных элементов, k-значные логики, полнота систем функций, сложность схемы, функционалы Шеннона.*

Оптимальная реализация дискретных отображений различными средствами – актуальная задача теоретической и технической кибернетики. Эту задачу часто называют синтезом управляющих систем. Наиболее исследованной является реализация булевых функций схемами из функциональных элементов. В данной работе рассмотрены вопросы оптимальной реализации конечнозначных функций схемами из функциональных элементов.

Функция, переменные которой принимают значения из алфавита $A_k = \{0,1, ..., k-1\}, k \geq 2,$ и которая сама принимает значения из этого алфавита, называется *k-значной* [1]. Множество всех *k*-значных функций обозначается через P_k. Функции из P_2 часто называют булевыми.

Рассмотрим задачу о реализации функций из P_k схемами из функциональных элементов в произвольном базисе.

Пусть Ф – произвольная конечная полная система функций из P_k, $k \geq 2$, каждая из которых (кроме функций, тождественно равных константе) существенно зависит от конечного числа всех своих переменных. Константы считаем функциями от одной переменной. Системе Ф сопоставим базис B, состоящий из реализующих ее функции элементов с одним состоянием, каждому из которых приписано положительное число (вес элемента). Базис B будем называть k-значным, а булевым – 2-значный базис.

Из элементов базиса строим схемы, в которых каждый вход каждого элемента присоединен либо к выходу другого элемента, либо к входу схемы. При этом запрещается соединять выходы различных элементов и образовывать «петли обратной связи» (ориентированные

циклы). Выходами схемы являются выходы некоторых элементов. Известно, что каждая схема реализует систему функций из P_k. Заметим, что любой элемент базиса имеет один выход.

В данной работе критерием оптимальности схемы считаем сумму весов ее элементов. Эту сумму назовем *сложностью схемы* S и обозначим $L(S)$.

Практически наиболее востребованной является задача нахождения функционала $L^B(f)$, равного минимальной сложности схем в базисе B, реализующих функцию f. В настоящее время эффективного метода (отличного от перебора схем) решения этой задачи нет. Вследствие этого часто рассматривают задачу исследования асимптотического поведения функционала $L^B(k,n)$, равного максимуму функционалов $L^B(f)$, $f \in P_k^n$, где P_k^n – множество k-значных функций от переменных $x_1, x_2, ..., x_n$. При этом полагают, что k – фиксировано, а $n \to \infty$. Функционал $L^B(k,n)$ для $k=2$ обозначим $L^B(n)$. Отметим, что $|P_k^n| = k^{k^n}$.

Для имеющего не менее двух входов элемента базиса его приведенным весом [2] называют отношение веса к уменьшенному на единицу числу входов. Приведенным весом базиса называется минимум приведенных весов его элементов.

Базис, приведенный вес которого равен 1, называют *нормированным* [3]. Без ограничения общности, в дальнейшем будем рассматривать нормированные базисы.

Случай $k=2$ исследован достаточно хорошо. Приведем используемый далее результат О.Б. Лупанова [2].

Теорема 1. *Для любого нормированного* 2*-базиса* B

$$L^B(n) \sim \frac{2^n}{n}.$$

Отметим, что нижние оценки сложности схем, рассматриваемых в работе, получаются из «мощностных» соображений: оценивается число функций и число схем заданной сложности.

Для $k \geq 3$ до появления работ [4–6] рассматривалось поведение функционала $L^B(k,n)$ только при фиксированных базисах B (см., например [7]).

Обычно полагают, что функции из P_k^n определены на всех k^n наборах значений их переменных. Однако рассматривают и функции, значения которых на некоторых наборах безразличны. Такие функ-

ции называют *не всюду определенными*; при их реализации схемами необходимо полное доопределение. Реализация не всюду определенных *булевых* функций – хорошо исследованная область синтеза управляющих систем (отметим работы Э.И. Нечипорука, Л.А. Шоломова, А.А. Андреева).

Пусть A^1 и A^2 – подалфавиты алфавита A_k. Функцию, значения аргументов (значения выходов) которой принадлежат A^1 (принадлежат A^2), назовем (A^1, A^2)-функцией. (A_k, A_2)-функцию – $(k,2)$-функцией. На практике при реализации функций из P_k допустимо рассматривать и базисы, в которых некоторые элементы реализуют (A^1, A^2)-функции. При этом на схему накладываются дополнительные естественные ограничения: вход элемента E нельзя присоединять к выходу элемента, выходные значения которого могут не принадлежать входному алфавиту элемента E.

Функцию $f \in P_k$ одного аргумента будем задавать вектором, i-й компонент которого, $0 \le i \le k-1$, равен $f(i)$. Систему $F = \{f_1, f_2, ..., f_r\}$ (A_k, A_2)-функций одного аргумента назовем $(k,2)$-*достаточной*, если все столбцы (r,k)-матрицы, строки которой суть векторы функций из F, различны. Отметим, что $r \ge]\log_2 k[$. Пример $(7,2)$-*достаточно*й системы приведен ниже:

x	0	1	2	3	4	5	6
f_1	0	1	0	1	0	1	1
f_2	0	0	1	1	0	0	1
f_3	0	0	0	0	1	1	1

Пусть Φ_1 – система функций из P_k такая, что с помощью операций суперпозиции над Φ_1 можно получить:

- функционально полную систему булевых функций Φ_1^b;
- $(k,2)$-достаточную систему функций Φ_1^2;
- функцию $f_{2,k}$, которая на булевых наборах значений ее аргументов принимает все значения из алфавита A_k.

Нетрудно проверить, что система $\Phi_1^b \cup \Phi_1^2$ является $(k,2)$-полной.

Системе Φ_1 сопоставим базис B_1 и покажем, что любую функцию из P_k можно реализовать схемой в этом базисе.

Для простоты изложения будем полагать, что система Φ_1^b состоит из функции $\neg(x_1 \& x_2)$ (штрих Шеффера). Пусть E_1 – элемент с двумя входами, реализующий эту функцию и имеющий вес 1. Пусть $E_1^2, E_2^2, ..., E_r^2$ – элементы, реализующие функции из Φ_1^2 и имеющие вес k; $E_{2,k}$ – элемент, реализующий функцию $f_{2,k}$ и имеющий равный sk вес (s – число аргументов функции $f_{2,k}$). Нетрудно проверить, что базис B_1 является нормированным.

Поскольку для доказательства полноты базиса B_1 сложности схем не имеют значения, используем упрощенный вариант предложенного автором [4] *принципа глобального компактного кодирования*: таблице, задающей произвольную функцию $f \in P_k^n$, сопоставим таблицу, задающую систему $]\log_2 k[$ булевых функций от rn переменных, следующим образом.

Символу i, $0 \le i \le k-1$, набора значений переменных функции f сопоставим булев набор (длины r), являющийся i-м столбцом матрицы, соответствующей $(k,2)$-достаточной системе Φ_1^2. В таблице, задающей произвольную функцию $f \in P_k^n$, символ i, $0 \le i \le k-1$, набора значений переменных заменим его кодом (булевым набором). Символ i, $0 \le i \le k-1$, значения функции заменим булевым набором длины $]\log_2 k[$, являющимся двоичной записью числа i. В случае необходимости ($r \ne \log_2 k$) к полученной таким образом таблице добавим неиспользованные булевы наборы длины nr. На этих наборах значения функции дополним нулями. Эта (новая) таблица задает систему G_f^0 (всюду определенных) $]\log_2 k[$ булевых функций от nr переменных.

Имеющая n входов и m выходов схема называется (n,m)-схемой или (n,m)-блоком.

Опишем схему S_f^0 в базисе B_1, реализующую произвольную функцию $f \in P_k^n$.

Пусть $K20$ – $(1,r)$-блок, состоящий из элементов $E_1^2, E_2^2, ..., E_r^2$, входы которых присоединены к его входу; выходами блока являются выходы его элементов. Пусть $K20N$ – (n,rn)-блок, состоящий из n блоков $K20$. Входами блока $K20N$ являются входы блоков $K20$. Выходами блока $K20N$ являются выходы блоков $K20$.

Пусть S_f^b – $(nr,]\log_2 k[)$-схема, состоящая из элементов E_1 и реализующая систему G_f^0.

Пусть $2K0$ – (q,s)-блок, состоящий из элементов E_1 и реализующий систему функций. Выходной набор этой функции на булевом наборе, являющемся записью числа i, $0 \le i \le k-1$, будет набор, на котором функция $f_{2,k}$ принимает значение i.

Схема S_f^0 имеет n входов, один выход и состоит из блока $K20N$, схемы S_f^b, блока $2K0$ и элемента $E_{2,k}$. Входы блока $K20N$ присоединены к входам схемы. Входы схемы S_f^b присоединены к выходам блока $K20N$. Входы блока $2K0$ присоединены к выходам схемы S_f^b. Входы элемента $E_{2,k}$ присоединены к выходам блока $2K0$. Выходом схемы S_f^0 является выход элемента $E_{2,k}$.

Нетрудно проверить, что схема S_f^0 является схемой в базисе B_1 и реализует (произвольную) функцию $f \in P_k^n$. Таким образом, доказано, что базис B_1 функционально полон в P_k.

Исследуем асимптотическое поведение функционала $L^{B_1}(k,n)$.

Вначале рассмотрим случай, когда k является степенью 2, т. е. $q = \log_2 k =]\log_2 k[$.

Пусть $C1$ – $(r,]\log_2 k[)$-блок, состоящий из элементов E_1 и реализующий систему функций, выходной набор которой на входном наборе, являющемся выходным набором элемента $K20$ при равном i, $0 \le i \le k-1$, значении входа последнего, является двоичной записью числа i.

Пусть $K2N$ – $(1,q)$-блок, состоящий из блока $K20$ и блока $C1$. Входы блока $C1$ присоединены к выходам блока $K20$. Входом блока $K2N$ является вход блока $K20$, а выходами блока $K2N$ – выходы блока $C1$.

Отметим, что при равном i, $0 \le i \le k-1$, значении входа блока $K2N$ набор значений его выходов является двоичной записью числа i.

Пусть $K2NN$ – (n,qn)-блок, состоящий из n блоков $K2N$. Входами (выходами) блока $K2NN$ являются входы (выходы) блоков $K2N$. Нетрудно проверить, что последовательностью значений выходов блока $K2NN$ является двоичная запись числа, k-ичной записью которого является набор значений его входов. Пусть $2KN$ – $(q,1)$-блок, состоящий из (q,s)-блока $2KO$ и элемента $E_{2,k}$. Входы элемента $E_{2,k}$ присоединены к выходам блока $2KO$. Выходом блока

$2KN$ является выход элемента $E_{2,k}$. Отметим, что блок $2KN$ на булевых наборах выдает значение, равное числу, двоичной записью которого является набор значений его входов.

Воспользуемся принципом глобального компактного кодирования: символу i, $0 \le i \le k-1$, сопоставим булев набор, являющийся двоичной записью числа i (код символа). В таблице, задающей произвольную функцию $f \in P_k^n$, символы i, $0 \le i \le k-1$, заменим их кодами. Полученная таким образом таблица истинности задает систему G_f (всюду определенных) q булевых функций от nq переменных.

Пусть GB – (qn, q)-схема, реализующая систему G_f.

Пусть SFN – схема, состоящая из блока $K2NN$, схемы GB и блока $2KN$. Соединение элементов схемы SFN представлено на рис. 1.

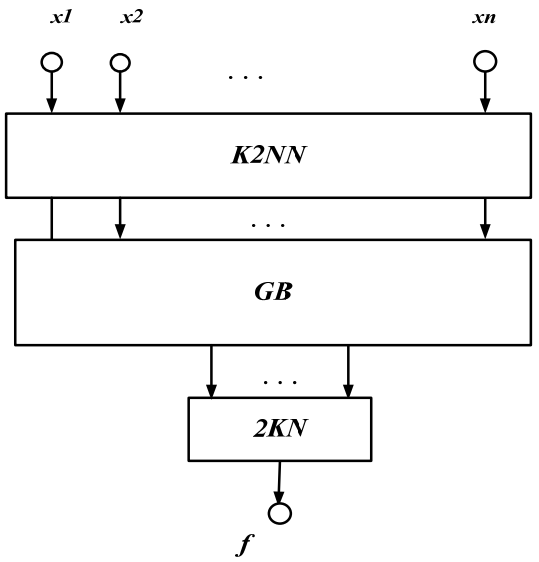

Рис. 1. Схема *SFN*

Нетрудно проверить, что схема SFN реализует функцию f.

Очевидно, что

$$L(SFN) = L(K2NN) + L(GB) + L(2KN).$$

Далее c_j означены константы.

Оценка $L(K2N) \le c_1$ очевидна (напомним, что значность логики (число k) считается величиной постоянной). Отсюда получаем оценку $L(K2NN) \le c_1 n$. Оценка $L(2KN) \le c_2$ также очевидна.

Из теоремы 1 получаем оценку

$$L(GB) \le\sim \frac{k^n}{n}.$$

Таким образом, справедливо следующее утверждение.

Теорема 2. *Если k является степенью двойки, то*

$$L^{B_1}(k,n) \sim \frac{k^n}{n}.$$

Случай, когда q не является целым числом, более сложный ввиду не тривиальности перевода в этом случае записи чисел в k-значной системе счисления в их запись в двоичной системе счисления.

Через K_2N обозначим $(n,]qn[)$-блок такой, что последовательностью значений его выходов является двоичная запись числа, k-ичной записью которого является последовательность значений его входов. Блок K_2N строим следующим образом.

Через $T_j, 1 \le j \le n,$ обозначим $(1,]qn[)$-блок такой, что последовательностью значений его выходов является двоичная запись числа ik^{j-1}, где $i,\ 0 \le i \le k-1,$ – значение входа этого блока.

Пусть $SUMN$ – $(2]qn[,]qn[)$-блок, состоящий из элементов $E1$ и являющийся $]qn[$-разрядным параллельным двоичным сумматором последовательного действия. Известно, что $L(SUMN) \le c_3]qn[$.

Схема блока K_2N представлена на рис. 2.

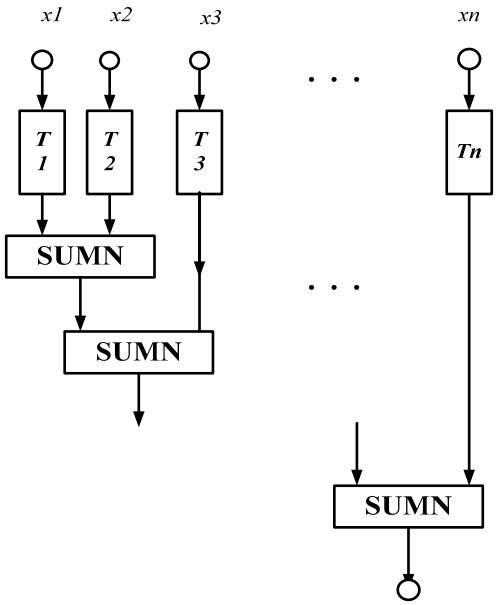

Рис. 2. Блок *K_2N*

Опишем блоки $T_j, 1 \le j \le n$. Пусть $M_j, 1 \le j \le n$, – $(k,]qn[)$-матрица, у которой i-я строка, $0 \le i \le k-1$, является двоичной записью числа ik^{j-1}. Пусть теперь $f_t^j, 0 \le t \le]qn[-1$, – функция от одного аргумента, вектором задания которой является t-й столбец матрицы $M_j, 1 \le j \le n$. Блок $T_j, 1 \le j \le n$, состоит из $]qn[$ (1, 1)-блоков, реализующих функции f_t^j.

Входы этих блоков присоединены к входу блока T_j. Нетрудно проверить справедливость оценки $L(T_j) \le c_4]qn[$.

Таким образом, получена следующая оценка

$$L(K\_2N) \le c_5 n^2.$$

Пусть 2_K – $(]q[,1)$-блок, который на булевых наборах выдает значение, равное числу, двоичной записью которого является набор значений его входов. Очевидна оценка $L(2\_K) \le c_6$.

Пусть BFN – $(]qn[,]q[)$-схема, реализующая систему $]q[$ булевых функций от $]qn[$ переменных, аналогичную системе G_f. На наборах значений входов схемы BFN, являющихся двоичной записью чисел больше или равных k^n, значения ее выходов полагаем равным 0.

Из работы [3] следует оценка

$$L(BFN) \le\sim]\log k[\frac{k^n}{n\log k} = \frac{]\log k[}{\log k}\frac{k^n}{n}.$$

Таким образом, справедливо следующее утверждение.

Теорема 3.

$$L^{B_1}(k,n) \le\sim \frac{]\log k[}{\log k}\frac{k^n}{n}.$$

Замечание. Разлагая (по аналогии с [6]) функцию f по переменным, можно получить оценку $L^{B_1}(k,n) \sim \frac{k^n}{n}$ при любых k.

Таким образом, предложено семейство *k*-значных базисов и показана их полнота. Для этих базисов построены методы синтеза схем из функциональных элементов, обеспечивающие асимптотически

наилучшие оценки функционалов $L^B(k,n)$. Полученные результаты могут быть использованы, например, при построении аппаратных средств защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Яблонский С. В. Функциональные построения в k-значной логике // Труды Матем. ин-та им. В.А. Стеклова LI, 1958. С. 5 – 142.
2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Сб. «Проблемы кибернетики». – М.: Физматгиз, 1963. – Вып. 10. – С. 3–97.
3. Лупанов О. Б. Об одном подходе к синтезу управляющих систем – принципе локального кодирования // Сб. «Проблемы кибернетики». – М.: Физматгиз, 1965. – Вып. 14. – С. 31–110.
4. Орлов В. А. О реализации функций из P_k схемами в произвольном базисе // Тез. докл. XI Международной конференции «Проблемы теоретической кибернетики». – Ульяновск: Изд-во РГГУ, 1996. – С. 154–155.
5. Орлов В. А. Реализация функций из P_k схемами в произвольном базисе из функциональных элементов // Доклады РАН. – 1998. – Т. 359. №. 3. – С. 308–309.
6. Орлов В. А. О реализации *k*-значных функций схемами из функциональных элементов // Математические заметки. – 1998. – Т. 64. – Вып. 3. – С. 431–436.
7. Захарова Е. Ю. Реализация функций из P_k формулами $k \geq 3$ // Математические заметки. – 1972. – Т. 11. – Вып. 1. – С. 99–108.

Статья поступила в редакцию 14.05.2012