Короткие тесты для схем в базисе Жегалкина

Д. С. Романов (МГУ им. М. В. Ломоносова),
Е. Ю. Романова (РГСУ)

В работе предлагается метод синтеза неизбыточных схем из функциональных элементов в базисе Жегалкина, реализующих произвольные булевы функции без дополнительных входов и выходов и допускающих относительно произвольных константных неисправностей на входах и выходах элементов единичные проверяющие тесты, длина которых ограничена сверху константой 16.

Ключевые слова: схема из функциональных элементов, проверяющий тест, константная неисправность, функция Шеннона, легкотестируемая схема.

В данной статье рассматривается задача синтеза неизбыточных легкотестируемых схем из функциональных элементов (СФЭ) при одиночных произвольных константных неисправностях а) на входах и выходах элементов (обозначим источник таких неисправностей через IO_1^{const}) и б) на входах и выходах элементов или входах схемы (обозначим источник таких неисправностей через PIO_1^{const}). Все необходимые определения могут быть найдены в статье [1]. Пусть $B_1 = \{x \;\&\; y, x \oplus y, 1\}$ — базис Жегалкина, $B' = \{x \,\&\, y, x \oplus y, x \sim y\}$. Настоящая работа улучшает оценки функций Шеннона длины теста, полученные в статье [2] (с учетом [3, стр. 113–116]).

Теорема 1. *При любом $n \in \mathbb{N}_0$ любую булеву функцию f от n переменных можно реализовать неизбыточной СФЭ в базисе B' (B_1) с n входами и одним выходом, допускающей единичный проверяющий тест длины не более 16 относительно IO_1^{const}.*

Доказательство. Построим неизбыточную схему S в базисе B', реализующую функцию f и допускающую единичный проверяющий тест длины 16 (для базиса B_1 рассуждения аналогичны). Пусть $f(\tilde{x}^n)$ — произвольная булева функция, зависящая от переменных $x_1, x_2, \ldots, x_n$. Схемы в базисе B' для всех функций, зависящих не более чем от двух переменных, описаны в работе [1, рис. 6 и случай 2 в док-ве теоремы 1], — они являются неизбыточными и относительно IO_1^{const}. Пусть теперь функция f существенно зависит не менее чем от трех переменных. Обозначим $f_{\sigma_1\sigma_2}(x_3, \ldots, x_n) = f(\sigma_1, \sigma_2, x_3, \ldots, x_n)$. Разложим функцию f по первым двум переменным: $f(\tilde{x}^n) = \bar{x}_1\bar{x}_2 f_{00} \oplus \bar{x}_1 x_2 f_{01} \oplus x_1\bar{x}_2 f_{10} \oplus x_1 x_2 f_{11}$. Это разложение будем рассматривать с учетом следующих дополнений: если какая-то функция $f_{\sigma_1\sigma_2}$ тождественно равна константе 0, то соответствующее ей слагаемое пропадает в данном разложении, а если какая-то функция $f_{\sigma_1\sigma_2}$ тождественно равна константе 1, то соответствующее ей слагаемое в данном разложении приобретает вид $x_1^{\sigma_1} x_2^{\sigma_2}$. То есть в дальнейшем будем считать, что каждая моделируемая функция $f_{\sigma_1\sigma_2}$ тождественно не равна константе.

Запишем полином Жегалкина функции $f_{\sigma_1\sigma_2}$ в виде $\bigoplus\limits_{i=1}^{t_{\sigma_1\sigma_2}} K_i^{(\sigma_1\sigma_2)} \oplus a_0^{(\sigma_1\sigma_2)}$, где $K_i^{(\sigma_1\sigma_2)}$ — монотонные конъюнкции, $a_0^{(\sigma_1\sigma_2)} \in \{0,1\}$. Пусть $K_1^{(\sigma_1\sigma_2)} = x_{j_{\sigma_1\sigma_2,1}} x_{j_{\sigma_1\sigma_2,2}} \cdots x_{j_{\sigma_1\sigma_2,s(\sigma_1,\sigma_2)}}$ — слагаемое минимального ранга в полиноме функции $f_{\sigma_1\sigma_2}$, отличное от константы. Условимся, что в каждой монотонной конъюнкции $K_i^{(\sigma_1\sigma_2)}$ $(i = \overline{2, t_{\sigma_1\sigma_2}})$ последний множитель отличен от $x_{j_{\sigma_1\sigma_2,s(\sigma_1,\sigma_2)}}$.

Договоримся под схемой $S_I^{\sim\sigma}$ при $\sigma = 1$ понимать схему с левым входом y, являющимся выходом схемы, и с (фиктивным) правым входом z, а при $\sigma = 0$ — схему, моделирующую формулу $(y \oplus z) \sim z$. Схема $S_\oplus^{\oplus\sigma}$ при $\sigma = 0$ моделирует формулу $x \oplus y$, а при $\sigma = 1$ — формулу $x \sim y$. Пусть $K_i^{(\sigma_1\sigma_2)} = x_{\nu_1} x_{\nu_2} \cdots x_{\nu_r}$ — слагаемое полинома Жегалкина функции $f_{\sigma_1\sigma_2}$ $(r \in \{1, 2, \ldots, n-2\},\ \nu_1 \in \{3, \ldots, n\})$. Построим схему $S_{K_i^{(\sigma_1\sigma_2)}}$, при условии $(x_1 = \sigma_1)\ \&\ (x_2 = \sigma_2)$ на своем выходе реализующую $K_i^{(\sigma_1\sigma_2)}$ (рис. 1). Схема S_{comp} (рис. 2), играет роль схемы сравнения значений, подаваемых на ее входы y_1, y_2. Схема S_{detect} моделирует формулу $(x_1 \oplus x_2)(y_1 \oplus x_3) \oplus (x_1 \oplus x_2)(y_2 \oplus x_3) \oplus (x_2 \oplus y_1)(y_2 \oplus x_3) \oplus (x_2 \oplus y_1)(y_1 \oplus x_3) \oplus y_2$ и играет роль схемы передачи на выход сигнала о том, что $y_1 \neq x_1$ или $y_2 \neq x_1$.

Для каждого слагаемого $K_i^{(\sigma_1\sigma_2)} = x_{\nu_1} x_{\nu_2} \cdots x_{\nu_r}$ полинома Жегалкина функции $f_{\sigma_1\sigma_2}$ построим схему $S_i^{(\sigma_1\sigma_2)}$ следующим образом. Возьмем две копии $S^{(1)}_{K_i^{(\sigma_1\sigma_2)}}$ и $S^{(2)}_{K_i^{(\sigma_1\sigma_2)}}$ схемы $S_{K_i^{(\sigma_1\sigma_2)}}$ и для каждой пары дублирующих друг друга элементов этих схем возьмем «собственную» подсхему S_{comp}, к первому и второму входам которой подсоединим выходы

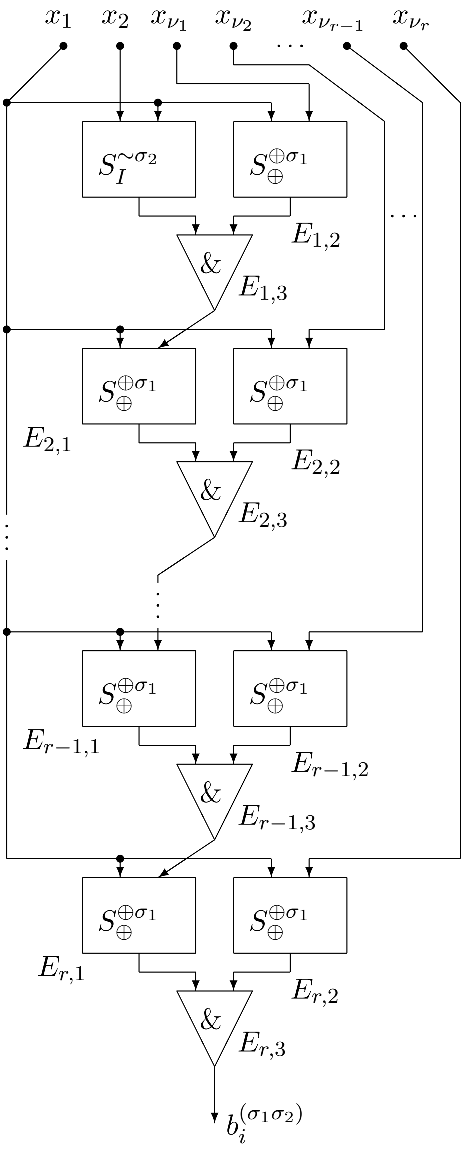

Рис. 1. Схема $S_{K_i^{(\sigma_1\sigma_2)}}$.

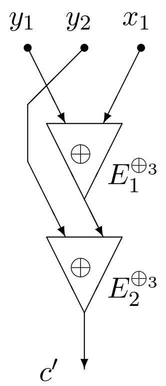

Рис. 2. Схема S_{comp}.

дублирующих элементов первой и второй копии соответственно, а третий вход ассоциируем с входной переменной x_1. Выходами полученной схемы $S_i^{(\sigma_1\sigma_2)}$ объявим выход $b_i^{(\sigma_1\sigma_2)}$ подсхемы $S^{(1)}_{K_i^{(\sigma_1\sigma_2)}}$ (обозначим этот выход в схеме $S_i^{(\sigma_1\sigma_2)}$ через $b_i^{(\sigma_1\sigma_2),1}$), а также все выходы подсхем вида

S_{comp}. Построим теперь схему $S^{(\sigma_1\sigma_2)}$, содержащую в качестве подсхем построенные ранее (и не имеющие общих элементов) подсхемы $S_1^{(\sigma_1\sigma_2)}$, $\ldots$, $S_{t_{\sigma_1\sigma_2}}^{(\sigma_1\sigma_2)}$.

Если $t_{\sigma_1\sigma_2} = 1$ и $a_0^{(\sigma_1\sigma_2)} = 0$, то $S^{(\sigma_1\sigma_2)}$ совпадает с $S_1^{(\sigma_1\sigma_2)}$, выход $b_1^{(\sigma_1\sigma_2),1}$ объявляется выходом $b^{(\sigma_1\sigma_2)}$ подсхемы $S^{(\sigma_1\sigma_2)}$, при этом выходы всех подсхем вида S_{comp} также считаются выходами схемы $S^{(\sigma_1\sigma_2)}$. Если $t_{\sigma_1\sigma_2} = 1$ и $a_0^{(\sigma_1\sigma_2)} = 1$, то отличие от предыдущего случая заключается лишь в том, что выход $b_1^{(\sigma_1\sigma_2),1}$ подсоединяется к левому входу новой подсхемы вида $S_I^{\sim 0}$ (правый вход этой подсхемы ассоциируется с входной переменной x_3). Выход этой подсхемы объявляется выходом $b^{(\sigma_1\sigma_2)}$ подсхемы $S^{(\sigma_1\sigma_2)}$, при этом выходы всех подсхем вида S_{comp} также считаются выходами схемы $S^{(\sigma_1\sigma_2)}$. Если $t_{\sigma_1\sigma_2} > 1$ и $a_0^{(\sigma_1\sigma_2)} = 0$, то к подсхемам $S_1^{(\sigma_1\sigma_2)}, \ldots, S_{t_{\sigma_1\sigma_2}}^{(\sigma_1\sigma_2)}$ добавляется цепочка $C^{(\sigma_1\sigma_2)}$ из $t_{\sigma_1\sigma_2}-1$ элементов сложения по модулю 2, при этом к первому входу каждого элемента цепочки $C^{(\sigma_1\sigma_2)}$, начиная со второго, подсоединяется выход предыдущего элемента цепочки, к остальным входам элементов цепочки подсоединяются выходы $b_1^{(\sigma_1\sigma_2),1}, \ldots, b_{t_{\sigma_1\sigma_2}}^{(\sigma_1\sigma_2),1}$ в «естественнном» порядке. Выход последнего элемента цепочки $C^{(\sigma_1\sigma_2)}$ объявляется выходом $b^{(\sigma_1\sigma_2)}$ подсхемы $S^{(\sigma_1\sigma_2)}$, при этом выходы всех подсхем вида S_{comp} также считаются выходами схемы $S^{(\sigma_1\sigma_2)}$. Если $t_{\sigma_1\sigma_2} > 1$ и $a_0^{(\sigma_1\sigma_2)} = 1$, то последним элементом цепочки $C^{(\sigma_1\sigma_2)}$ является элемент эквивалентности.

Построим подсхему Σ_D, состоящую из подсхемы $\Sigma_D^{(1)}$, подсхемы $\Sigma_D^{(2)}$, нескольких подсхем вида S_{comp} и четырех подсхем вида $S_I^{\sim 0}$. Подсхема $\Sigma_D^{(1)}$ моделирует 4 формулы: $d^{(00)} = ((x_1 \oplus x_2) \sim x_2)\&((x_2 \oplus x_1) \sim x_1)$, $d^{(01)} = ((x_1 \oplus x_2) \sim x_2)\&x_2$, $d^{(10)} = x_1\&((x_2 \oplus x_1) \sim x_1)$, $d^{(10)} = x_1\&x_2$. Подсхема $\Sigma_D^{(2)}$ — копия подсхемы $\Sigma_D^{(1)}$, в которой удалены конъюнкторы, выходы которых имеют такое обозначение $d^{(\sigma_1\sigma_2)}$, что $a_0^{(\sigma_1\sigma_2)} = 1$. Для каждой пары дублирующих друг друга элементов подсхем $\Sigma_D^{(1)}$ и $\Sigma_D^{(2)}$, кроме элементов E_{20} и E_{25}, возьмем «собственную» подсхему S_{comp}, к первому и второму входам которой подсоединим выходы дублирующих элементов первой и второй копии соответственно, а третий вход ассоциируем с входной переменной x_1. Выходы элементов E_{20} и E_{25} в подсхемах $\Sigma_D^{(1)}$ и $\Sigma_D^{(2)}$ подсоединим к первым входам новых подсхем вида $S_I^{\sim 0}$ (назовем их $S_{20}^{(1)}$, $S_{25}^{(1)}$, $S_{20}^{(2)}$, $S_{25}^{(2)}$), вторые входы этих подсхем ассоциируем с входной переменной x_2. Схема Σ_D построена полностью. Выходами полученной схемы Σ_D объявим выходы $d^{(00)}$, $d^{(01)}$, $d^{(10)}$, $d^{(11)}$ подсхемы

$\Sigma_D^{(1)}$ (сохраним для них эти обозначения и в подсхеме Σ_D), все выходы подсхем вида S_{comp}, а также выходы подсхем $S_{20}^{(1)}$, $S_{25}^{(1)}$, $S_{20}^{(2)}$, $S_{25}^{(2)}$.

Построим подсхему Σ_{detect}. Эта подсхема представляет собой цепочку подсхем вида S_{detect}, причем количество подсхем S_{detect} в этой цепочке на 3 больше общего числа подсхем вида S_{comp} в подсхемах $S^{(00)}$, $S^{(01)}$, $S^{(10)}$, $S^{(11)}$ и Σ_D. Последние три входа каждой подсхемы S_{detect} ассоциируются с входными переменными x_1, x_2, x_3 (в этом порядке). К первому входу каждой подсхемы S_{detect} в цепочке, начиная со второй, подсоединяется выход предыдущей подсхемы S_{detect} в цепочке. К остальным входам подсхем S_{detect} подсоединяются (вообще говоря, в произвольном порядке) выходы подсхем вида S_{comp}, а также выходы подсхем $S_{20}^{(1)}$, $S_{25}^{(1)}$, $S_{20}^{(2)}$, $S_{25}^{(2)}$. Выход последней подсхемы S_{detect} в цепочке считается выходом подсхемы Σ_{detect} — обозначим его через e. Легко заметить, что в отсутствие неисправностей в Σ_{detect} если на один из первых двух входов одной из подсхем вида S_{detect} в подсхеме Σ_{detect} оказалось подано значение, отличное от значения переменной x_1, то на выходе e появится значение $\bar{x}_1$.

Подсхема Σ_{out} моделирует формулу $d^{(00)}b^{(00)} \oplus d^{(01)}b^{(01)} \oplus d^{(10)}b^{(10)} \oplus d^{(11)}b^{(11)} \oplus x_1 \oplus e$. Единственным выходом схемы S объявляется выход подсхемы Σ_{out}. Схема S построена полностью.

Легко доказать, что при отсутствии неисправностей схема S реализует функцию f. Последовательной проверкой устанавливается, что единичный проверяющий тест для схемы S может состоять из следующих не более чем 16 наборов: а) не более чем 8 наборов вида $\tilde{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_3)$; б) не более чем 4 набора вида $\tilde{\beta}^{(\sigma_1\sigma_2)} = (\sigma_1, \sigma_2, \beta_3^{(\sigma_1\sigma_2)}, \dots, \beta_n^{(\sigma_1\sigma_2)})$, где $\beta_j^{(\sigma_1\sigma_2)} = 1$ тогда и только тогда, когда множитель x_j входит в конъюнкцию $K_1^{(\sigma_1\sigma_2)}$ ($j \in \{3, \dots, n\}$); в) не более чем 4 набора вида $\tilde{\gamma}^{(\sigma_1\sigma_2)} = (\bar{\sigma}_1, \sigma_2, 1, \dots, 1, 0, 1, \dots, 1)$, где единственный (среди координат с 3-ей по n-ю) ноль является значением переменной $x_{j_{\sigma_1\sigma_2, s(\sigma_1,\sigma_2)}}$. Теорема доказана.

Следствие 1. *При любом $n \in \mathbb{N}_0$ в базисе B' (B_1) функция Шеннона длины единичного проверяющего теста относительно PIO_1^{const} (при реализации функций n переменных неизбыточными СФЭ с n входами и одним выходом) имеет вид $2n - 2\log_2 n + \Theta(1)$.*

Следствие 2. *При любом $n \in \mathbb{N}_0$ в базисе B' (B_1) любую булеву функцию n переменных можно реализовать неизбыточной СФЭ с n входами и с 3-мя выходами, допускающей единичный проверяющий тест длины не более 18 относительно PIO_1^{const}.*

Работа выполнена при финансовой поддержке грантов РФФИ № 15–01–07474-а и № 13–01–00958-а и Государственного задания № 2014/601 от 06.02.2014.

Список литературы

[1] Романов Д. С. Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. — 2014. — Т. 26, вып. 2. — С. 100–130.

[2] Reddy S. M. Easily testable realization for logic functions // IEEE Trans. Comput. — 1972. — Vol. 21, Iss. 1. — P. 124–141.

[3] Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.