

## САМОКОРРЕКТИРУЮЩИЕСЯ СХЕМЫ, РЕАЛИЗУЮЩИЕ «УЗКИЕ» СИСТЕМЫ ЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ\*)

*А. В. Чашкин*

Приведены конструкции самокорректирующихся схем, реализующих «узкие» системы линейных булевых функций и исправляющих любое конечное число произвольных неисправностей. Доказана асимптотическая минимальность построенных схем.

### § 1. Постановка задачи. Формулировка результата

В настоящей работе представлены самокорректирующиеся схемы, реализующие «узкие» системы линейных булевых функций и исправляющие любое фиксированное число произвольных ошибок. Как обычно, базис самокорректирующихся схем состоит из элементов двух видов: надежных и ненадежных. Каждый надежный элемент всегда реализует одну и ту же приписанную ему булеву функцию. Любой ненадежный элемент может находиться в одном из двух состояний: либо в исправном, либо в неисправном. В исправном состоянии ненадежный элемент реализует приписанную этому элементу булеву функцию, в неисправном состоянии — произвольную булеву функцию, зависящую от переменных, подаваемых на его входы. В рассматриваемых схемах как надежная, так и ненадежная часть базиса содержит элементы, реализующие все двухместные булевы функции. Будем полагать, что вес каждого ненадежного элемента равен единице, а вес каждого надежного элемента — некоторой положительной постоянной  $w$ . Сложностью  $L(S)$  схемы  $S$  называется сумма весов элементов, составляющих схему. Сложностью  $L_t(F)$  системы булевых функций  $F$  называется сложность минимальной схемы, реализующей  $F$  и корректирующей не менее  $t$  ошибок. Положим

$$L_t(m, n) = \max L_t(F),$$

---

\*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-01068) и Федеральной целевой программы «Интеграция» (код проекта 473).

где максимум берется по всем системам, состоящим из  $m$  линейных булевых функций, зависящих от  $n$  переменных и имеющих нулевой свободный член. Далее такие системы будем называть линейными  $(m, n)$ -системами. Полагаем, что  $n$  — число аргументов всех рассматриваемых ниже функций — больше некоторой постоянной. Все общеупотребительные понятия, используемые ниже без определений, можно найти в [2].

**Теорема 1.** Пусть  $t \geq 1$  — произвольное целое,  $w \geq \frac{2}{3}(2t+1)$  — постоянная,  $m \geq \log_2 n$ ,  $\lceil \frac{m}{2t+1} \rceil (t+1) \leq (1-\varepsilon) \log_2 n$ , где  $\varepsilon$  — произвольное положительное число. Тогда при  $n \rightarrow \infty$

$$L_t(m, n) \sim (2t+1)n.$$

## § 2. Доказательство верхней оценки

Опишем конструкцию схемы требуемой сложности.

Пусть  $F = \{f_i = \bigoplus_{j=1}^n f_{ij} x_j\}_{i=1}^m$  — произвольная система  $m$  линейных булевых функций  $f_i$ , а  $\tilde{F} = (f_{ij})$  — матрица этой системы.

Из функций системы  $F$  составим  $2t+1$  новых систем  $I_p$ ,  $p = 1, 2, \dots, 2t+1$ , каждая из которых содержит не более  $\lceil \frac{m}{2t+1} \rceil$  функций и задается следующим образом:

$$f_i \in I_p \iff (p-1) \left\lceil \frac{m}{2t+1} \right\rceil < i \leq \min \left( p \left\lceil \frac{m}{2t+1} \right\rceil, m \right).$$

Из систем  $I_p$  составим  $2t+1$  новых систем  $J'_q$ ,  $q = 1, 2, \dots, 2t+1$ , каждая из которых содержит не более  $\lceil \frac{m}{2t+1} \rceil (t+1)$  функций и задается следующим образом:

$$I_p \subset J'_q \iff 0 \leq (p-q) \bmod (2t+1) < t+1.$$

Каждую систему  $J'_q$  дополним функцией  $\bigoplus_{i=1}^n x_i$ . Расширенную систему обозначим через  $J_q$ .

Идея построения требуемой схемы  $S$  состоит в следующем. Схема  $S$  содержит подсхемы  $S_1, \dots, S_{2t+1}$ , где подсхема  $S_q$  реализует систему линейных функций  $J_q$ . Системы  $J_q$  определены так, что каждая функция  $f_i$  из  $F$  содержится в  $t+1$  системах  $J_q$ . Все ненадежные элементы схемы  $S$  реализуют функцию сложения и содержатся в подсхемах  $S_1, \dots, S_{2t+1}$ . Так как каждая система  $J_q$  содержит функцию  $\bigoplus_{i=1}^n x_i$ , то в схеме  $S$  эта функция вычисляется  $2t+1$  раз. Если  $S$  содержит не более  $t$  неисправных элементов, то, используя функцию голосования, вычисленную при помощи надежных элементов, можно определить истинное значение функции  $\bigoplus_{i=1}^n x_i$ . Далее, все подсхемы  $S_1, \dots, S_{2t+1}$  устроены так, что, сравнивая значение  $\bigoplus_{i=1}^n x_i$ , вычисленное любой подсхемой  $S_q$ , с истинным значением функции  $\bigoplus_{i=1}^n x_i$ , можно определить четность числа

неисправных элементов в  $S_q$ . Пусть  $d_1(d_2)$  — число подсхем, содержащих нечетное (четное) число неисправных элементов. Если в схеме  $S$  содержится не более  $t$  неисправных элементов, то

$$d_1 + 2d_2 \leq t \quad \text{или} \quad (t+1) - d_1 > 2d_2.$$

Следовательно, при каждом  $i$ ,  $1 \leq i \leq m$ , среди подсхем  $S_q$ , реализующих функцию  $f_i$  и содержащих четное (в том числе нулевое) число неисправных элементов, более половины подсхем состоят только из исправных элементов и вычисляют значение  $f_i$  правильно. Таким образом, рассматривая только подсхемы с четным числом неисправных элементов, можно определить истинные значения всех функций исходной системы  $F$ .

Рассмотрим строение и сложность подсхем, составляющих требуемую схему  $S$ .

1. Опишем обычные (несамокорректирующиеся) схемы, реализующие  $(k, n)$ -системы при условии, что  $k \leq (1 - \varepsilon) \log_2 n$ , где  $\varepsilon$  — положительная константа.

Пусть  $U_k$  — такая  $(k, 2^k - 1)$ -система линейных функций, что  $j$ -й столбец матрицы  $\tilde{U}_k$  совпадает с двоичным разложением числа  $j$ . Известны схемы [1], которые реализуют  $U_k$ , состоят только из элементов сложения и имеют сложность не более  $2^{k+1}$ . Пусть  $A_k$  — одна из таких схем.

Пусть  $M$  — произвольная  $(k, n)$ -система линейных булевых функций, где  $k \leq (1 - \varepsilon) \log_2 n$ . Из условия  $k \leq (1 - \varepsilon) \log_2 n$  следует, что матрица  $\tilde{M}$  содержит не более  $n^{1-\varepsilon}$  различных столбцов. Множество переменных  $\{x_i\}_{i=1}^n$  разобьем на классы эквивалентности так, что переменная  $x_s$  принадлежит классу  $R_i$  в том случае, если  $s$ -й столбец матрицы  $\tilde{M}$  совпадает с двоичным разложением числа  $i$ . Схема  $B$ , реализующая систему  $M$ , состоит из подсхем  $B_i$ ,  $0 \leq i \leq n^{1-\varepsilon}$ , и устроена следующим образом. При каждом  $i > 0$  подсхема  $B_i$  суммирует все  $x_s$ , принадлежащие классу  $R_i$ . Подсхема  $B_0$  является экземпляром схемы  $A_k$ , и ее  $i$ -й вход присоединен к выходу подсхемы  $B_i$ . Легко видеть, что

$$L(B_0) \leq 2n^{1-\varepsilon}, \quad L\left(\bigcup_{i>0} B_i\right) \leq n, \quad L(B) \leq n(1 + o(1)).$$

2. Так как  $\lceil \frac{m}{2t+1} \rceil (t+1) \leq (1 - \varepsilon) \log_2 n$ , то для построения подсхемы  $S_q$ , реализующей систему линейных функций  $J_q$ , используем конструкцию из предыдущего пункта. Подсхемы  $S_{qi}$ , соответствующие подсхемам  $B_i$  при  $i > 0$ , составим из ненадежных элементов, а подсхему  $S_{q0}$ , соответствующую подсхеме  $B_0$ , составим из надежных элементов.

Очевидно, что

$$L(S_q) = L(S_{q0}) + L\left(\bigcup_{i>0} S_{qi}\right) \leq n + cwn^{1-\epsilon},$$

где  $c$  — некоторая константа. Нетрудно убедиться в том, что если в подсхеме  $S_q$  содержится нечетное число неисправных элементов, то значение функции  $\bigoplus_{i=1}^n x_i$  вычисляется неверно, а если в  $S_q$  содержится четное число неисправных элементов, то значение  $\bigoplus_{i=1}^n x_i$  вычисляется верно.

3. Подсхема  $S_m$ , вычисляющая истинное значение функции  $\bigoplus_{i=1}^n x_i$ , реализует функцию голосования, состоит из надежных элементов, а к ее входам присоединены выходы подсхем  $S_q$ , на которых вычисляются значения функции  $\bigoplus_{i=1}^n x_i$ . Очевидно, что

$$L(S_m) = c_1 w(2t + 1),$$

где  $c_1$  — некоторая константа.

4. Подсхема  $S_c$  определяет подсхемы  $S_q$  с нечетным числом неисправных элементов. Для этого вычисляются эквивалентности ( $\sim$ ) истинного значения функции  $\bigoplus_{i=1}^n x_i$  и значения этой функции, вычисленные подсхемами  $S_q$ ,  $q = 1, 2, \dots$ . Подсхема  $S_c$  состоит из надежных элементов, имеет  $2t + 2$  входов и  $2t + 1$  выход. Очевидно, что

$$L(S_c) = w(2t + 1).$$

5. Подсхема  $S_N$  для каждой функции  $f_i$ ,  $i = 1, 2, \dots, m$ , вычисляет число  $z'_i$ , равное числу подсхем  $S_q$ , реализующих  $f_i$  и содержащих четное (в том числе и нулевое) число неисправных элементов. Эта подсхема имеет  $2t + 1$  вход (они подключены к выходам подсхемы  $S_c$ ),  $m \lceil \log_2(t + 1) \rceil$  выход и состоит из надежных элементов. Легко видеть, что

$$L(S_N) = c_2 w m(t + 1),$$

где  $c_2$  — некоторая константа.

6. Подсхема  $S_{f_i}$  вычисляет значение функции  $f_i$ . Эта подсхема имеет  $t + 1 + \lceil \log_2(t + 1) \rceil + 1$  вход, один выход и состоит из надежных элементов. Первые входы подсхемы  $S_{f_i}$  присоединены к тем выходам подсхем  $S_q$ , на которых вычисляются значения функции  $f_i$ . Число таких подсхем  $S_q$  равно  $t + 1$ . Следующие  $\lceil \log_2(t + 1) \rceil$  входы подсхемы  $S_{f_i}$  присоединены к выходам подсхемы  $S_N$  (на них вычисляется число подсхем  $S_q$ , реализующих функцию  $f_i$  и содержащих четное (в том числе и нулевое) число неисправных элементов) и выход подсхемы  $S_c$ , на котором вычислена соответствующая эквивалентность. Подсхема  $S_{f_i}$  суммирует значения, поступающие на ее первые  $t + 1$  входы, предварительно обнулив те из них, что были вычислены подсхемами  $S_q$  с нечетным числом неисправных элементов. Далее полученная сумма  $z_i$  сравнивается

со значением  $s'_i$ , вычисленным подсхемой  $S_N$ . Если  $s_i \geq s'_i/2$ , то  $f_i = 1$ , в противном случае  $f_i = 0$ . Легко видеть, что

$$L(S_{f_i}) = c_3 w(t+1),$$

где  $c_3$  — некоторая константа.

7. Очевидно, что схема  $S$  состоит из  $2t+1$  подсхем  $S_q$ , одной подсхемы  $S_m$ , одной подсхемы  $S_c$ , одной подсхемы  $S_N$  и  $m$  подсхем  $S_{f_i}$ . Поэтому

$$\begin{aligned} L(S) &= (2t+1)L(S_q) + L(S_m) + L(S_c) + L(S_N) + mL(S_{f_i}) \\ &\leq (2t+1)(n + cwn^{1-\epsilon}) + c_1 w(2t+1) + w(2t+1) + c_2 wm(2t+1) + mc_3 w(t+1) \\ &\leq (2t+1)n(1 + o(1)). \end{aligned}$$

Верхняя оценка доказана.

### § 3. Доказательство нижней оценки

Далее, говоря о том, что элемент  $u$  реализует функцию  $f$ , под  $f$  будем понимать функцию, приписанную этому элементу, т. е. функцию, аргументами которой являются величины, подаваемые на входы  $u$ , а говоря о том, что элемент  $u$  вычисляет функцию  $f$ , под  $f$  будем понимать функцию, аргументами которой являются величины, подаваемые на входы схемы. Доказывая нижнюю оценку, будем использовать операцию удаления элемента, на вход которого подается константа. Прежде чем ввести эту операцию, определим две вспомогательные операции:

(а) операцию удаления одноходового элемента, выход которого не является выходом схемы;

(б) операцию удаления одноходового элемента, выход которого является выходом схемы.

Под операцией (а) понимаем следующее. Пусть на вход одноходового элемента  $u$  подается величина  $z$  (либо входной полюс схемы, либо выход некоторого элемента схемы), элемент  $u$  реализует функцию  $g$ , выход элемента  $u$  присоединен к первому входу элемента  $v$ , элемент  $v$  реализует функцию  $g_1$ . На первый вход элемента  $v$  подадим  $z$ , функцию  $g_1$  заменим функцией  $g'_1$  такой, что  $g'_1(z, y) = g_1(g(z), y)$ . Подобную операцию сделаем со всеми элементами, входы которых присоединены к выходу элемента  $u$ . Удалим элемент  $u$ .

Легко видеть, что после выполнения операции (а) преобразованная схема реализует ту же систему функций и корректирует такое же число ошибок, что и исходная схема, т. е. функционирование схемы после такого преобразования не изменится.

Под операцией (б) понимаем следующее. Рассмотрим три случая.

1. Пусть одноходовый элемент  $u$  реализует функцию  $g$ , на его вход подается выход элемента  $v$ , этот выход не является выходом схемы, элемент  $v$  реализует функцию  $g_1$ , выход  $v$  присоединен к первому входу элемента  $w$ , элемент  $w$  реализует функцию  $g_2$ . К элементу  $u$  применим операцию (а). Функцию  $g_1$  заменим функцией  $g'_1$  такой, что  $g'_1(z, y) = g(g_1(z, y))$ , а функцию  $g_2$  — функцией  $g'_2$  такой, что  $g'_2(g(g_1(z, y)), x) = g_2(g_1(z, y), x)$ . Вторую замену сделаем со всеми элементами, к входам которых присоединен выход элемента  $v$ . Выход элемента  $v$  объявим выходом схемы.

2. Пусть одноходовый элемент  $u$  реализует функцию  $g$ , на его вход подается выход элемента  $v$ , этот выход является выходом схемы. Так как рассматриваемые схемы реализуют линейные функции с нулевым свободным членом, то очевидно, что  $g$  является тождественной функцией. Поэтому элементы  $u$  и  $v$  вычисляют одну и ту же функцию  $f_j$ . Удалим элемент  $u$ .

3. Пусть одноходовый элемент  $u$  реализует функцию  $g$  и его вход подключен к входному полюсу  $x_j$ . Как и в предыдущем случае, видим, что  $g$  — тождественная функция. Поэтому удаляем элемент  $u$ , а полюс  $x_j$  объявляем выходом схемы. Легко видеть, что функционирование схемы после преобразования (b) не изменится.

Теперь можно легко определить операцию удаления двухходового элемента, на вход которого подается константа. Пусть на первый вход элемента  $u$  подается константа  $\alpha$ , элемент  $u$  реализует функцию  $g$ . Функцию  $g$  заменим функцией  $g'$  такой, что  $g'(y) = g(\alpha, y)$ . После этого удалим элемент  $u$  при помощи либо операции (а), либо операции (b). Очевидно, что после такого преобразования функционирование схемы не изменится, а сложность уменьшится не менее чем на величину веса элемента  $u$ .

Для доказательства нижней оценки покажем, что сложность любой схемы  $S$ , корректирующей  $t$  неисправностей и реализующей линейную  $(m, n)$ -систему  $F$ , матрица которой состоит из попарно различных ненулевых столбцов, удовлетворяет неравенству  $L(S) \geq (2t + 1)(n - m)$ , т. е.

$$L_i(F) \geq (2t + 1)(n - m). \quad (1)$$

Неравенство (1) докажем индукцией по  $n$ . В основание индукции положим очевидный случай  $n = m$ , а также схемы специального вида, в которых каждый входной полюс (далее для краткости называемый входом) присоединен к нескольким ненадежным элементам и ровно к одному надежному элементу, причем разные входы схемы присоединены к разным надежным элементам. Справедливость неравенства (1) для таких схем будет установлена в конце данного доказательства.

Предположим, что неравенство (1) верно при  $n \leq k$ . Покажем, что оно верно и при  $n = k + 1$ . Пусть схема  $S$  реализует линейную  $(m, k + 1)$ -систему. Возможны следующие случаи:

1. Существует входной полюс  $x_i$ , присоединенный не менее чем к двум надежным элементам.

2. Существует входной полюс  $x_i$ , присоединенный только к ненадежным элементам.

3. Каждый входной полюс присоединен к одному надежному и нескольким ненадежным элементам.

В первом случае на  $i$ -й вход схемы  $S$  вместо переменной  $x_i$  подадим тождественный нуль. Тогда в схеме можно удалить не менее двух двух-входовых надежных элементов. Новая схема  $S'$  реализует некоторую линейную  $(m', k)$ -систему  $F'$ , матрица которой состоит из попарно различных ненулевых столбцов. По предположению индукции справедливо неравенство  $L_i(F') \geq (2t + 1)(k - m')$ . Так как  $m \geq m'$ , то

$$\begin{aligned} L_i(F) &\geq (2t + 1)(k - m') + 2w \geq (2t + 1)(k - m') + \frac{4}{3}(2t + 1) \\ &> (2t + 1)(k + 1 - m') \geq (2t + 1)(k + 1 - m). \end{aligned}$$

Во втором случае сначала покажем, что число ненадежных элементов, к которым присоединен полюс  $x_i$ , не меньше  $2t + 1$ . Предположим, что это не так и число таких ненадежных элементов в схеме равно  $2t$ . Эти элементы обозначим через  $u_1, \dots, u_{2t}$ . Без ограничения общности будем считать, что значение элемента  $u_{i-1}$  не зависит от значения элемента  $u_i$ , т. е. не существует ориентированной цепи, связывающей выход элемента  $u_i$  с одним из входов элемента  $u_{i-1}$ . Положим

$$x_1 = \dots = x_{i-1} = x_{i+1} = \dots = x_{k+1} = 0, \quad x_i = x.$$

Рассматриваемую схему  $S$  преобразуем следующим образом. Последовательно будем удалять из схемы каждый такой элемент  $v$ , что  $v \notin \{u_1, \dots, u_{2t}\}$  и хотя бы на один из его входов подается константа. Преобразованная схема  $S'$  будет содержать элементы  $u_1, \dots, u_{2t}$ , а также некоторые другие элементы, зависящие от  $u_1, \dots, u_{2t}$ . Зависимость (не обязательно существенную) элементов  $u_1, \dots, u_{2t}$  друг от друга и от переменной  $x$  можно выразить так:

$$\begin{aligned} u_1 &= u_1(x), \\ u_2 &= u_2(x, u_1), \\ &\dots \dots \dots \\ u_{2t} &= u_{2t}(x, u_1, \dots, u_{2t-1}). \end{aligned}$$

Схема  $S'$  реализует новую систему линейных функций  $F'$  и корректирует  $t$  неисправностей. Очевидно, что среди функций системы  $F'$

найдется функция  $f(x) = x$ . Без ограничения общности такой функцией будем считать  $f_1$ . Легко видеть, что значение функции  $f_1$  определяется только значениями, вычисленными ненадежными элементами  $u_1, \dots, u_{2t}$ , т. е.  $f_1$  есть функция величин, вычисленных в элементах  $u_1, \dots, u_{2t}$ . Пусть  $R \in \{0, 1\}^{2t}$  — вектор, определяющий в каком состоянии находятся элементы  $u_1, \dots, u_{2t}$ . Если  $u_i$  находится в исправном состоянии, то  $R_i = 0$ , иначе  $R_i = 1$ . Через  $U(R, x) \in \{0, 1\}^{2t}$  обозначим вектор,  $i$ -я координата которого равна  $u_i(x)$  при условии, что состояния элементов  $u_1, \dots, u_{2t}$  определяются вектором  $R$ . При этом полагаем, что значение элемента в неисправном состоянии отличается от значения элемента в исправном состоянии. Покажем, что найдутся векторы  $R$  и  $R'$  такие, что  $U(R, 0) = U(R', 1)$  и в каждом из этих векторов содержится не более  $t$  единиц. Сделаем это индукцией по  $t$ . При  $t = 1$  утверждение очевидно. Предположим, что оно верно при  $t = d$ . Тогда из предположения индукции следует, что существуют такие векторы  $R$  и  $R'$  длины  $2d + 2$ , что каждый из этих векторов содержит не более  $d$  единиц,

$$R_{2d+1} = R_{2d+2} = R'_{2d+1} = R'_{2d+2} = 0$$

и первые  $2d$  координат векторов  $U(R, 0)$  и  $U(R', 1)$  совпадают. Переопределим предпоследнюю координату вектора  $R'$ : если  $(2d+1)$ -я координата вектора  $U(R, 0)$  не совпадает с такой же координатой вектора  $U(R', 1)$ , то положим  $R'_{2d+1} = 1$ ; в противном случае оставим  $R'_{2d+1} = 0$ . Если  $R'_{2d+1} = 1$ , то будем полагать, что значение элемента  $u_{2d+1}$  в неисправном состоянии отлично от его значения в исправном состоянии. Далее переопределим последнюю координату вектора  $R$ : если  $(2d+2)$ -я координата вектора  $U(R', 0)$  не совпадает с такой же координатой вектора  $U(R, 1)$ , то положим  $R_{2d+2} = 1$ ; в противном случае оставим  $R_{2d+2} = 0$ . Если  $R_{2d+2} = 1$ , то, как и ранее, полагаем, что значение элемента  $u_{2d+2}$  в неисправном состоянии отлично от его значения в исправном состоянии. Легко видеть, что в каждом из новых векторов  $R$  и  $R'$  содержится не более  $d+1$  единиц, и первые  $2d+2$  координат векторов  $U(R, 0)$  и  $U(R', 1)$  совпадают.

Таким образом, при  $x = 0$  и неисправностях, определяемых вектором  $R$ , с одной стороны, и при  $x = 1$  и неисправностях, определяемых вектором  $R'$ , с другой стороны, значения, вычисляемые в элементах  $u_1, \dots, u_{2t}$ , совпадают. Следовательно,  $f_1(0) = f_1(1)$ , что неверно, так как  $f_1(x) = x$ . Поэтому схема  $S'$  не будет корректировать  $t$  неисправностей. Следовательно, неверно предположение о том, что число ненадежных элементов, которые присоединены к полюсу  $x_i$ , меньше  $2t + 1$ .

Положим  $x_i = 0$ . Тогда из схемы  $S$  можно удалить не менее  $2t + 1$  ненадежных элементов. Новая схема  $S''$  реализует некоторую линейную



$(m', k)$ -систему  $F''$ , матрица которой состоит из попарно различных ненулевых столбцов. По предположению индукции справедливо неравенство  $L_i(F'') \geq (2t + 1)(k - m')$ . Так как  $m \geq m'$ , то

$$L_i(F) \geq L_i(F'') + 2t + 1 \geq (2t + 1)(k + 1 - m).$$

Рассмотрим третий случай. Предположим, что в минимальной схеме  $S$ , реализующей систему  $F$  и корректирующей  $t$  неисправностей, найдутся два входных полюса, присоединенных к входам одного и того же надежного элемента  $u$ . Без ограничения общности будем полагать, что это  $k$ -й и  $(k + 1)$ -й полюсы. Пусть надежный элемент  $u$  реализует нелинейную функцию. В этом случае каждый из рассматриваемых входных полюсов должен быть присоединен не менее чем к  $2t + 1$  ненадежным элементам. Предположим, что это не так и  $k$ -й полюс присоединен менее чем к  $2t + 1$  ненадежным элементам. Так как  $u$  реализует нелинейную функцию, то существует такое значение  $\alpha$  переменной  $x_{k+1}$ , что при  $x_{k+1} = \alpha$  выход элемента  $u$  не зависит от  $k$ -го полюса. В этом случае удалим элемент  $u$  и все такие ненадежные элементы, которые присоединены к  $(k + 1)$ -му полюсу и не присоединены к  $k$ -му полюсу. Новая схема  $S'$  реализует новую систему линейных функций  $F'$  и при этом должна корректировать  $t$  неисправностей. Легко видеть, что мы пришли к ситуации, рассмотренной ранее при разборе второго случая. Выше было показано, что такая ситуация невозможна. Поэтому разбор ситуации, когда  $u$  реализует нелинейную функцию, закончен.

Рассмотрим теперь случай, когда надежный элемент  $u$  реализует линейную функцию. Предположим, что  $k$ -й и  $(k + 1)$ -й полюсы присоединены в совокупности менее чем к  $2t + 1$  ненадежным элементам. Положим

$$x_1 = x_2 = \dots = x_{k-1} = 0, \quad x_k = x_{k+1} = x.$$

Так как система  $F$  несимметрична относительно  $x_k$  и  $x_{k+1}$ , что следует из попарной различности столбцов матрицы системы, то после выполнения подстановки среди функций новой системы  $F'$  найдется функция, равная  $f(x) = x$ . Без ограничения общности такой функцией будем считать  $f_1$ . Легко видеть, что на выходе элемента  $u$  вычисляется константа, не зависящая от  $x$ . Следовательно, значение функции  $f_1$  определяется только значениями, вычисленными ненадежными элементами, которые присоединены к  $k$ -му и  $(k + 1)$ -му полюсам. Вновь приходим к ситуации, рассмотренной выше при разборе второго случая. Следовательно, к  $k$ -му и  $(k + 1)$ -му полюсам присоединено в совокупности не менее чем  $2t + 1$  ненадежных элементов. Поэтому к одному из них, например к  $(k + 1)$ -му, присоединено не менее  $t + 1$  ненадежных элементов.

Положим  $x_{k+1} = 0$ . Тогда из схемы  $S$  можно удалить один надежный элемент и не менее  $t + 1$  ненадежных элементов. Новая схема  $S''$

реализует некоторую линейную  $(m', k)$ -систему  $F''$ , матрица которой состоит из попарно различных ненулевых столбцов. По предположению индукции справедливо неравенство  $L_i(F'') \geq (2t + 1)(k - m')$ . Так как  $m \geq m'$ , то

$$L_i(F) \geq L_i(F'') + t + 1 + w > (2t + 1)(k + 1 - m).$$

Перейдем к доказательству неравенства (1) для схем, каждый вход которых присоединен только к одному надежному элементу, причем разные входы присоединены к разным надежным элементам.

Пусть  $\tilde{S}$  — подсхема схемы  $S$ , состоящая только из надежных элементов  $S$ . Вершину  $u$  подсхемы  $\tilde{S}$  назовем *особой вершиной* схемы  $S$ , если выполняется хотя бы одно условие: (1) выходная степень вершины  $u$  в подсхеме  $\tilde{S}$  больше единицы; (2) выход элемента  $u$  является выходом схемы  $S$ .

Особую вершину  $u$  схемы  $S$  назовем *особой вершиной*  $i$ -го входа схемы  $S$ , если  $i$ -й вход и  $u$  связаны ориентированной цепью, проходящей только через надежные вершины (далее такие цепи называем *надежными*) и не проходящей через другие особые вершины.

Элемент  $u$  подсхемы  $\tilde{S}$  назовем *общим элементом*  $i$ -го и  $j$ -го входов схемы  $S$ , если в подсхеме  $\tilde{S}$  этот элемент связан с  $i$ -м и  $j$ -м входами цепями, ориентированными от входов к  $u$ . Эти цепи не проходят через особые вершины, отличные от элемента  $u$  (если  $u$  — особая вершина), и не имеют особых вершин, отличных от  $u$ .

Будем говорить, что  $i$ -й и  $j$ -й входы схемы  $S$  *соседние*, если в  $S$  имеется элемент  $u$ , являющийся общим элементом этих входов, и надежные цепи, связывающие эти входы с  $u$ , не проходят через общие элементы, отличные от  $u$ .

Легко видеть, что любой вход схемы  $S$  может иметь не более одного соседнего входа. Так же очевидно, что цепи, связывающие в  $\tilde{S}$  различные пары соседних входов, не пересекаются.

Вход схемы  $S$  назовем *изолированным*, если этот вход не имеет особой вершины и не имеет соседнего входа.

Очевидно, что каждый вход схемы  $S$  либо имеет собственную особую вершину, либо является изолированным, либо имеет один соседний вход.

Пусть  $k$ -й вход является изолированным. Пусть  $P$  — множество ненадежных элементов  $u_i$ , к которым присоединены  $k$ -й вход и выходы надежных элементов, связанных с этим входом надежными цепями, ориентированными от входа к  $u_i$ . Как и при разборе второго случая, легко показать, что  $|P| \geq 2t + 1$ .

Пусть  $k$ -й и  $(k + 1)$ -й входы являются соседними. Через  $u$  обозначим их общий элемент. Пусть  $P$  — множество ненадежных элементов,

к которым присоединены  $k$ -й и  $(k+1)$ -й входы и выходы надежных элементов, лежащих на ориентированных надежных цепях, соединяющих эти входы с элементом  $u$ . Покажем, что

$$|P| \geq 2t + 1.$$

Сделаем это методом от противного. Предположим, что  $|P| = 2t$ . Обозначим через  $u_1, \dots, u_{2t}$  ненадежные элементы из множества  $P$ . Без ограничения общности будем считать, что значение элемента  $u_{i-1}$  не зависит от значения элемента  $u_i$ . Положим

$$x_1 = \dots = x_{k-1} = 0, \quad x_k = x, \quad x_{k+1} = y.$$

Как и ранее, рассматриваемую схему  $S$  преобразуем следующим образом. Последовательно будем удалять из схемы каждый такой элемент  $v$ , что  $v \notin \{u_1, \dots, u_{2t}\}$  и хотя бы на один из его входов подается константа. Преобразованная схема  $S'$  будет содержать элементы  $u_1, \dots, u_{2t}$ , а также некоторые другие элементы, зависящие от  $u_1, \dots, u_{2t}$ . Схема  $S'$  реализует новую систему линейных функций  $F'$  и корректирует  $t$  неисправностей. Так как  $k$ -й и  $(k+1)$ -й столбцы матрицы  $F$  различны, то система  $F'$  содержит две различные функции. Без ограничения общности такими функциями будем считать  $f_1$  и  $f_2$ . Легко видеть, что значения этих функций определяются только значениями, вычисленными ненадежными элементами  $u_1, \dots, u_{2t}$  и надежным элементом  $u$ . Поэтому найдутся функции  $f'_1$  и  $f'_2$  такие, что

$$f'_1(u_1, \dots, u_{2t}, u(x, y)) = f_1(x, y), \quad f'_2(u_1, \dots, u_{2t}, u(x, y)) = f_2(x, y).$$

Пусть, как и ранее,  $R \in \{0, 1\}^{2t}$  — вектор, определяющий, в каком состоянии находятся элементы  $u_1, \dots, u_{2t}$ . Если  $u_i$  находится в исправном состоянии, то  $R_i = 0$ , иначе  $R_i = 1$ . Через  $U(R, x, y) \in \{0, 1\}^{2t}$  обозначим вектор,  $i$ -я координата которого равна  $u_i(x, y)$  при условии, что состояния элементов  $u_1, \dots, u_{2t}$  определяются вектором  $R$ . Как и при разборе второго случая, покажем, что найдутся векторы  $R$ ,  $R'$  и  $R''$  такие, что  $U(R, 0, 1) = U(R', 1, 0) = U(R'', 0, 0)$  и в каждом из этих векторов содержится не более  $t$  единиц. Сделаем это индукцией по  $t$ . При  $t = 1$  утверждение очевидно. Предположим, что оно верно при  $t = d$ . Тогда из предположения индукции следует, что существуют такие векторы  $R$ ,  $R'$  и  $R''$  длины  $2d+2$ , что в каждом из этих векторов содержится не более  $d$  единиц,

$$R_{2d+1} = R_{2d+2} = R'_{2d+1} = R'_{2d+2} = R''_{2d+1} = R''_{2d+2} = 0$$

и первые  $2d$  координат векторов  $U(R, 0, 1)$ ,  $U(R', 1, 0)$  и  $U(R'', 0, 0)$  совпадают. Не менее чем у двух из этих векторов совпадают также и предпоследние координаты. Без ограничения общности такими векторами

будем считать векторы  $U(R, 0, 1)$  и  $U(R', 1, 0)$ . Переопределим предпоследнюю координату вектора  $R''$ , положив  $R''_{2d+1} = 1$ . При этом полагаем, что значение элемента  $u_{2d+1}$  в неисправном состоянии отлично от его значения в исправном состоянии. Следовательно, после переопределения предпоследние координаты векторов  $U(R, 0, 1)$ ,  $U(R', 1, 0)$  и  $U(R'', 0, 0)$  совпадают. Очевидно, что не менее чем у двух из этих векторов совпадают также и последние координаты. Допустим, что одним из двух таких векторов является вектор  $U(R'', 0, 0)$  и  $U(R', 1, 0)_{2d+2} = U(R'', 0, 0)_{2d+2}$ . В этом случае изменим последнюю координату вектора  $R$ . Легко видеть, что после переопределения векторы  $U(R, 0, 1)$ ,  $U(R', 1, 0)$  и  $U(R'', 0, 0)$  полностью совпадают, а в каждом векторе  $R$ ,  $R'$  и  $R''$  содержится не более  $d + 1$  единиц. Если последняя координата вектора  $U(R'', 0, 0)$  отличается от последних координат двух других векторов, то изменим значения последних координат векторов  $R$  и  $R'$ . Снова видим, что векторы  $U(R, 0, 1)$ ,  $U(R', 1, 0)$  и  $U(R'', 0, 0)$  полностью совпадают, а в каждом из векторов  $R$ ,  $R'$  и  $R''$  содержится не более  $d + 1$  единиц.

Таким образом, при  $x = 0$ ,  $y = 1$  и неисправностях, определяемых вектором  $R$ , при  $x = 1$ ,  $y = 0$  и неисправностях, определяемых вектором  $R'$ , и при  $x = 0$ ,  $y = 0$  и неисправностях, определяемых вектором  $R''$ , значения, вычисляемые в элементах  $u_1, \dots, u_{2t}$ , совпадают. Введем обозначение ( $i = 1, 2$ ):

$$f'_i(u_1(x, y), \dots, u_{2t}(x, y), u(x, y)) = f'_i(U(R, x, y), u(x, y)).$$

Пусть значения элементов из  $P$  равны соответствующим координатам вектора  $U(R, 0, 1)$ .

Возможны два случая:

- (1)  $k$ -й и  $k + 1$ -й столбцы матрицы  $F$  несравнимы;
- (2) один из столбцов, например  $k + 1$ -й, больше второго.

Рассмотрим первый случай. Очевидно, что среди функций системы  $F'$  найдутся функции, равные  $x$  и  $y$ . Пусть  $f_1 = x$  и  $f_2 = y$ .

Пусть элемент  $u$  такой, что  $u(0, 1) = u(1, 0)$ . Тогда

$$0 = x(0, 1) = f'_1(U(R, 0, 1), u(0, 1)) = f'_1(U(R', 1, 0), u(1, 0)) = x(1, 0) = 1.$$

Противоречие.

Пусть элемент  $u$  такой, что  $u(0, 1) \neq u(1, 0)$ . Без ограничения общности будем считать, что  $u(1, 0) = u(0, 0)$ . Тогда

$$1 = x(1, 0) = f'_1(U(R', 1, 0), u(1, 0)) = f'_1(U(R'', 0, 0), u(0, 0)) = x(0, 0) = 0.$$

Противоречие.

Рассмотрим случай (2). Без ограничения общности будем считать, что  $f_1 = x$  и  $f_2 = x \oplus y$ .

Пусть элемент  $u$  такой, что  $u(0, 1) = u(1, 0)$ . Тогда

$$0 = x(0, 1) = f'_1(U(R, 0, 1), u(0, 1)) = f'_1(U(R', 1, 0), u(1, 0)) = x(1, 0) = 1.$$

Противоречие.

Пусть  $u(0, 1) \neq u(1, 0)$ . Если  $u(1, 0) = u(0, 0)$ , то

$$1 = x(1, 0) = f'_1(U(R', 1, 0), u(1, 0)) = f'_1(U(R'', 0, 0), u(0, 0)) = x(0, 0) = 0.$$

Противоречие. Если  $u(0, 1) = u(0, 0)$ , то

$$\begin{aligned} 1 &= (x \oplus y)(0, 1) = f'_2(U(R, 0, 1), u(0, 1)) \\ &= f'_2(U(R'', 0, 0), u(0, 0)) = (x \oplus y)(0, 0) = 0. \end{aligned}$$

Противоречие.

Таким образом, неравенство  $|P| \geq 2t + 1$  доказано.

Каждому входу схемы  $S$  поставим в соответствие входы элементов этой схемы. Сделаем это следующим образом.

(1) Если  $i$ -й вход имеет собственную особую вершину, отличную от выхода схемы, то этому входу поставим в соответствие вход надежного элемента, к которому присоединен  $i$ -й вход, а также входы двух надежных элементов, к которым присоединены выходы особой вершины.

(2) Если  $i$ -й вход является изолированным, то этому входу поставим в соответствие входы ненадежных элементов из множества  $P$ .

(3) Если  $i$ -й и  $j$ -й входы являются соседними, то этим входам поставим в соответствие входы надежных элементов, к которым присоединены  $i$ -й и  $j$ -й входы, входы их общего элемента, а также входы ненадежных элементов из соответствующего множества  $P$ . Так как общим элементов двух соседних входов может быть надежный элемент, к которому присоединен только один из этих входов, то каждой паре соседних входов ставится в соответствие не менее трех входов надежных элементов.

Пусть схема  $S$  содержит  $n$  входов,  $m$  выходов. Пусть среди входов  $S$  имеется  $k$  пар соседних входов,  $q$  входов, имеющих собственную особую вершину, отличную от выхода схемы, и  $p$  изолированных входов. Легко видеть, что

$$2k + q + p \geq n - m. \quad (2)$$

Каждому входу элемента схемы, поставленному в соответствие входу либо паре соседних входов схемы  $S$ , соответствует ребро схемы, выходящее либо из некоторого надежного элемента, либо из входа схемы. Пусть  $h_1$  — число надежных элементов схемы  $S$ ,  $h_2$  — число ненадежных элементов  $S$ . Тогда, учитывая, что из каждого ненадежного элемента

схемы выходит хотя бы одно ребро, для  $N$  — общего числа выходящих ребер — имеем неравенство

$$N \geq k(2t + 1 + 3) + 3q + p(2t + 1) + h_2.$$

Здесь первое слагаемое в правой части — число входов элементов, поставленных в соответствие парам соседних входов схемы; второе слагаемое — число входов элементов, поставленных в соответствие входам схемы, имеющих собственную особую вершину; третье слагаемое — число входов элементов, поставленных в соответствие изолированным входам схемы; четвертое слагаемое — число ребер, выходящих из ненадежных элементов схемы. В каждый элемент схемы  $S$  входит два ребра. Поэтому

$$2h_1 + 2h_2 = N \geq k(2t + 1 + 3) + 3q + p(2t + 1) + h_2,$$

или

$$2h_1 + h_2 \geq k(2t + 1) + 3(k + q) + p(2t + 1). \quad (3)$$

Так как различным входам схемы поставлено в соответствие  $3(k + q)$  входов надежных элементов, то очевидно, что

$$2h_1 \geq 3(k + q). \quad (4)$$

Поэтому из (2), (3), (4) и условий теоремы имеем

$$\begin{aligned} L(S) &= wh_1 + h_2 = (w - 2)h_1 + 2h_1 + h_2 \\ &\geq (w - 2)\frac{3}{2}(k + q) + k(2t + 1) + p(2t + 1) + 3(k + q) \\ &= \frac{3}{2}w(k + q) - 3(k + q) + k(2t + 1) + p(2t + 1) + 3(k + q) \\ &\geq \frac{3}{2}(k + q)\frac{2}{3}(2t + 1) + k(2t + 1) + p(2t + 1) = (2t + 1)(n - m). \end{aligned}$$

Теорема доказана.

### Заключение

Из доказательства теоремы легко следует, что для любой линейной  $(m, n)$ -системы  $F$  такой, что  $\lceil \frac{m}{2t+1} \rceil(t + 1) \leq (1 - \varepsilon) \log_2 n$  и матрица  $\tilde{F}$  состоит из попарно различных столбцов, справедливо равенство

$$L_t(F) \sim (2t + 1)n. \quad (5)$$

Асимптотически точная формула для сложности схем, корректирующих постоянное число однотипных константных неисправностей и реализующих конкретную последовательность функций, была найдена в [3].

Сравним схемы, построенные при доказательстве верхней оценки, с тривиальными схемами, вычисляющими при помощи ненадежных элементов  $2t + 1$  раз значение каждой функции  $f_i$  и использующими далее функции голосования. Известно [6], что схема, реализующая линейную  $(m, n)$ -систему, матрица которой состоит из попарно различных ненулевых столбцов, содержит не менее  $2(n - m)$  элементов. Поэтому, так как в нашем случае  $m = o(n)$ , сложность любой тривиальной схемы асимптотически не менее  $2n(2t + 1)$ , т. е. в два раза больше сложности построенных выше схем.

Рассмотрим линейные системы, вычисляющие синдром кода Хэмминга. Известно [1, 6], что сложность таких систем асимптотически равна  $2n$ . Следовательно, корректирование  $t$  неисправностей при вычислении синдрома кода Хэмминга приводит к увеличению сложности примерно в  $(2t + 1)/2$  раз. Ранее эффект увеличения сложности для схем, корректирующих неисправности, был установлен в [3, 4].

Наконец, отметим следующий любопытный факт. При  $w \geq 2t + 1$  индукцией по числу переменных легко показать, что сложность минимальной схемы, реализующей линейную функцию от  $2^n - 1$  переменных и корректирующей  $t$  неисправностей, асимптотически не меньше  $(2t + 1)2^n$ . Такая же верхняя оценка следует из (5). Следовательно, для линейной системы, вычисляющей синдром кода Хэмминга длины  $2^n - 1$ , и линейной функции  $2^n - 1$  аргументов сложности соответствующих минимальных схем, корректирующих конечное число неисправностей, асимптотически равны, а сложности обычных схем отличаются в два раза.

Автор благодарен профессору Н. П. Редькину, прочитавшему первоначальный вариант статьи и сделавшему ряд полезных замечаний.

## ЛИТЕРАТУРА

1. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности: Сб. науч. тр. Новосибирск: Ин-т математики СО РАН, 1992. Вып. 52. С. 22–40.
2. Редькин Н. П. Надежность и диагностика схем. М.: Изд-во Моск. ун-та, 1992.
3. Редькин Н. П. Асимптотически минимальные самокорректирующиеся схемы для одной последовательности булевых функций // Дискрет. анализ и исслед. операций. 1996. Т. 3, № 2. С. 62–79.
4. Турдалиев Н. И. Синтез самокорректирующихся схем из функциональных элементов для некоторых последовательностей булевых функций: Дис. ... канд. физ.-мат. наук. М., 1989.

5. **Чашкин А. В.** О сложности булевых матриц, графов и соответствующих им булевых функций // Дискрет. математика. 1994. Т. 6, вып. 2. С. 43–73.
6. **Чашкин А. В.** Сложность и глубина синдрома кода Хэмминга // Радиотехника. 1996. Вып. 12. С. 35–39.

Адрес автора:

МГУ, мех.-мат. факультет,  
Воробьевы горы,  
119899 Москва, Россия.  
E-mail: chash@glasnet.ru

Статья поступила

2 февраля 1998 г.