ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ X МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

Москва,
5–11 октября 2015 г.

МАТЕРИАЛЫ
X МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ
И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 5–11 октября 2015 г.)

ИПМ им. М. В. Келдыша РАН
Москва 2015

УДК 519.7
ББК 22.176
М34

М34 Материалы X молодежной научной школы по дискретной математике и ее приложениям (Москва, 5–11 октября 2015 г.). Под редакцией А. В. Чашкина. — М.: ИПМ им. М. В. Келдыша, 2015. — 88 с.

Сборник содержит материалы X молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 5 по 11 октября 2015 г. Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики. Информация о молодежных школах по дискретной математике в сети Интернет по адресу: `http://keldysh.ru/dmschool/`.

Научное издание

МАТЕРИАЛЫ
X МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ
И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 5–11 октября 2015 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *А. Д. Яшунский*

СОДЕРЖАНИЕ

О СЛОЖНОСТИ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ В БЕСКОНЕЧНО-ПОРОЖДЕННЫХ КЛАССАХ

А. А. Андреев (Москва)

Рассматривается задача получения высоких нижних оценок различных мер сложности реализации функций многозначной логики из замкнутых классов над бесконечными базисами, порождающими эти классы. Под базисом понимается любая порождающая система, не обязательно полная и не обязательно минимальная по включению. Бесконечным базисом называется базис, содержащий функции, существенно зависящие от сколь угодно большого числа переменных.

В качестве основных модельных классов управляющих систем рассматриваются формулы [1] и схемы из функциональных элементов [2]. В качестве мер сложности рассматриваются глубина и собственно сложность. В работе переменные и константы для удобства также будем считать формулами (такие формулы будем называть тривиальными). Под сложностью формулы понимается количество символов переменных и констант, входящих в формулу, под сложностью схемы из функциональных элементов (далее просто схемы) — число функциональных элементов в ней. Понятие глубины $D(F)$ формулы F определим индуктивно. Если формула F тривиальная, то $D(F) = 0$, а если $F = G(F_1, \ldots, F_m)$ (где G — некоторая функция), то $D(F) = \max D(F_i)+1$, где максимум берется по всем $i = 1, \ldots, m$. Сложностью $L^{\Phi}_{\mathfrak{B}}(f)$ функции f при реализации формулами над базисом $\mathfrak{B}$ называется минимальная сложность формулы над базисом $\mathfrak{B}$, реализующей эту функцию. Аналогично определяются сложность $L^{\text{СФЭ}}_{\mathfrak{B}}(f)$ функции f при реализации схемами над базисом $\mathfrak{B}$ и глубина функции $D_{\mathfrak{B}}(f)$ (понятие глубины функции не отличается для случаев реализации схемами и формулами). Функцией Шеннона $L^{\Phi}_{\mathfrak{B}}(n)$ назовем максимальную сложность реализации формулами над базисом $\mathfrak{B}$ функций от n переменных из замыкания $[\mathfrak{B}]$ базиса $\mathfrak{B}$. Аналогично определим функцию Шеннона $L^{\text{СФЭ}}_{\mathfrak{B}}(n)$ сложности реализации функций из класса $[\mathfrak{B}]$ схемами над базисом $\mathfrak{B}$ и функцию Шеннона глубины $D_{\mathfrak{B}}(n)$ реализации функций из класса $[\mathfrak{B}]$ над базисом $\mathfrak{B}$.

Асимптотика роста функций Шеннона $L^{\text{СФЭ}}_{\mathfrak{B}}(n)$, $L^{\Phi}_{\mathfrak{B}}(n)$ и $D_{\mathfrak{B}}(n)$ над произвольным полным конечным базисом булевых функций установлена О. Б. Лупановым [3–5]. Для всякого конечного полного базиса $\mathfrak{B}$ функция Шеннона $L^{\text{СФЭ}}_{\mathfrak{B}}(n)$ сложности реализации булевых функций схемами над этим базисом при $n \to \infty$ растет по порядку как $2^n/n$, сложности реализации формулами $L^{\Phi}_{\mathfrak{B}}(n)$ — как $2^n/\log n$, а функция Шеннона глубины $D_{\mathfrak{B}}(n)$ — как n.

При переходе от конечного полного базиса к бесконечному полному базису булевых функций порядки роста введенных функций Шеннона понижаются. Из результатов О. Б. Лупанова непосредственно следует, что для любых полных базисов $\mathfrak{B}_1$ и $\mathfrak{B}_2$, где $\mathfrak{B}_1$ — конечный, а $\mathfrak{B}_2$ — бесконечный, справедливы соотношения $L^{\text{СФЭ}}_{\mathfrak{B}_2}(n) = o(L^{\text{СФЭ}}_{\mathfrak{B}_1}(n))$, $L^{\Phi}_{\mathfrak{B}_2}(n) = o(L^{\Phi}_{\mathfrak{B}_1}(n))$, $D_{\mathfrak{B}_2}(n) = o(D_{\mathfrak{B}_1}(n))$. На самом деле О. М. Касим-Заде установлено [6, 7], что при переходе от конечных к бесконечным полным базисам булевых функций порядок роста функций Шеннона $L^{\text{СФЭ}}_{\mathfrak{B}}(n)$ и $D_{\mathfrak{B}}(n)$ меняется качественно: в случае бесконечных базисов $L^{\text{СФЭ}}_{\mathfrak{B}}(n)$ растет по порядку как $2^{n/2}$ или медленнее, а $D_{\mathfrak{B}}(n)$ имеет порядок роста не больше $\log n$. В случае реализации функций k-значной логики при $k \geqslant 3$ для функции Шеннона глубины при переходе от конечных полных к бесконечным полным базисам имеет место аналогичное понижение порядка роста. Для любого конечного базиса $\mathfrak{B}$ функций k-значной логики ($k \geqslant 3$) функция Шеннона глубины $D_{\mathfrak{B}}(n)$ при $n \to \infty$ растет по порядку как линейная функция (для этого случая также известна асимптотика [8]). Для бесконечных базисов многозначной логики известно [9], что функция Шеннона глубины $D_{\mathfrak{B}}(n)$ растет по порядку не быстрее, чем $\log n$. Стоит отметить, что при переходе от конечных базисов, порождающих замкнутые классы булевых функций, к бесконечным может также иметь место аналогичный эффект понижения порядков роста соответствующих функций Шеннона (см., например, [10]). Однако, к примеру, для класса линейных функций и в случае конечного, и в случае бесконечного базиса, порождающего этот класс, функция Шеннона сложности реализации формулами растет по порядку как n.

В связи с этим возникает вопрос о возможности получения высоких нижних оценок сложности (для всех трех мер) над бесконечными базисами, аналогичных известным [11–13] высоким нижним оценкам сложности в конечных неполных базисах функций k-значной логики, $k \geqslant 3$.

Стоит отметить, что в случае булевых функций все замкнутые классы конечно-порожденные. Это значит, что любой бесконечный базис будет избыточным, и из него можно выделить конечную подсистему, порождающую тот же замкнутый класс. Следовательно, порядок роста при переходе от конечного базиса булевых функций к бесконечному не может увеличиться. В случае же функций многозначной логики ситуация иная. Существуют примеры замкнутых классов, не имеющих конечного базиса [14], что дает дополнительные возможности для получения высоких нижних оценок в бесконечных базисах по сравнению с оценками в конечных базисах.

Построим замкнутые классы функций многозначной логики, не являющиеся конечно-порожденными, в которых для всех типов рассматриваемых функций Шеннона при соответствующем выборе базиса (бесконечного неполного) будут справедливы нижние оценки с более высоким порядком роста, чем у известных [11–13] соответствующих нижних оценок в случае конечно-порожденных классов.

Пусть $\varphi(x)$ — функция трехзначной логики, принимающая значение 1 при $x = 2$ и значение 0 в остальных случаях. Пусть $\Omega(\tilde{x})$ — отображение из E_3^n в E_2^n, которое набору $(x_1, \ldots, x_n)$ сопоставляет набор $(\varphi(x_1), \ldots, \varphi(x_n))$. Пусть $\tilde{\alpha}$ — набор из E_2^n. Определим функцию $\lambda_{\tilde{\alpha}}^3(y, x_1, \ldots, x_n)$ из P_3 следующим образом.

$$\lambda_{\tilde{\alpha}}^3(y, x_1, \ldots, x_n) = \begin{cases} 0, & \text{если } y = 0 \text{ и } \Omega(\tilde{x}) \neq \tilde{\alpha}, \text{ или если } y = 2, \\ 1, & \text{если } y = 1, \text{ или если } y = 0 \text{ и } \Omega(\tilde{x}) = \tilde{\alpha}; \end{cases}$$

Определим функции трехзначной логики $\zeta_n^3(x_1, \ldots, x_n)$, $n \geqslant 1$, следующим образом. Функция ζ_n^3 принимает значение 0, если среди ее аргументов четное количество двоек, и значение 1, если нечетное. Пусть $R_2 = \bigcup\limits_{n \in \mathbb{N}} E_2^n$. Рассмотрим неполный бесконечный базис $\mathfrak{A} = \{0\} \cup \{\lambda_{\tilde{\alpha}}^3 \mid \tilde{\alpha} \in R_2\}$. Справедливо следующее утверждение.

Теорема 1. *Для функции трехзначной логики ζ_n^3, $n \geqslant 1$, выполняется равенство*

$$D_{\mathfrak{A}}(\zeta_n^3) = 2^{n-1}.$$

Заметим также, что сложность реализации функции схемами над некоторым базисом не меньше глубины этой функции над этим базисом. Поэтому приведенная выше формула доставляет пример минимальной схемы над базисом $\mathfrak{A}$ для функции ζ_n^3, т. е.

$$L_{\mathfrak{A}}^{\text{СФЭ}}(\zeta_n^3) = 2^{n-1},$$

причем полученное значение сложности превосходит максимальные нижние оценки, известные [11] для случая конечных базисов.

Покажем теперь как на основе этого примера построить бесконечный базис в P_4 и последовательность функций, сложность реализации которых формулами над этим базисом растет сверхэкспоненциально (и быстрее известных рекордных высоких оценок для случая конечно-порожденных классов P_4).

Пусть $\varphi(x)$ — функция четырехзначной логики, принимающая значение 1 при $x = 2$ и значение 0 в остальных случаях. Пусть $\Omega(\tilde{x})$ — отображение из E_4^n в E_2^n, которое набору $(x_1, \ldots, x_n)$ сопоставляет набор $(\varphi(x_1), \ldots, \varphi(x_n))$. Пусть $\tilde{\alpha}$ — набор из E_2^n. Определим функции $\lambda_{\tilde{\alpha}}^4(y, x_1, \ldots, x_n)$ и $\mu_{\tilde{\alpha}}(x_1, \ldots, x_{n+2})$ из P_4 следующим образом:

$$\lambda_{\tilde{\alpha}}^4(y, x_1, \ldots, x_n) = \begin{cases} \lambda_{\tilde{\alpha}}^3(y, x_1, \ldots, x_n), \text{ если } (y, x_1, \ldots, x_n) \in E_3^n \\ 3, \text{ иначе;} \end{cases}$$

$$\mu_{\tilde{\alpha}}(x_1, \ldots, x_{n+2}) = \begin{cases} 3, \text{ если } x_i = 3 \text{ для некоторого} \\ \quad i \in \{1, \ldots, n+2\}, \text{ или если } x_1 \neq x_2, \\ \lambda_{\tilde{\alpha}}^4(x_2, \ldots, x_{n+2}), \text{ иначе.} \end{cases}$$

Определим последовательность функций четырехзначной логики $\zeta_n^4(x_1, \ldots, x_n)$, $n \geqslant 1$, следующим образом. Если среди аргументов функции есть хотя бы одна тройка, то она принимает значение 3. Если же нет, то функция ζ_n^4 принимает значение 0, если среди ее аргументов четное количество двоек, и значение 1, если нечетное. Рассмотрим неполный бесконечный базис $\mathfrak{A} = \{0\} \cup \{\mu_{\tilde{\alpha}} \mid \tilde{\alpha} \in R_2\}$. Имеет место следующее утверждение.

Теорема 2. *Для функции четырехзначной логики ζ_n^4, $n \geqslant 1$, верно равенство*

$$L_{\mathfrak{A}}^{\Phi}(\zeta_n^4) = 2^{2^{n-1}} - 1.$$

Отметим, что установленный в теореме 2 рост сложности реализации последовательности функций ζ_n^4 формулами над бесконечным базисом $\mathfrak{A}$, порождающий замкнутый класс в P_4, не имеющий конечного базиса, превосходит известную [12] рекордную оценку сложности реализации последовательности функций над конечным базисом в P_4, имеющую вид

$$2^{C_n^{[n/2]}}([n/2] + 1) - [n/2].$$

Конструкции из доказательств теоремы 1 (для функций трехзначной логики) и теоремы 2 (для функций четырехзначной логики) могут быть обобщены на случай функций k-значной логики для бóльших значений k, и результаты такого обобщения превосходят рекордные результаты в случае конечнопорожденных классов [13]. Справедливы следующие утверждения.

Теорема 3. *Пусть r, n — произвольные натуральные числа, такие что $r \geqslant 2$. Тогда существует натуральное число $k = k(r) = r + 1$, замкнутый класс функций k-значной логики, не имеющий конечного базиса, и лежащая в нем функция от n переменных, глубина (и сложность реализации схемами) которой над некоторым бесконечным базисом, порождающим этот класс, равна r^{n-1}.*

Теорема 4. *Пусть r, m — произвольные натуральные числа, такие что $r \geqslant 2$. Тогда существует натуральное число $k = k(r) = r + 2$, замкнутый класс функций k-значной логики, не имеющий конечного базиса, и лежащая в нем последовательность функций от n переменных, сложность реализации формулами которых над некоторым бесконечным базисом, порождающим этот класс, равна по порядку $m^{r^{n-1}}$.*

Работа выполнена при поддержке РФФИ (проект № 14-01-00598-а) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986. 384 с.
2. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М.: Изд-во Моск. ун-та, 1984. 136 с.
3. Лупанов О. Б. Об одном методе синтеза схем // Известия ВУЗ. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.
4. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. — М.: Физматгиз, 1960. — С. 61–80.
5. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.
6. Касим-Заде О. М. Общая верхняя оценка сложности схем в произвольном бесконечном полном базисе // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 1997. — № 4. — С. 59–61.
7. Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным базисом // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2007. — № 1. — С. 18–21.
8. Кочергин А. В. О глубине функций k-значной логики в конечных базисах // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2013. — № 1. — С. 56–59.
9. Кочергин А. В. О глубине функций k-значной логики в бесконечных базисах // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2011. — № 1. — С. 22–26.
10. Угольников А. Б. Синтез схем и формул в неполных базисах // Препринт ИПМ АН СССР. — М., 1980. — № 112.
11. Ткачев Г. А. О сложности реализации одной последовательности функций k-значной логики // Вестник Моск. ун-та. Сер. 15. Вычислительная математика и кибернетика. — 1977. — № 1. — С. 45–47.
12. Угольников А. Б. О сложности реализации формулами одной последовательности функций 4-значной логики // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2004. — № 3. — С. 52–55.
13. Андреев А. А. О нижних оценках сложности для некоторых последовательностей функций многозначной логики // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2013. — № 6. — С. 25–30.
14. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

СВИТЧИНГОВАЯ РАЗДЕЛИМОСТЬ ГРАФОВ ПО МОДУЛЮ Q

Е. А. Беспалов (Новосибирск)

Введение

Рассматриваются неориентированные графы, ребра которых помечены элементами из множества $\{1,\dots,q-1\}$, $q \geqslant 2$ — натуральное, которые будем называть *весом* ребра (вес можно также трактовать как кратность). Метку 0 будем ассоциировать с отсутствием ребра, т. е. пару несмежных вершин будем считать ребром веса 0 (что тем не менее не позволяет считать эти вершины соседними). Таким образом, реберно помеченный граф удобно представлять парой (V,E), где V — множество вершин, а $E : V^2 \to \{0,1,\dots,q-1\}$ — симметричное отображение, равное нулю везде на диагонали $\{(v,v)|v \in V\}$. Под *подграфом* графа $G = (V,E)$ будем подразумевать граф $G_W = (W,I)$, порожденный множеством вершин $W \subset V$ и унаследовавший от G веса ребер: $I(v,w) = E(v,w)$, для любых $v,w \in W$. Результатом сложения двух графов G_1 и G_2 с общим множеством вершин будет граф G на том же множестве вершин, определенный следующим образом: вес любого ребра графа G равен сумме по модулю q весов соответствующих ребер в графах G_1 и G_2. Граф будем называть *аддитивным*, если каждую его вершину можно пометить числами от 0 до $q-1$ таким образом, что вес каждого ребра будет равен сумме по модулю q меток двух вершин ребра. Далее определим *свитчинг* графа G, как результат сложения графа G с некотором аддитивным графом на том же множестве вершин. Множество вершин W графа G назовем *отделимым*, если некоторый свитчинг графа G не содержит ребер (ненулевого веса) между W и $V\backslash W$. Легко видеть, что любое множество вершин мощности 0, 1, $n-1$ или n в графе порядка n является отделимым. Любые другие отделимые множества назовем *нетривиальными*. Граф $G = (V,E)$ назовем *свитчингово разделимым* (далее в тексте — просто *разделимым*), если существует нетривиальное отделимое множество его вершин.

Исследуется, для каких k верно следующее утверждение (признак разделимости): если в графе G порядка n все подграфы порядка k разделимы, то и сам граф G разделим.

В случае $k = n-1$ этот вопрос оказывается важным с точки зрения изучения другого класса комбинаторных объектов — n-арных квазигрупп, в комбинаторике известных также как латинские гиперкубы. Под n-арной квазигруппой конечного порядка q понимается n-местная операция $\Sigma^n \to \Sigma$, обратимая по каждому аргументу, где Σ — некоторое множество мощности q (носитель квазигруппы). Будем называть n-арную квазигруппу разделимой, если она представима в виде бесповторной суперпозиции квазигрупп меньшей арности.

В случае $q = 2$ в статье [1] была построена серия примеров неразделимых графов нечетного порядка n, у которых все подграфы порядка $n-1$ разделимы, а также описан способ построений по этим графам неразделимых квазигрупп, у которых все ретракты, полученные фиксированием одной переменной, разделимы. Позже эти результаты были использованы в статье [2] при характеризации квазигрупп порядка 4. В статье [3] было показано, что других графов с такими свойствами не существует. Настоящая работа содержит обобщение результатов про свитчинговую разделимость графов на случай произвольного q.

Признаки свитчинговой разделимости графов по модулю q

Сумма двух аддитивных графов также является аддитивным графом. Поэтому отношение «граф G — свитчинг графа H» является эквивалентностью. Если множество отделимо в графе, то оно отделимо и в каждом его свитчинге. Таким образом, в вопросах разделимости мы всегда можем рассматривать наиболее удобный свитчинг графа. Имеет место следующая

Лемма. *Если в графе G порядка n все подграфы порядков $n-1$ и $n-2$ разделимы, то и граф G разделим.*

Для формулировки основных результатов при четном q определим семейство графов $G_{n,\gamma}$, $\gamma \in \{0, \dots, q-1\}$, $n = 2k+1 \geqslant 5$. Множество вершин графа — $\{a_0, a_1, \dots, a_k, b_1, \dots, b_k\}$, вершина a_0 изолирована, веса остальных ребер определяются следующим образом:

- для любых l, m вес ребра $\{a_l, b_m\}$ равен γ, если $l < m$, и $\gamma + q/2 (\mathrm{mod}\, q)$, если $l \geqslant m$;
- для любых различных l, m ребра $\{a_l, a_m\}$ и $\{b_l, b_m\}$ имеют вес γ.

Граф $G_{n,0}$ изображен на рис. 1.

Получены следующие результаты:

Теорема 1. *Если в графе G порядка n все подграфы порядка $n-1$ разделимы, то либо граф G разделим, либо q — четно, n — нечетно и граф G изоморфен некоторому свитчингу графа $G_{n,\gamma}$.*

Теорема 2. *Если в графе G порядка $n \geqslant 9$ все подграфы порядка $n-2$ разделимы, то и граф G разделим.*

Теорема 3. *Если в графе G порядка $n \geqslant 9$ все подграфы порядка $k \geqslant 7$ разделимы, то либо граф G разделим, либо q, k — четны, n — нечетно и граф G изоморфен некоторому свитчингу графа $G_{n,\gamma}$.*

Исследование выполнено за счет гранта Российского научного фонда (проект №14-11-00555).

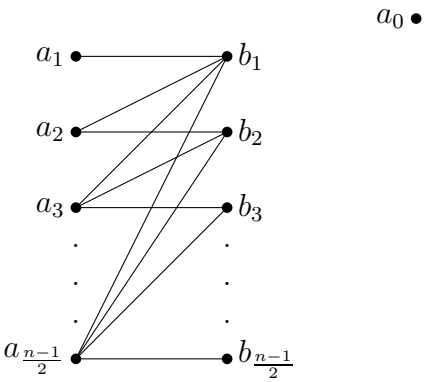

Рис. 1: Граф $G_{n,0}$.

Список литературы

1. Кротов Д. С. О связи свитчинговой разделимости графа и его подграфов // Дискрет. анализ и исслед. операций — 2010. — Т. 17, вып. 2. — С. 46–56.
2. Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4. SIAM J. Discrete Math. — 2009. — Т. 23, вып. 2. — С. 561–570.
3. Беспалов Е. А. On switching nonseparable graphswith switching separable subgraphs // Сиб. электр. матем. изв. — 2014. — Т. 11. — С. 988–998.

МИНИМАЛЬНЫЕ НОСИТЕЛИ СОБСТВЕННЫХ ФУНКЦИЙ НЕКОТОРЫХ ГРАФОВ ХЭММИНГА

А. А. Валюженич (Новосибирск)

Расстоянием Хэмминга $d(x, y)$ между словами $x, y \in \{0, 1, \ldots, q-1\}^n$ называется число позиций, в которых x и y различны. *Графом Хэмминга* называется граф, вершины которого — это все слова длины n над алфавитом $\{0, 1, \ldots, q-1\}$, а ребрами графа соединяются вершины на расстоянии Хэмминга 1. Обозначим граф Хэмминга через $H(n, q)$. Хорошо известно, что множество собственных значений матрицы смежности графа $H(n, q)$ есть $\{\lambda_m = n(q-1) - qm | m = 0, 1, \ldots, n\}$. Функция $f : H(n, q) \longrightarrow \mathbb{R}$ называется *собственной функцией* графа $H(n, q)$, отвечающей собственному значению λ, если $Af = \lambda f$, где A — матрица смежности $H(n, q)$. Собственную функцию графа $H(n, q)$, отвечающую собственному значению λ_m, обозначим через f_m.

Пусть $f : H(n,q) \longrightarrow \mathbb{R}$. Множество $S(f) = \{x \in H(n,q) | f(x) \neq 0)\}$ называется *носителем функции* f. Для носителя собственной функции известна следующая нижняя оценка:

Теорема 1 [2]. *Пусть* $f_m : H(n,q) \longrightarrow \mathbb{R}$ *и* $f_m \not\equiv 0$. *Тогда* $|S(f_m)| \geqslant 2^m(q-2)^{n-m}$ *для* $\frac{mq^2}{2n(q-1)} > 2$ *и* $|S(f_m)| \geqslant q^n(\frac{1}{q-1})^{m/2}(\frac{m}{n-m})^{m/2}(1-\frac{m}{n})^{n/2}$ *для* $\frac{mq^2}{2n(q-1)} \leqslant 2$.

Из результатов работы [3] следует, что для мощности носителя собственной функции $f : H(n,q) \longrightarrow \{-1,0,1\}$, отвечающей собственному значению $\lambda = q(n-m)-n$, выполнена нижняя оценка $|S(f)| \geqslant 2^m$.

Функцию $f : H(2,q) \longrightarrow \mathbb{R}$, для которой $f(x) = 1$ при $x = (k,j)$ для всех $k \neq i$ и $f(x) = -1$ при $x = (i,t)$ для всех $t \neq j$, и $f(x) = 0$ для остальных x, обозначим через $a_{i,j}(q)$.

Основной результат работы состоит в нахождении минимального носителя собственной функции графа Хэмминга $H(2,q)$ с собственным значением $q-2$, а также минимального носителя собственной функции графа Хэмминга $H(3,q)$ с собственным значением $q-3$. Кроме того, найдена полная характеризация соотвествующих собственных функций с минимально возможным носителем.

Теорема 2. *Пусть* $f_{q-2} : H(2,q) \longrightarrow \mathbb{R}$ *и* $f_{q-2} \not\equiv 0$. *Тогда* $|S(f_{q-2})| \geqslant 2(q-1)$. *Более того, если* $|S(f_{q-2})| = 2(q-1)$, *то* f_{q-2} *с точностью до умножения на константу совпадает с функцией* $a_{i,j}(q)$ *для некоторых* i *и* j.

Теорема 3. *Пусть* $f_{q-3} : H(3,q) \longrightarrow \mathbb{R}$ *и* $f_{q-3} \not\equiv 0$. *Тогда* $|S(f_{q-3})| \geqslant 4(q-1)$. *Более того, если* $|S(f_{q-3})| = 4(q-1)$, *то существуют числа* t_1, t_2, i *и* j *такие, что* f_{q-3} *с точностью до умножения на константу и перестановки координат равна* $a_{i,j}(q)$ *для* $x = (a,b,t_1)$, *равна* $-a_{i,j}(q)$ *для* $x = (a,b,t_2)$ *и равна* 0 *в остальных случаях.*

Исследование выполнено за счет гранта Российского научного фонда (проект №14-11-00555).

Список литературы

1. Воробьев К. В, Кротов Д. С. Оценки мощности минимального 1-совершенного битрейда в графе Хэмминга // Дискретн. анализ и исслед. опер. — 2014. — Т. 21, вып. 6. — С. 3–10.
2. Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования. — М.: Мир, 1976.
3. Potapov V. N. On perfect 2-colorings of the q-ary n-cube // Discrete Math. — 2012. — V. 312, N. 8. — P. 1269–1272.

О ЦИРКУЛЯНТАХ ДЕЗА

А. Л. Гаврилюк[1], С. В. Горяинов[1,2], Л. В. Шалагинов[2]
([1]Екатеринбург, [2]Челябинск)

Введение

В 1998 году в работе [1] впервые было рассмотрено естественное обобщение понятия сильно регулярного графа — графы Деза. Граф Деза называется точным графом Деза, если не является сильно регулярным и имеет диаметр 2. Авторы указали на базовые соотношения в графах Деза и предложили несколько конструкций.

В ряде исследований было выяснено, что графы Деза наследуют некоторые свойства сильно регулярных графов. Например, в [2] показано, что вершинная связность графа Деза, полученного из сильно регулярного графа с помощью инволюции, совпадает с валентностью.

Однако, данное обобщение приводит и к потере части свойств. Например, в [3] было показано, что существует граф Деза, имеющий сколь угодно большое число различных собственных значений.

Изучение некоторых классов графов, которые также являются графами Кэли, — популярная тема на стыке теории графов и теории групп. Например, одним из направлений исследования сильно регулярных графов является изучение сильно регулярных графов, являющихся графами Кэли. В [4], [5] и [6] независимо была получена классификация сильно регулярных графов Кэли над циклическими группами. В [7] была получена классификация сильно регулярных графов Кэли над $\mathbb{Z}_{p^n} \bigoplus \mathbb{Z}_{p^n}$. В [8] и [9] были классифицированы дистанционно регулярные графы Кэли над циклическими и диэдральными группами.

Для графов Деза, как для графов, «родственных» сильно регулярным, представляет интерес постановка аналогичных вопросов.

Проблемой, на решение которой направлена данная работа, является получение классификации точных графов Деза, являющихся графами Кэли.

Первые результаты по точным графам, которые являются графами Кэли, с помощью компьютерного перебора были получены в [10]. В статье для каждой конечной группы, имеющей порядок менее 60, приводится классификация с точностью до изоморфизма точных графов Деза, которые являются графами Кэли данной группы. Предметом дальнейших исследований является изучение вопроса о том, могут ли найденные графы быть вложены в серии.

В данной работе приводятся промежуточные результаты для класса точных графов Деза, которые являются графами Кэли циклических групп. Авторами доклада с помощью компьютерного перебора была получена классифи-

кация точных графов Деза, являющихся графами Кэли циклических групп и имеющих не более 95 вершин. За исключением двух графов, имеющих 8 и 9 вершин, каждый точный граф Деза, являющийся графом Кэли циклической группы и имеющий не более 95 вершин, является представителем одной из шести серий, две из которых являются новыми.

1. Основные определения и обозначения

Мы рассматриваем неориентированные графы без петель и кратных ребер.

Для графа Γ и его произвольной вершины x определим окрестность $\Gamma(x)$ вершины x как множество $\Gamma(x) := \{y \mid y \in V(\Gamma), y \sim x\}$.

Граф Γ называется регулярным валентности k, если для любой вершины $x \in \Gamma$ выполняется $|\Gamma(x)| = k$.

Граф Γ называется сильно регулярным с параметрами (v, k, λ, μ), если Γ имеет v вершин, регулярен валентности k и для любой пары различных вершин $x, y \in \Gamma$ выполняется:

$$|\Gamma(x) \cap \Gamma(y)| = \begin{cases} \lambda, & \text{если } x \sim y, \\ \mu, & \text{если } x \nsim y. \end{cases}$$

Граф Γ называется графом Деза с параметрами (v, k, b, a) (обычно принимается, что $b \geqslant a$), если Γ имеет v вершин, регулярен валентности k и любые две различные вершины $x, y \in \Gamma$ имеют либо a, либо b общих соседей.

Граф Деза называется точным графом Деза, если не является сильно регулярным и имеет диаметр 2.

Пусть G — конечная группа. Пусть S — непустое подмножество в G, не содержащее нейтральный элемент группы и замкнутое относительно операции обращения (т. е. $1_G \notin S$ и $\forall s \in S \Rightarrow s^{-1} \in S$). Граф $Cay(G, S)$, построенный на элементах группы G с правилом смежности

$$x \sim y \Leftrightarrow xy^{-1} \in S, \quad \forall x, y \in G,$$

называется графом Кэли группы G с системой образующих S.

Граф Кэли циклической группы называется циркулянтом.

Проблема: Классифицировать точные циркулянты Деза.

Пусть $\Gamma_1 = (V_1, E_1)$ и $\Gamma_2 = (V_2, E_2)$ графы. Композицией $\Gamma_1[\Gamma_2]$ графов Γ_1 и Γ_2 называется граф с множеством вершин $V_1 \times V_2$ и правилом смежности

$$(x_1, x_2) \sim (y_1, y_2) \Leftrightarrow (x_1 \sim y_1 \text{ ИЛИ } (x_1 = y_1 \text{ И } x_2 \sim y_2)).$$

Пусть $\Gamma_1 = (V_1, E_1)$ и $\Gamma_2 = (V_2, E_2)$ графы. Прямым произведением $\Gamma_1 \times \Gamma_2$ графов Γ_1 и Γ_2 называется граф с множеством вершин $V_1 \times V_2$ и правилом смежности

$$(x_1, x_2) \sim (y_1, y_2) \Leftrightarrow ((x_2 = y_2 \text{ И } x_1 \sim y_1) \text{ ИЛИ } (x_1 = y_2 \text{ И } x_2 \sim y_2)).$$

Матрица H размера $m \times m$ с элементами из множества $\{1, -1\}$ называется матрицей Адамара, если $HH^T = mI_m$, где I_m — единичная матрица размера $m \times m$.

Пусть F_q — конечное поле и $q \equiv 1(4)$. Пусть $S_q := \{x^2 \mid x \in F_q^*\}$. Графом Пэли $Paley(q)$ называется граф $Cay(F_q^+, S_q)$.

Пусть V — множество мощности v. Пусть $\mathcal{R}$ — разбиение множества $V \times V$ на $d+1$ бинарных отношений $R_0, R_1, \ldots, R_d$ со свойствами:

- $R_0 = \{(x, x) \mid x \in V\}$,
- $\forall i$: $R_i^\top = \{(y, x) \mid (x, y) \in R_i\}$ является элементом разбиения $\mathcal{R}$,
- если $(x, y) \in R_k$, то число элементов z, таких, что $(x, z) \in R_i$ и $(z, y) \in R_j$ является константой p_{ij}^k.

Тогда $\mathcal{R}$ называется схемой отношений с d классами.

Пусть q — нечетная степень простого, и e — делитель $q-1$. Пусть α — примитивный элемент поля F_q. Пусть $\langle \alpha^e \rangle$ подгруппа индекса e в $\mathbb{F}_q^*$, $\alpha^i \langle \alpha^e \rangle$, $(0 \leqslant i \leqslant e-1)$ — соответствующие смежные классы. Определим $R_0 = \{(x, x) \mid x \in \mathbb{F}_q\}$ и $R_i = \{(x, y) \mid x - y \in \alpha^i \langle \alpha^e \rangle, x, y \in \mathbb{F}_q\}$ $(1 \leqslant i \leqslant e)$. Тогда $(V, \mathcal{R}) = (\mathbb{F}_q, \{R_i\}_{i=0}^e)$ образуют схему отношений, которая называется циклотомической с e классами над $\mathbb{F}_q$.

2. Результаты

В данном разделе в теоремах 1–6 приводятся конструкции серий точных циркулянтов Деза. Теорема 7 соотносит результаты перечисления с помощью компьютера точных циркулянтов Деза, имеющих не более 95 вершин с приведенными конструкциями.

Теорема 1. *Пусть K_x — клика размера $x \geqslant 2$ и yK_2 — граф, являющийся объединением $y \geqslant 2$ изолированных ребер. Тогда граф $K_x[yK_2]$ является точным циркулянтом Деза.*

Теорема 2. *Пусть K_n — клика размера $n \geqslant 3$ и n — нечетно. Тогда граф $K_n \times K_4$ является точным циркулянтом Деза.*

Теорема 3. *Пусть* $H := \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix}$ *— матрица Адамара.*

Пусть $n \geqslant 3$ — нечетное число. Пусть I_n — единичная матрица размера $n \times n$ и $\overline{I}_n := J_n - I_n$, где J_n — матрица размера $n \times n$, состоящая из единиц. Пусть Γ_n — граф, матрица смежности которого получается из матрицы H заменой 1 на I_n и -1 на $\overline{I}_n$. Тогда граф Γ_n является точным циркулянтом Деза.

Теорема 4. *Пусть* Γ *— точный циркулянт Деза, имеющий* $2p$ *вершин, где* p *— простое, тогда* Γ *изоморфен* $Paley(p)[K_2]$*, при этом* $p \equiv 1(4)$.

Теорема 5. *Пусть* q *— степень простого, и* $\mathcal{S}$ *— циклотомическая схема с* 3*-мя классами над* $\mathbb{F}_q$*. Пусть* $F \subset \{1, 2, 3\}$.

Граф с матрицей смежности $A_F = \sum_{f \in F} A_f$ *является точным циркулянтом Деза тогда и только тогда* q*, когда* q *— простое и выполняется один из следующих случаев*:

- $|F| = 1$ *и* $q = x^2 + 3$ *для некоторого целого* x*,*
- $|F| = 2$ *и* $q = x^2 + 12$ *для некоторого целого* x.

Теорема 6 (совместно с Г. С. Исаковой). *Пусть* q_1*,* q_2 *— нечетные простые и* $q_2 - q_1 = 4$*. Пусть*

- $S_{q_1} := \{x^2 \mid x \in \mathbb{F}_{q_1}^*\}$ *и, аналогично,* S_{q_2}*,*
- $\overline{S}_{q_1} = \mathbb{F}_{q_1}^* \setminus S_{q_1}$ *и, аналогично,* $\overline{S}_{q_2}$.

Пусть $S_0 = \{(0, x) \mid x \in \mathbb{F}_{q_2}^*\}$*,* $S_1 = S_{q_1} \times \overline{S}_{q_2}$*,* $S_2 = \overline{S}_{q_1} \times S_{q_2}$*. Тогда* $Cay(\mathbb{F}_{q_1}^+ \times \mathbb{F}_{q_2}^+, S_0 \cup S_1 \cup S_2)$ *— точный циркулянт Деза.*

Теорема 7. *Пусть* Γ *— точный циркулянт Деза, имеющий не более* 95 *вершин, тогда* Γ *изоморфен либо* $Cay(\mathbb{Z}_8, \{\pm 1, \pm 2\})$*, либо* $Cay(\mathbb{Z}_9, \{\pm 1, \pm 2\})$*, либо графу из шести описанных серий.*

Список литературы

1. Erickson M., Fernando S., Haemers W.H., Hardy D. and Hemmeter J. Deza graphs: a generalization of strongly regular graphs // J. Comb. Designs. — 1999. — Vol. 7. — Pp. 359–405.
2. Гаврилюк А. Л., Горяинов С. В., Кабанов В. В. О вершинной связности графов Деза // Тр. Ин-та математики и механики УрО РАН. — 2013. — Т. 19, № 3 — С. 94–104.
3. Гаврилюк А. Л., Шалагинов Л. В. О графах Деза с 4-мя различными собственными значениями // Тезисы Международной (43-ей Всероссийской) молодежной школы-конференции. Екатеринбург, 2012. — С. 20–23.
4. Bridges W. G., Mena R. A. Rational circulants with rational spectra and cyclic strongly regular graphs // Ars Combin. — 1979. — Vol. 8. — Pp. 143–161.
5. Hughes D. R., van Lint J. H., Wilson R. M. Unpublished Manuscript (announcement at the 7th British Combinatorial Conference) // Cambridge, 1979.
6. Ma S. L. Partial differences sets // Discrete Math. — 1984. — Vol. 72. — Pp. 75–89.

7. Leifman Y. I., Muzychuk M. E. Strongly regular Cayley graphs over the group $\mathbb{Z}_{p^n} \bigoplus \mathbb{Z}_{p^n}$ // Discrete Math. — 2005. — Vol. 305. — Pp. 219–239.
8. Miklavic S., Potocnik P. Distance-regular circulants // Eur. J. Combin. — 2003. — Vol. 24. — Pp. 777–784.
9. Miklavic S., Potocnik P. Distance-regular Cayley graphs on dihedral groups // Journal of Combinatorial Theory, Series B. — 2007. — Vol. 97. — Issue 1. — Pp. 14–33.
10. Горяинов С. В., Шалагинов Л. В. Кэли–Деза графы, имеющие менее 60 вершин // Сиб. электрон. матем. изв. — 2014. — Т. 11. — С. 268–310.

О ПОВЕДЕНИИ ФУНКЦИИ ШЕННОНА ДЛЯ ОБОБЩЕННОЙ ГЛУБИНЫ СХЕМ В МОДЕЛИ, ГДЕ ГЛУБИНА МЕЖЭЛЕМЕНТНОГО СОЕДИНЕНИЯ ОПРЕДЕЛЯЕТСЯ НАДСХЕМОЙ ОГРАНИЧЕННОГО РАЗМЕРА

Б. Р. Данилов (Москва)

В настоящей работе рассматривается массовая задача синтеза асимптотически оптимальных по глубине в худшем случае схем из функциональных элементов (далее СФЭ или просто схем) над конечным полным базисом Б, состоящим из функциональных элементов (ФЭ) $\mathcal{E}_1, \ldots, \mathcal{E}_b$, которые реализуют соответственно функции алгебры логики (ФАЛ) $\varphi_1(x_1, \ldots, x_{k_1}), \ldots, \varphi_b(x_1, \ldots, x_{k_b})$, существенно зависящие при $k_i \geqslant 2$, $1 \leqslant i \leqslant b$, от всех своих булевых переменных. Рассматривается одно из возможных обобщений понятия глубины схем рассматриваемого класса. Получены асимптотические оценки функции Шеннона $D_{\text{Б}}(n)$ для обобщенной глубины функций из класса $P_2(n)$ ФАЛ, зависящих от переменных $x_1, \ldots, x_n$, при их реализации схемами над базисом Б и обобщенной глубины $D_{\text{Б}}(\mu_n)$ мультиплексорной[1] функций μ_n порядка n, в некоторых случаях имеющие так называемую высокую степень точности. При этом под глубиной $D_{\text{Б}}(f)$ ФАЛ f при ее реализации схемами над базисом Б традиционно понимается глубина наименьшей по глубине такой схемы ее реализующей.

Классическое понятие глубины СФЭ — наибольшее количество ФЭ на ориентированных путях графа схемы, начинающихся от входов и заканчивающихся ее выходами. Одно из первых обобщений понятия глубины предложил О. Б. Лупанов в работе [1], где глубина каждого ФЭ базиса задавалась

[1]Мультиплексорной функцией порядка n называется ФАЛ с n адресными и 2^n информационными переменными, равная той информационной переменной, номер которой задается в двоичной системе счисления набором значений адресных переменных.

положительным действительным числом. О. Б. Лупанов изучал только так называемые правильные схемы, но если рассматривать вариант обобщенной глубины [1], не принимая во внимание правильность схем и определять глубину геометрическим образом, подобно тому как это сделано в [2], то для так определенной глубины из работы [1] вытекают асимптотические соотношения:

$$D_{\text{Б}}(n) = \tau_{\text{Б}} n \pm O(\log n), \tag{1}$$

$$D_{\text{Б}}(\mu_n) = \tau_{\text{Б}} n \pm O(\log n), \tag{2}$$

где $\tau_{\text{Б}}$ — константа, определяемая характеристиками ФЭ базиса Б. В работе [2] установлены оценки высокой степени точности вида:

$$D_{\text{Б}}(n) = \tau_{\text{Б}}(n - \log_2 \log_2 n) \pm O(1), \tag{3}$$

$$D_{\text{Б}}(\mu_n) = \tau_{\text{Б}} n \pm O(1). \tag{4}$$

Различные способы обобщения понятия глубины нам удобно называть *моделями* глубины СФЭ. В работе [3] была рассмотрена одна из таких моделей, продолжающая понятие глубины [2], где для рассматриваемой там обобщенной глубины установлено асимптотическое поведение функций $D_{\text{Б}}(n)$, $D_{\text{Б}}(\mu_n)$ вида $\tau_{\text{Б}} n$, а константа $\tau_{\text{Б}}$ по-прежнему определяется характеристиками элементов базиса и совпадает с одноименной величиной определенной выше, когда базис Б является базисом типа [2]. При этом в [3] для *равномерных по глубине* базисов, глубины которых удовлетворяют некоторым ограничениям, установлены асимптотические оценки высокой степени точности вида (3), (4). Если в модели [3] ограничиться рассмотрением целочисленных значений глубин, то из результатов работы [4] без каких-либо дополнительных ограничений на эти величины следуют оценки (1), (2).

Рассматриваемый в настоящей работе вариант модели обобщенной глубины СФЭ продолжает обобщения [1, 2, 3]. Заметим, что для задания модели глубины СФЭ типа моделей, рассматриваемых в работах [2, 3], достаточно указать способ, который позволяет каждому входу каждого ФЭ любой схемы приписать положительное число — его глубину. После этого глубина схемы в заданной таким образом модели определяется через глубину ее *инициальных цепей* — одновыходных подсхем без висячих вершин, в которых у каждого ФЭ выделен ровно один вход, а соединения элементов осуществляются только через выделенные входы. Под *глубиной инициальной цепи* мы понимаем сумму глубин, приписанных ее выделенным входам, а *глубина схемы* — это наибольшая глубина ее инициальных цепей. Например, если в любой схеме входам ФЭ приписать число 1, то мы придем к классической модели глубины схем. Глубину в такой классической модели будем также называть *структурной глубиной* схемы, чтобы отделить это понятие от различных его обобщений.

Назовем формулу *абсолютной*, если каждая ее переменная входит в эту формулу ровно один раз. Две формулы назовем *конгруэнтными*, если они по-

лучаются друг из друга переименованием вхождений переменных. Рассмотрим класс $\mathcal{F}$ всех абсолютных конгруэнтных друг другу формул над базисом Б, структурная глубина которых не превосходит константы c. Будем называть $\mathcal{F}$ *типом* всех тех (одновыходных) схем, которые приводятся поднятием ветвлений выходов ФЭ к (не обязательно абсолютной) формуле конгруэнтной формулам этого класса. Будем говорить, что к ФЭ E в содержащей его схеме Σ по выделенному входу *подключена надсхема типа* $\mathcal{F}$, если наибольшая по включению одновыходная подсхема схемы Σ без висячих вершин, выход которой поступает в схеме Σ на выделенный вход элемента E, а структурная глубина которой не превосходит c, имеет тип $\mathcal{F}$.

Если теперь зафиксировать величину c и, подобно количеству b элементов базиса Б, считать эту константу неотъемлемой характеристикой базиса, то указанных выше типов одновыходных схем будет конечное число. Для каждого такого типа $\mathcal{F}$ и ФЭ $\mathcal{E}_i$, $1 \leqslant i \leqslant b$, мы обозначим через $D_{i,j,\mathcal{F}}$ положительное число — *обобщенную глубину* указанного ФЭ по входу с номером j, $1 \leqslant j \leqslant k_i$, когда к этому входу подключена надсхема типа $\mathcal{F}$. Набор всех таких чисел $D_{i,j,\mathcal{F}}$ полностью определяет глубину каждого входа каждого ФЭ в любой схеме и таким образом задает модель обобщенной глубины СФЭ над базисом Б. Указанный набор чисел мы традиционно включаем в определение базиса Б, считая два базиса различными не только когда они отличаются наборами своих ФЭ, но и тогда когда они различны лишь по своим сложносным характеристикам. При ссылке на модель глубины рассматриваемого типа (также как и на связанный с ней базис) будем иногда в качестве уточнения называть ее моделью (соответственно базисом), в которой глубина межэлементного соединения определяется надсхемой ограниченного размера. Заметим, что модели глубины [2, 3] можно рассматривать как частный случай описанной здесь конструкции: для базисов типа [3] константа c равна единице, а для базисов типа [2] — нулю, кроме того в последнем случае глубины ФЭ не зависят от номеров входов. При этом понятие равномерного по глубине базиса из [3] переносится на описанную здесь модель следующим образом: базис Б — *равномерный*, когда для любых указанных выше типа $\mathcal{F}$ и числа i выполняются соотношения $D_{i,1,\mathcal{F}} = \cdots = D_{i,k_i,\mathcal{F}}$.

Результатом настоящей работы являются теоремы 1, 2, в которых константа $\tau_{\text{Б}}$ однозначно задается набором глубин базиса Б и для базисов вида [2] или вида [3] совпадает с одноименными величинами упоминавшимися ранее.

Теорема 1. *Для любого* (*конечного, полного*) *базиса* Б *с целочисленными глубинами, в котором глубина межэлементного соединения определяется надсхемой ограниченного размера, выполняются асимптотические оценки* (1), (2).

Теорема 2. *Для равномерного по глубине* (*конечного, полного*) *базиса* Б *с действительными глубинами, в котором глубина межэлементного соеди-*

нения определяется надсхемой ограниченного размера, выполняются асимптотические оценки высокой степени точности (3), (4).

Заметим, что в рассматриваемой здесь модели обобщенной глубины поднятие ветвлений выходов ФЭ к входам схемы не изменяет глубины схем и поэтому достаточно ограничиться изучением схем формульного типа (формул) в базисе Б. *Ранг* формулы — это количество дуг, исходящих из входов, при ее схемном представлении. Путь к нахождению асимптотических оценок для $D_{\text{Б}}(n)$, $D_{\text{Б}}(\mu_n)$ лежит через получение оценок для так называемой *ранговой функции* $R_{\text{Б}}(t)$ базиса Б действительного аргумента, равной наибольшему рангу формул над Б глубины, не превосходящей t. При этом величина $\tau_{\text{Б}}$, которая традиционно называется *приведенной глубиной* базиса Б, задается через ранговую функцию базиса Б соотношением:

$$\tau_{\text{Б}} = \lim_{t\to+\infty} \frac{t}{\log R_{\text{Б}}(t)}. \tag{5}$$

В работе [4] для модели глубины [3] с целочисленными глубинами получена асимптотическая оценка следующего вида:

$$R_{\text{Б}}(t) = h(t)2^{\frac{t}{\tau_{\text{Б}}}} + o\big(2^{\frac{t}{\tau_{\text{Б}}}}\big), \tag{6}$$

где $h(t) = O(t^q)$ для некоторой целочисленной неотрицательной константы q которая зависит от базиса Б. Соотношение (6) позволяет в рассматриваемом случае с использованием мощностного метода и методов [2] подобно тому как это сделано в [3] получить необходимые нижние и верхние оценки (1), (2). Если в асимптотической оценке (6) $h(t) = O(1)$, как это имеет место для равномерных по глубине базисов из работы [3], то использование указанных выше методов приводит нас к асимптотическим оценкам высокой степени точности (3), (4). Следующая лемма позволяет аналогичным образом доказать теоремы 1, 2.

Лемма 1. *Пусть в (конечном, полном) базисе* Б *глубина межэлементного соединения определяется надсхемой ограниченного размера. Тогда если глубины базиса* Б *являются целыми числами, то для ранговой функции* $R_{\text{Б}}(t)$ *базиса* Б *выполняются соотношения* (6), *в которых для некоторого целого неотрицательного числа* q *справедливо* $h(t) = O(t^q)$. *Если же базис* Б *равномерен по глубине, то независимо от целочисленности его глубин в соотношениях* (6) $h(t) = O(1)$.

Для доказательства леммы 1 используется подход [3] к определению аналогичных (6) асимптотических оценок ранговой функции подмножеств множества всех формул над Б определенного вида, которыми описывается множество формул последовательности, определяющей значение предела (5). Ранговая функция $R_{\mathfrak{S}}(t)$ множества $\mathfrak{S}$ формул над Б определяется аналогич-

но $R_{\text{Б}}(t)$ за тем уточнением, что указанные в ее определении формулы пробегают лишь множество $\mathfrak{S}$. Само множество формул $\mathfrak{S}$ совпадает с множеством корневых поддеревьев бесконечного информационного (ориентированного корневого) дерева, узлами которого являются ФЭ базиса Б. Указанное информационное дерево упрощается при помощи операции отождествления эквивалентных вершин до конечного или бесконечного ориентированного упорядоченного графа $\mathcal{S}$, который мы называем *шаблоном подключений*. Когда шаблон подключений конечен, его можно тарктовать как СФЭ с обратными связями над базисом Б. В случае, когда количество вершин r шаблона $\mathcal{S}$ конечно, он называется *однородным*. Вершины шаблона $\mathcal{S}$ нумеруются натуральными числами так, чтобы корню информационного дерева соответствовала вершина с номером один. Выделяя в $\mathcal{S}$ вершину с номером i мы порождаем множество формул $\mathfrak{S}_i$, причем $\mathfrak{S} = \mathfrak{S}_1$. Функции $R_{\mathfrak{S}_1}(t), R_{\mathfrak{S}_2}(t), \ldots$ связаны между собой системой линейных однородных конечноразностных уравнений

$$R_{\mathfrak{S}_i}(t) = \sum_{j=1}^{k_i} \sum_{s=1}^{r} \varepsilon_{ij}^{(s)} R_{\mathfrak{S}_s}\big(t - D_{\eta_i,j,\mathcal{F}_s}\big) \qquad (t \geqslant \max_{i,j,\mathcal{F}} D_{i,j,\mathcal{F}}), \tag{7}$$

где η_i — тип ФЭ приписанного в шаблоне $\mathcal{S}$ вершине номер i, $\mathcal{F}_s$ — тип максимальной по включению подсхемы шаблона $\mathcal{S}$, структурная глубина которой не превосходит c и выходом которой является выход ФЭ, связанного в $\mathcal{S}$ с вершиной номер s, а $\varepsilon_{ij}^{(s)} = 1$, если в $\mathcal{S}$ дуга с номером j ведет из вершины номер i в вершину номер s, и $\varepsilon_{ij}^{(s)} = 0$ иначе. Для однородных шаблонов подключений асимптотическое поведение решения системы (7) находится [3] при помощи спектральной теории Перрона неотрицательных матриц. Для неоднородного шаблона $\mathcal{S}$ в случае целочисленных глубин ФЭ базиса Б асимптотическое поведение решений системы (7) находится с использованием обобщений [5, 6] теории неотрицательных матриц.

Список литературы

1. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — 1970. — С. 43–82.
2. Ложкин С. А. О глубине функций алгебры логики в произвольном полном базисе // Вестник Московского университета. Серия 1. Математика. Механика. — 1996. — № 2. — С. 80–82.
3. Данилов Б. Р. О поведении функции Шеннона для задержки схем в модели, где задержка соединений определяется типами соединяемых элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2014. — Т. 3, № 31. — С. 78–100.
4. Данилов Б. Р. Асимптотическое поведение ранговой функции базиса для модели обобщенной целочисленной глубины схем из функциональных элементов // Труды IX международной конференции (Москва и Подмосковье, 20–22 мая 2015 г.). — М.: МАКС Пресс, 2015. — С. 70–72.

5. Vere-Jones D. Ergodic properties of nonnegative matrices // Pacific Journal of Mathematics. — 1967. — V. 22, N 2 — P. 361–386.
6. Seneta E. Non-negative matrices and Markov chains. — Springer, 2006. — P. 199–220.

СИНТЕЗ И СЛОЖНОСТЬ ДИЗЪЮНКТИВНЫХ ДЕШИФРАТОРНЫХ СХЕМ КОНТАКТНОГО ТИПА

Д. И. Добровецкий, С. А. Ложкин (Москва)

Введение

При синтезе контактных схем возникает задача реализации произвольного (m,n)-дизъюнктивного дешифратора (ДД), т. е. системы из m различных элементарных дизъюнкций, существенно зависящих от переменных $x_1,\dots,x_n$, с помощью контактного $(1,m)$-полюсника, проводимость между единственным входом и i-м выходом которого, где $i=1,\dots,m$, равна i-й дизъюнкции данной системы. Обозначим через $L_\vee(m,n)$ наименьшее число контактов, достаточное для реализации произвольного (m,n)-ДД, который в случае $m=2^n$ будем считать полным ДД порядка n.

Очевидно, что $L_\vee(m,n)\geqslant m$ так как любой связный контактный $(1,m)$-полюсник содержит по крайней мере m контактов, если он реализует систему из m различных функций алгебры логики (ФАЛ), отличных от констант. Известно также (см. лемму из п. 1), что $L_\vee(m,n)\geqslant 2m-\frac{m}{2^{n-1}}$.

Заметим, что для полного ДД порядка n, согласно [1], справедливо асимптотическое равенство[1] $L_\vee(2^n,n)\sim 2^{n+1}$. При этом из [1] следует также, что $L_\vee(m,n)\sim 2m$, если $m=m(n)$ и $\frac{2^n}{n}=o(m(n))$.

К проблеме получения верхних оценок для величины $L_\vee(m,n)$ при $m=O(\frac{2^n}{n})$, мы подойдем на основе известных верхних оценок аналогичной величины $L_\&(m,n)$ для (m,n)-конъюнктивного дешифратора (КД), которым посвящено много работ. Впервые задача синтеза схемы для реализации всех элементарных конъюнкций ранга n от n переменных была поставлена в 1949 г. К. Шенноном [2]. В этой работе он получил оценку

$$L_\&(2^n,n)\leqslant 2^{n+1}-2,$$

построив искомую схему в виде контактного дерева.

[1] Асимптотическое неравенство $a(n)\leqslant b(n)$ для двух указанных функций натурального аргумента $n=1,2,\dots$, понимается как неравенство вида $a(n)\leqslant b(n)\cdot(1+\epsilon(n))$, где $\epsilon(n)\to 0$ при $n\to\infty$. При этом асимптотическое равенство $a(n)\sim b(n)$ означает, что $a(n)\leqslant b(n)\cdot(1+\epsilon(n))$ и $a(n)\geqslant b(n)\cdot(1+\epsilon(n))$.

О. Б. Лупанов улучшил эту оценку, показав [3], что

$$L_{\&}(2^n, n) \sim 2^n.$$

Задача синтеза (m, n)-КД, где $m < 2^n$, была впервые рассмотрена в 1969 г. Э. И. Нечипоруком [4], а затем ее исследовали Н. П. Редькин [5] и другие.

Главный результат, на котором основана первая часть данной работы, был получен И. А. Вихлянцевым [6]:

$$L_{\&}(m, n) \sim m$$

при $m \geqslant 2^{\log_2^3 n}$.

В настоящей работе установлено, что при $m \geqslant 2^{\log_2^3 n}$ справедливо асимптотическое равенство:

$$L_{\vee}(m, n) \sim 2m.$$

Установлено также, что сложности полных ДД порядка 2, 3 и 4 равны соответственно 6, 14 и 34.

Кроме того, во второй части работы рассмотрена сложность $L_{\vee}(n, p, q)$, которая равна минимальному числу контактов, достаточному для реализации полного ДД порядка n в классе контактных схем с $p, p \geqslant 1$, входами и $q, q \geqslant \frac{2^n}{p}$, отличными от них выходами как системы ФАЛ проводимости от входов к выходам. При этом доказано что

$$\min_{p \cdot q \geqslant 2^n} L_{\vee}(n, p, q) \sim 2^{n+1}.$$

Таким образом, при увеличении количества входов асимптотика сложности полного ДД порядка n не изменяется, что существенно отличает его от универсального контактного многополюсника порядка n, реализующего как функции проводимости между своими полюсами все функции от n переменных, или полного КД порядка n. Действительно, увеличивая число входов КС, порядок роста сложности первого из них при $n = 1, 2, \ldots$ можно уменьшить с 2^{2^n} до $2^{2^{n-1}}$, а второго — с 2^n до $2^{\frac{n}{2}}$

1. Основные понятия[1] и нижние оценки сложности реализации (m, n)-дизъюнктивных дешифраторов в классе $(1, m)$-контактных схем

Множество B^n, где $B = \{0; 1\}$ и $n = 1, 2, \ldots$, т. е. множество наборов длины n из 0 и 1, будем называть единичным кубом размерности n, а отображение $f : B^n \to B$ — функцией алгебры логики (ФАЛ) от булевых переменных (БП) $\{x_1, \ldots, x_n\} = X(n)$. При этом множество N_f наборов α, $\alpha \in B^n$, для которых $f(\alpha) = 1$, считается характеристическим множеством ФАЛ f. Множество всех ФАЛ от БП $X(n)$ обозначается как $P_2(n)$.

[1] Те понятия, которые здесь не определены, могут быть найдены, например, в [7].

Элементарная дизъюнкция (ЭД) ранга n от БП $X(n)$ определяется как ФАЛ вида

$$D = x_1^{\alpha_1} \vee \ldots \vee x_n^{\alpha_n},$$

где $\alpha_i = \{0, 1\}$ и $x_i^1 = x_i, x_i^0 = \overline{x_i}$. Заметим, что характеристическое множество указнной ЭД равно $B^n \backslash \{\alpha\}$, где $\alpha = (\overline{\alpha_1}, \ldots, \overline{\alpha_n})$ и напомним, что система из m различных ЭД ранга n от БП $X(n)$ называется (m, n)-дизъюнктивным дешифратором (ДД).

Неориентированный граф Σ с p входами и q отличными от них выходами, все ребра которого помечены БП $x_1, \ldots, x_n$ или их отрицаниями $\overline{x}_1, \ldots, \overline{x}_n$ называется (p, q)-контактной схемой (КС). Ребро или дуга КС с пометкой $x_i(\overline{x}_i)$ называется замыкающим (соответственно, размыкающим) контактом БП x_i. При этом число контактов называется сложностью КС Σ и обозначается через $L(\Sigma)$. Указанная КС Σ реализует систему (матрицу), составленную из всех ФАЛ проводимости от входов Σ к ее выходам.

Через $L_\vee(m, n)$ мы по-прежнему обозначаем наименьшее число контактов, достаточное для реализации произвольного (m, n)-ДД в классе $(1, m)$-контактных схем. Нижняя оценка данной величины получается, если к произвольному (m, n)-ДД J применить следующее утверждение, доказанное С. А. Ложкиным в [7]:

Лемма. *Если система ФАЛ $F = (f_1, \ldots, f_m)$ состоит из попарно различных ФАЛ от БП $X(n)$, отличных от* 0 *и* 1, *то для сложности реализующей ее $(1, m)$-КС справедливо неравенство*:

$$L(\Sigma) \geqslant 2^{1-n} \cdot \sum_{j=1}^{m} |N_{f_j}|.$$

Следствие. $L_\vee(m, n) \geqslant 2m - \frac{m}{2^{n-1}}$

Действительно, полагая $F = J$ и, учитывая, что при этом $|N_{f_j}| = 2^n - 1$ для всех $j = 1, \ldots, m$, мы получим $L(\Sigma) \geqslant 2^{1-n} m(2^n - 1) = 2m - \frac{m}{2^{n-1}}$.

2. Каскадные контактные схемы и верхние оценки сложности реализации (m, n)-дизъюнктивных дешифраторов в классе $(1, m)$-контактных схем

Определим, далее, (см. [7]) каскадную контактную схему (ККС) как приведенную КС без изолированных полюсов, которая может быть получена из системы тождественных вершин в результате ряда операций присоединения одного или двух противоположных контактов и операций переименования выходов. ККС считается полной, если она была построена без использования операции присоединения одного контакта. Вершина ККС, введенная в нее с помощью операции присоединения одного контакта, называется неполной вершиной этой ККС. Будем говорить, что ККС Σ'' является дополнением

неполной ККС Σ', если она получается в результате соединения всех неполных вершин Σ' отсутствующими в них контактами с новым входом, удаления всех «старых» входов и перехода к соответствующей приведенной КС. При этом, очевидно

$$L(\Sigma'') \leqslant 2 \cdot L(\Sigma').$$

Было доказано, что построенная в [5] КС, реализующая произволный (m,n)-КД Q со сложностью не больше, чем $m + o(m)$, является ККС. Таким образом, построив дополнительную КС к данной ККС, которая будет реализовывать (m,n)-ДД $J = \overline{Q}$, мы получим следующую оценку:

$$L_{\vee}(m,n) \leqslant 2 \cdot m + o(m).$$

Принимая во внимание нижнюю оценку следствия из леммы в п. 1, мы получаем следующие необходимые оценки сложности КС, реализующей произвольный (m,n)-ДД.

Теорема 1. *Если* $m \geqslant 2^{\log_2^3 n}$, *то*

$$L_{\vee}(m,n) \sim 2m.$$

Следующая теорема устанавливает точные значения сложности реализации полных ДД порядка 2, 3 и 4 в классе $(1,m)$-контактных схем.

Теорема 2. $L_{\vee}(4,2) = 6$, $L_{\vee}(8,3) = 14$, $L_{\vee}(16,4) = 34$.

3. Сложность реализации полных дизъюнктивных дешифраторов в классе (p,q)-контактных схем

Опираясь на введенные выше величины $L_{\vee}(n,p,q)$, положим:

$$\hat{L}_{\vee}(n) = \min_{p \cdot q \geqslant 2^n} L_{\vee}(n,p,q)$$

Пусть КС Σ является минимальной КС с p, $p \geqslant 1$, входами и q, $q \geqslant \frac{2^n}{p}$, отличными от них выходами, реализующей полный дизъюнктивный дешифратор от n переменных. Тогда сопоставим ей схему Σ', вершинами которой являются входные и выходные вершины схемы Σ, а ребрами соединяются те вход-выходные пары вершин, между которыми в схеме Σ реализуется какая-то ЭД ранга n от БП $X(n)$. Будем считать, что ребро в схеме Σ' проводит тогда и только тогда, когда сопоставляемая ему дизъюнкция обращается в 1.

Утверждение. *В схеме* Σ' *нет циклов.*

На основе данного утверждения устанавливается справедливость следующей теоремы.

Теорема 3. *Для полного дизъюнктивного дешифратора от n переменных,* $n = 1, 2 \ldots$, *справедлива следующая оценка*:

$$\hat{L}_{\vee}(n) \geqslant 2 \cdot 2^n - 2.$$

Следствие. *Так как, согласно* [1], $L_{\vee}(n, 1, 2^n) \sim 2^{n+1}$, *то*

$$\min_{p \cdot q \geqslant 2^n} L_{\vee}(n, p, q) \sim 2^{n+1}.$$

Работа выполнена при финансовой поддержке РФФИ, грант № 15-01-07474.

Список литературы

1. Ложкин С.А., Кошкин М.А. О сложности реализации некоторых систем функций алгебры логики контактными и обобщенными контактными схемами // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 257–287.
2. Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963.
3. Лупанов О. Б. О синтезе контактных схем // ДАН СССР. — 1958. — Т. 119, № 1. — С. 23–26.
4. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 5–102.
5. Редькин Н. П. О реализации систем конъюнкций контактными схемами // Проблемы кибернетики. Вып. 30. — М.:Наука, 1975. — С. 263–276.
6. Вихлянцев И. А. О реализации систем конъюнкций контактными схемами // Дискретная математика. — 1989. — Т. 1, вып. 4. — С. 3–11.
7. Ложкин С. А. Лекции по основам кибернетики. М.: МГУ, 2004.

О МИНИМИЗАЦИИ ПОЛНОЙ СИСТЕМЫ ТОЖДЕСТВ ДЛЯ ФОРМУЛ В СТАНДАРТНОМ БАЗИСЕ

В. В. Жуков (Москва)

Введение

В работе рассматривается вопрос построения полной системы тождеств для формул алгебры логики в стандартном базисе из дизъюнкции ($\vee$), конъюнкции ($\wedge$) и отрицания ($\neg$). Такие системы из восьми и пяти тождеств приведены, например, в [2] и [1] соответственно, а также известна полная система, состоящая всего лишь из трех тождеств. В работе строится полная система из двух тождеств, а затем она обобщается на случай формул k-значной алгебры логики в базисе Россера-Туркетта.

1. Основные определения

Определение 1. Формулы $\mathcal{F}_1$ и $\mathcal{F}_2$ называются эквивалентными, если они реализуют равные функции.

Определение 2. Равенство эквивалентных формул $t : \mathcal{F}_1 = \mathcal{F}_2$ называется тождеством.

Определение 3. Тождество $t' : \mathcal{F}'_1 = \mathcal{F}'_2$ называется подстановкой тождества $t : \mathcal{F}_1 = \mathcal{F}_2$, если оно получено заменой вхождений переменных в формулы $\mathcal{F}_1$ и $\mathcal{F}_2$ на некоторые формулы, причем каждое вхождение одной и той же переменной заменяется на одну и ту же формулу.

Определение 4. Однократным эквивалентным преобразованием формулы $\mathcal{G}$ с использованием тождества $t : \mathcal{F}_1 = \mathcal{F}_2$ называется замена подформулы $\mathcal{F}'_1$ формулы $\mathcal{G}$ на формулу $\mathcal{F}'_2$, где тождество $t' : \mathcal{F}'_1 = \mathcal{F}'_2$ является некоторой подстановкой тождества t. В результате получается некоторая формула $\mathcal{G}'$. Обозначение: $\mathcal{G} \xrightarrow{t} \mathcal{G}'$.

Определение 5. Множество тождеств $\tau = \{t_1, \ldots, t_n\}$ называется системой тождеств.

Определение 6. Тождество $t : \mathcal{F}_1 = \mathcal{F}_2$ называется выводимым при помощи системы тождеств τ, если существует последовательность однократных эквивалентных преобразований с использованием тождеств из системы τ, такая что при применении данной последовательности к формуле $\mathcal{F}_1$ получается формула $\mathcal{F}_2$.

Определение 7. Система тождеств τ называется полной, если любое тождество выводимо при помощи τ.

2. Полная система из двух тождеств

Как известно, существует полная конечная система τ из шести тождеств для формул в стандартном базисе (см. [1]). Каждое тождество в τ имеет вид $\mathcal{F}_1 = \mathcal{F}_2$. Заметим, что $\mathcal{F}_1 = \mathcal{F}_2$ тогда и только тогда, когда $\mathcal{F}_1\mathcal{F}_2 \vee \overline{\mathcal{F}_1}\ \overline{\mathcal{F}_2} = 1$.

Приступим к построению полной системы из двух тождеств. Каждое тождество $\mathcal{F}_{i_1} = \mathcal{F}_{i_2}$ из системы τ запишем в виде $\mathcal{F}_{i_1}\mathcal{F}_{i_2} \vee \overline{\mathcal{F}_{i_1}}\ \overline{\mathcal{F}_{i_2}} = 1$, и обозначим $\mathcal{G}_i = \mathcal{F}_{i_1}\mathcal{F}_{i_2} \vee \overline{\mathcal{F}_{i_1}}\ \overline{\mathcal{F}_{i_2}}$. Введем также тождество ассоциативности t_a: $x_1(x_2x_3) = (x_1x_2)x_3$ и соответствующую формулу $\mathcal{G}_a = (x_1(x_2x_3))((x_1x_2)x_3) \vee \vee\ \overline{(x_1(x_2x_3))}\ \overline{((x_1x_2)x_3)}$. Запишем первое тождество:

$$t_1 : x = x(\mathcal{G}_1(\mathcal{G}_a(\mathcal{G}_2 \ldots (\mathcal{G}_{n-1}\mathcal{G}_n)\ldots)))).$$

Тождество t_1 верно, т. к. все $\mathcal{G}_i = 1$, а также $\mathcal{G}_a = 1$. Запишем второе тождество системы, справедливость которого также очевидна:

$$t_2 : x_1(x_3((x_1x_2 \vee \overline{x_1}\ \overline{x_2})x_4)) = x_2(x_3((x_1x_2 \vee \overline{x_1}\ \overline{x_2})x_4)).$$

Утверждение. *Система тождеств t_1, t_2 является полной для формул в стандартном базисе.*

Доказательство. Для краткости введем обозначения $\mathcal{F}_{a_1} = x_1(x_2x_3)$ и $\mathcal{F}_{a_2} = (x_1x_2)x_3$ и выведем с помощью тождеств t_1, t_2 тождество ассоциативности t_a:

$$\mathcal{F}_{a_1} \xrightarrow{t_1} \mathcal{F}_{a_1}(\mathcal{G}_1(\mathcal{G}_a(\mathcal{G}_2 \dots (\mathcal{G}_{n-1}\mathcal{G}_n)\dots)))) \xrightarrow{t_2} \\ \xrightarrow{t_2} \mathcal{F}_{a_2}(\mathcal{G}_1(\mathcal{G}_a(\mathcal{G}_2 \dots (\mathcal{G}_{n-1}\mathcal{G}_n)\dots)))) \xrightarrow{t_1} \mathcal{F}_{a_2}.$$

Теперь выведем тождества $\mathcal{F}_{i_1} = \mathcal{F}_{i_2}$ из системы τ, применяя тождества t_1, t_2, а также тождество ассоциативности t_a:

$$\mathcal{F}_{i_1} \xrightarrow{t_1} \mathcal{F}_{i_1}(\mathcal{G}_1(\mathcal{G}_a(\mathcal{G}_2 \dots (\mathcal{G}_{n-1}\mathcal{G}_n)\dots)))) \xrightarrow{t_a} \dots \xrightarrow{t_a} \\ \xrightarrow{t_a} \mathcal{F}_{i_1}((\mathcal{G}_1(\mathcal{G}_a \dots (\mathcal{G}_{i-2}\mathcal{G}_{i-1})\dots))(\mathcal{G}_i(\mathcal{G}_{i+1} \dots (\mathcal{G}_{n-1}\mathcal{G}_n)\dots)))) \xrightarrow{t_2} \\ \xrightarrow{t_2} \mathcal{F}_{i_2}((\mathcal{G}_1(\mathcal{G}_a \dots (\mathcal{G}_{i-2}\mathcal{G}_{i-1})\dots))(\mathcal{G}_i(\mathcal{G}_{i+1} \dots (\mathcal{G}_{n-1}\mathcal{G}_n)\dots)))) \xrightarrow{t_a} \dots \xrightarrow{t_a} \\ \xrightarrow{t_a} \mathcal{F}_{i_2}(\mathcal{G}_1(\mathcal{G}_a(\mathcal{G}_2 \dots (\mathcal{G}_{n-1}\mathcal{G}_n)\dots)))) \xrightarrow{t_1} \mathcal{F}_{i_2}.$$

Так как из системы тождеств t_1, t_2 выводимы все тождества полной системы тождеств τ, то система тождеств t_1, t_2 также является полной.

3. Полные системы тождеств для формул k-значной логики

Аналогичная задача возникает и для формул, которые реализуют функции k-значной алгебры логики. В данном случае формулы строятся в некотором полном базисе, состоящем из элементарных функций $\phi_1, \dots, \phi_n$.

Определение 8. Базис, состоящий из элементарных функций $\phi_1, \dots, \phi_n$, называется полным, если для любой функции f существует формула в данном базисе, реализующая функцию f.

В качестве примера полного базиса можно привести следующую систему функций Ψ (доказательство полноты см. [2]):

- Константы $0, 1, \dots, k-1$.
- Характеристическая функция $J_\sigma(x) = \begin{cases} 0, & x \neq \sigma \\ k-1, & x = \sigma \end{cases}$.
- Обобщенная конъюнкция $\min(x_1, x_2)$.
- Обобщенная дизъюнкция $\max(x_1, x_2)$.

Построим полную систему из двух тождеств таким же образом, как и в предыдущем параграфе. Для формул k-значной алгебры логики в полном базисе $\phi_1, \ldots, \phi_n$ существует полная конечная система тождеств τ (см. [2]). Выразим через функции $\phi_1, \ldots, \phi_n$ полного базиса обобщенную эквиваленцию

$$x_1 \sim x_2 = \begin{cases} 0, & x_1 \neq x_2 \\ k-1, & x_1 = x_2 \end{cases}$$

Например, в приведенном базисе Ψ

$$x_1 \sim x_2 = \max(\min(J_0(x_1), J_0(x_2)), \max(\min(J_1(x_1), J_1(x_2), \ldots, \\ \max(\min(J_{k-2}(x_1), J_{k-2}(x_2)), \min(J_{k-1}(x_1), J_{k-1}(x_2))) \ldots))$$

Для каждого тождества $\mathcal{F}_{i_1} = \mathcal{F}_{i_2}$ обозначим $\mathcal{G}_i = \mathcal{F}_{i_1} \sim \mathcal{F}_{i_2}$. Введем тождество ассоциативности для аналога конъюнкции t_a: $\min(x_1, \min(x_2, x_3)) = \min(\min(x_1, x_2), x_3)$ и для удобства обозначим $\mathcal{G}_a = \min(x_1, \min(x_2, x_3)) \sim \min(\min(x_1, x_2), x_3)$. Теперь запишем два искомых тождества и утверждение, доказательство которого аналогично доказательству утверждения из предыдущего пункта:

$$t_1 : x = \min(x, \min(\mathcal{G}_1, \min(\mathcal{G}_a, \min(\mathcal{G}_2, \ldots \min(\mathcal{G}_{n-1}, \mathcal{G}_n) \ldots))))),$$
$$t_2 : \min(x_1, \min(x_3, \min(x_1 \sim x_2, x_4))) = \min(x_2, \min(x_3, \min(x_1 \sim x_2, x_4))).$$

Утверждение. *Система тождеств t_1, t_2 является полной для формул в базисе $\phi_1, \ldots, \phi_n$.*

Замечание. Вообще говоря, аналогичным образом можно построить полную систему из двух тождеств для формул в любом базисе, в котором реализуема обобщенная конъюнкция и обобщенная эквиваленция, даже если этот базис не является полным.

Список литературы

1. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел Факультета ВМиК МГУ им. М. В. Ломоносова, 2004. — 256 с.
2. Яблонский С. В. Элементы математической кибернетики. — М.: Высшая школа, 2007. — 188 с.

СИНТЕЗ И СЛОЖНОСТЬ УНИВЕРСАЛЬНЫХ СХЕМ КОНТАКТНОГО ТИПА С РАЗДЕЛЕННЫМИ ПОЛЮСАМИ

В. С. Зиновьев (Москва)

1. Введение

В работе рассматривается задача о сложности совместной реализации «больших» систем функций алгебры логики контактными (p, q)-полюсниками, т. е. контактными схемами (КС) с p входами и q отличными от них выходами, в которых все функции данной системы реализованы как функции проводимости от входов КС к ее выходам. Такие КС будем считать КС с разделенными полюсами, чтобы выделить их из класса всех КС, допускающих, в общем случае, частичное или полное совпадение множества своих входов с множеством своих выходов. При этом в случае полного совпадения входов и выходов будем говорить о КС с неразделенными полюсами. Заметим, что оптимизировать схему по сложности очень важно, так как это позволяет уменьшить ее стоимость, размеры или потребляемую мощность СБИС.

Частным случаем указанной задачи является задача о нахождении сложности минимального универсального контактного многополюсника (УКМ), который вычисляет все функции алгебры логики от заданного количества переменных. В данной работе вводится и исследуется функция $L^K(p, q, n)$ равная минимальной из сложностей (p, q)-универсальных контактных многополюсников, где $p \cdot q \geqslant 2^{2^n}$, реализующих систему всех функций алгебры логики (ФАЛ) от n переменных. Напомним, что, как известно из [3], сложность $L^K(1, 2^{2^n}, n)$ асимптотически равна $2 \cdot 2^{2^n}$.

Эта же задача для класса контактных схем с 1 входом и отдельных систем ФАЛ рассматривалась в [4–7]. В этих работах были установлены асимптотические точные оценки сложности рассматриваемых систем функций в рамках данной модели. Оказалось, что для подавляющей части «больших» систем ФАЛ сложность их реализации в классе контактных схем с одним входом асимптотически равна удвоенному числу функций, входящих в этот класс. В частности, это верно для класса всех функций, класса всех самодвойственных функций, функций с фиксированным числом «1», а также для дизъюнктивного дешифратора. Заметим, что система всех элементарных конъюнкций ранга n от n переменных требует (асимптотически) для своей реализации всего лишь одного контакта на каждую функцию.

В настоящей работе устанавливается асимптотически точная оценка вида $2 \cdot (p+q)$ для функции $L^K(p, q, n)$, где $p = 2^l$, $q = 2^t$, и $l+t \geqslant 2^n$. Таким образом, в оптимальной контактной схеме рассматриваемого вида сложность универ-

сальной системы функций в исследуемом классе схем по-прежнему асимптотически в 2 раза больше числа полюсов. Путем перебора на компьютере доказано, что $L^K(p,q,2) \geqslant 10 = L^K(4,4,2)$ и что минимальная сложность УКМ от двух переменных с неразделенными полюсами равна 8.

2. Основные определения, постановка задачи и формулировка результатов

Напомним основные определения и введем обозначения, связанные с реализацией функций алгебры логики контактными схемами. Те понятия, которые здесь не определены, могут быть найдены, например, в [2, 4].

Определение 1. Пару $G = (V, E)$, где E — сочетание (с возможными повторениями) над множеством неупорядоченных пар из V, будем, как обычно, называть *графом с множеством вершин* $V = V(G)$ и *множеством ребер* $E = E(G)$.

Определение 2. Набор вида (G,V',V''), где G — граф,а V' и V'' — выборки из множества $V(G)$ длины p и q соответственно, причем выборка V' является выборкой без повторения, называется (p,q)-*сетью*, или, иначе, *сетью с* p *входами и* q *выходами*. Сеть Σ с входами $a_1',\ldots,a_p'$ и выходами $a_1'',\ldots,a_q''$, в которой все ребра помечены БП $x_1,\ldots,x_n$ или их отрицаниями $\overline{x_1},\ldots,\overline{x_n}$, называется (p,q)-*контактной схемой* (КС) от БП $x_1,\ldots,x_n$. При этом число контактов (ребер) КС Σ называется ее сложностью и обозначается $L(\Sigma)$. В том случае, когда множество входов и множество выходов КС Σ не пересекаются (совпадают как упорядоченные множества), будем считать ее КС с разделенными (соответственно неразделенными) полюсами. По умолчанию будем считать, что (p,q)-КС является КС с разделенными полюсами.

Определение 3. Пусть Σ — КС от БП $X(n)$ и $\alpha = (\alpha_1,\ldots,\alpha_n)$ — набор из B^n. Определим сеть $\Sigma|_\alpha$ как сеть, получающуюся из Σ в результате удаления всех ребер с пометками $x_1^{\overline{\alpha_1}},\ldots,x_n^{\overline{\alpha_n}}$, т. е. ребер, которые не проводят на наборе α, и снятия пометок с остальных ребер Σ. Для вершин u и v КС Σ введем *функции проводимости от вершины* u *к вершине* v как ФАЛ, которая равна 1 на наборе $\alpha = (\alpha_1,\ldots,\alpha_n)$ тогда и только тогда, когда в сети $\Sigma|_\alpha$ существует $(u-v)$-цепь, т. е. тогда и только тогда, когда в Σ имеется цепь из проводящих на наборе α контактов вида $x_1^{\alpha_1},\ldots,x_n^{\alpha_n}$, идущая из v в u. Считается, что (p,q)-КС Σ с входами $a_1',\ldots,a_p'$ и выходами $a_1'',\ldots,a_q''$ реализует матрицу $F = ||f_{ij}||, 1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q$, где f_{ij} — ФАЛ проводимости от входа a_i' к выходу a_j''.

Определение 4. *Универсальным контактным* (p,q)-*полюсником* (далее (p,q)-УКМ) порядка n будем называть (p,q)-КС, между p входами и q выходами которой реализованы все функции от n переменных (как функции проводимости), и при этом, как уже говорилось, ни один вход КС не является ее выходом.

Определение 5. Для натуральных чисел n, p и q таких, что $p \cdot q \geqslant 2^{2^n}$, обозначим через $L^K(p, q, n)$ минимальную сложность (p, q)-УКМ порядка n, а затем положим:

$$L^K(n) = \min_{p \cdot q \geqslant 2^{2^n}} L^K(p, q, n).$$

Введем, далее, величину $\hat{L}^K(n)$ равную минимальной сложности УКМ порядка n с неразделенными полюсами.

Целью данной работы было исследование поведения функций $L^K(p, q, n)$ и $L^K(n)$ при $n = 1, 2, 3, \ldots$ и $p = p(n), q = q(n)$. Ее основным результатом явилось следующее утверждение:

Теорема 1. *Пусть для* $n = 1, 2, 3 \ldots$ *натуральные последовательности* $l = l(n), t = t(n), p = p(n)$ *и* $q = q(n)$ *таковы, что* $p = 2^l$, $q = 2^t$ *и* $p \cdot q \geqslant 2^{2^n}$ *Тогда*

$$L^K(p, q, n) \sim 2 \cdot (p + q) \quad \text{и} \quad L^K(n) \sim 4 \cdot 2^{2^n}.$$

Были установлены также значения $L^K(2)$ и $\hat{L}^K(2)$:

Теорема 2.

$$L^K(2) = 10, \quad \hat{L}^K(2) = 8.$$

Кроме того были найдены все 37 УКМ с разделенными полюсами сложности 8, и все 300 УКМ с разделенными полюсами сложности 10 (без учета пометок ребер переменными и их отрицаниями).

Список литературы

1. Ложкин С. А. Лекции по дополнительным главам кибернетики. — М.: МГУ, 2013.
2. Ложкин С. А. Лекции по основам кибернетики. — М.: МГУ, 2004.
3. Ложкин С. А., Кошкин М. А. О сложности реализации некоторых систем функции алгебры логики контактными многополюсниками // ДАН СССР. — 1988. — Т. 298, № 4. — С. 807–811.
4. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып.10. — М.: Физматгиз, 1963. — С. 63–97.
5. Редькин Н. П. О реализации систем конъюнкций контактными схемами // Проблемы кибернетики. Вып.30. — М.: Наука, 1975. — С. 263–276.
6. Трусилова И. В. Асимптотическая оценка сложности многополюсника, реализующего одну систему функций // Численные методы в математической физике — М.: МГУ, 1986. — С. 122–123.
7. Ложкин С. А., Кошкин М. А. О сложности реализации некоторых систем функции алгебры логики контактными и обобщенными контактными схемами // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 257–285.

ИЕРАРХИЯ ДЛЯ ДВУСТОРОННИХ ДЕТЕРМИНИРОВАННЫХ, НЕДЕТЕРМИНИРОВАННЫХ И ВЕРОЯТНОСТНЫХ АВТОМАТОВ ПО ШИРИНЕ

Р. Н. Ибрагимов (Казань)

Введение

В данной работе рассматривается известная модель — двусторонние автоматы. В частности, двусторонние конечные детерминированные (2КДА) и недетерминированные (2КНА) автоматы.

Приведем формальное определение. Двусторонним конечным детерминированным автоматом (2КДА) D, работающим на входном слове $X = (x_1, \ldots, x_n)$, с левым (\$) и правым ограничителями (#), называется шестерка $D = (\Sigma, S, s_1, \delta, s_a, s_r)$, где Σ — входной алфавит (мы будем рассматривать только алфавит $\Sigma = \{0, 1\}$); S — множество состояний автомата, причем $|S| = const$, количество состояний $|S|$ будем называть размером автомата; s_1 — начальное состояние, причем $s_1 \in S$; $\delta : S \times \Sigma \cup \{\$, \#\} \to S \times \{\leftarrow, \downarrow, \rightarrow\}$, причем $\delta(s, \$) = (s, \rightarrow)$, $\delta(s', \#) = (s', \leftarrow)$, для любого $s \in S, s' \in S \backslash \{s_a, s_r\}$, где $\leftarrow$ означает, что читающая головка перемещается влево, $\rightarrow$ — вправо, $\downarrow$ — остается на месте; s_a — принимающее состояние, причем $s_a \in S$; s_r — отвергающее состояние, причем $s_r \in S$.

Опишем работу автомата D на слове $\nu \in \Sigma^n$. Первоначально автомат обозревает первую ячейку и находится в состоянии s_1. Затем применяется функция переходов $\delta(s_1, x_1) = (s', di)$, где $s' \in S$, $di \in \{\leftarrow, \downarrow, \rightarrow\}$. Читающая головка перемещается в соответствии с направлением di, при этом автомат переходит в состояние s', и так далее.

Автомат D принимает входное слово (выдает результат 1), если попадает в состояние s_a. Автомат D отвергает входной набор (выдает результат 0), если попадает в состояние s_r или попадает в бесконечный цикл. Причем, если автомат обозревает ячейку с номером i, где $i \in \{0, \ldots, n\}$, и находится в состоянии s_r или s_a, то автомат переводит читающую головку в конец слова без изменения состояния и завершает работу.

Аналогично можно определить недетерминированную модель 2КНА.

Также рассмотрим вероятностный аналог 2ВА двустороннего неоднородного детерминированного автомата 2КА, введенного в работе [3]. Его особенность заключается в наличии различных функций перехода для каждой позиции читающего устройства на ленте.

Вопрос об отношении классов языков, распознаваемых автоматами разного размера, рассматривался уже давно. К примеру, W. J. Sakoda и M. F. Sipser

в работе [4] показали, что любой 2КНА может быть смоделирован 2КДА экспоненциального размера. Кроме того, двусторонние автоматы моделировались односторонними и лучшие вариант был в работах [1, 2]. В работе [5] была построена иерархия для 2КДА и 2КНА, в данной работе этот результат уточняется.

1. Полученные результаты

Определим классы языков, относительно которых будет построена иерархия.

Определение 1. $\mathsf{2DFASIZE(d)}$ — класс языков, распознаваемых двусторонним детерминированным автоматом размера d.

Определение 2. $\mathsf{2NFASIZE(d)}$ — класс языков, распознаваемых двусторонним недетерминированным автоматом размера d.

Были получены следующие результаты.

Теорема 1.

$$\mathsf{2DFASIZE}\,(d) \subsetneq \mathsf{2DFASIZE}\,(\lceil 32(d+3)\log(d+3)\rceil)\,.$$

Теорема 2.

$$\mathsf{2NFASIZE}\,(d) \subsetneq \mathsf{2NFASIZE}\left(\left\lceil 32(d^2+3)\log(d^2+3)\right\rceil\right).$$

Теорема 3. *Пусть $d : \mathbb{N} \to \mathbb{N}$ отличная от константы функция, такая что $d^2(n) < n$. Тогда*

$$\mathsf{2PSIZE}\left(\left\lfloor \frac{\sqrt{(d+9)/13}-2}{4(8+3\log t)} \right\rfloor\right) \subsetneq \mathsf{2PSIZE}\,(d)\,.$$

Для доказательства теорем используются свойства булевый функций *Shuffled Address Function* $\mathtt{2\text{-}SAF}_{\mathtt{w}}$ [7] и ее модификация — *Uniform Shuffled Address Function* $\mathtt{2\text{-}USAF}_{\mathtt{w}}$. Сначала представим некоторые верхние оценки.

2. Верхние оценки

Рассмотрим булеву функцию $f = f(X)$ и разбиение $\pi = (X_A, X_B)$ переменных X. Для каждого фиксированного набора σ будем рассматривать отображение $\rho : X_A \to \sigma$. Подфункция $f|_\rho$ над переменными из множества X_B получается из функции f фиксированием переменных из множества X_A в соответствии с отображением ρ.

Обозначим за $N^\pi(f)$ количество различных подфункций, получаемых при рассмотрении всех возможных σ.

Рассмотрим множество Θ всех возможных перестановок чисел от 1 до n. Для $\theta = (j_1, \ldots, j_n)$ обозначим через $X^{\theta,u}$ множество переменных $(x_{j_1}, \ldots, x_{j_u})$.

Через $\Pi(\theta)$ обозначим множество разбиений

$$\Pi(\theta) = \{\pi : \pi = (X^{\theta,u}, X \setminus X^{\theta,u})\}, 1 \leqslant u \leqslant n.$$

Определение 3. *Количеством подфункций* для порядка $\theta \in \Theta$ для булевой функции f назовем величину

$$N^{\theta}(f) = \max_{\pi \in \Pi(\theta)} N^{\pi}(f).$$

Заметим, что если $id = (1, \ldots, n)$ и f — характеристическая фукнция языка L, то величина $N^{id}(f)$ совпадает с рангом языка L (количеством классов эквивалентности отношения $\equiv_L$).

Ранее были получены следующие оценки:

Теорема 4 [5]. *Если язык L распознается* 2КДА A *размера d и булева функция $f(X)$ — характеристическая функция языка L, то*

$$N^{id}(f) \leqslant (d+1)^{(d+1)}.$$

Теорема 5 [5]. *Если язык L распознается* 2КНА A *размера d и булева функция $f(X)$ — характеристическая функция языка L, то*

$$N^{id}(f) \leqslant 2^{(d+1)^2}.$$

Аналогичная оценка получена для модели двустороннего неоднородного вероятностного автомата.

Теорема 6. *Если язык L распознается* 2ВА A *с ε — изолированной точкой сечения и математическим ожиданием числа шагов автомата t, то*

$$N(f) \leqslant \left\lceil \frac{4d\,(8 + 3\log t)}{\log\,(1+2\varepsilon)\,(1+\varepsilon)} \right\rceil^{(d+1)^2}.$$

3. Булевы функции 2-SAF$_w$ и 2-USAF$_w$, их свойства

Булева функция 2-SAF$_w$ введена в работе [3], для нее получены следующие результаты.

Лемма 1 [3]. *Для целого значения $w = w(n)$, удовлетворяещего неравенству $2w(2w + \lceil \log 2w \rceil) < n$, выполняется неравенство*

$$N(\text{2-SAF}_w) \geqslant w^{w-2}.$$

Лемма 2 [3]. *Существует* 2КА A *размера $13w + 4$, распознающий язык, характеристической функцией которого является функция* 2-SAF$_w$.

Рассмотрим модификацию булевой функции $\texttt{2-SAF}_\texttt{w}$. Назовем ее *Uniform Shuffled Address Function* и обозначим $\texttt{2-USAF}_\texttt{w}$. Ее сложностные характеристики помогут нам построить иерархию для 2КДА и 2КНА. Булева функция $\texttt{2-USAF}_\texttt{w}$ определяется следующим образом: $\texttt{2-USAF}_\texttt{w}(X) : \{0,1\}^n \to \{0,1\}$ и пусть $w = w(n)$ такое целое, что

$$4w(2w + \lceil \log 2w \rceil) < n. \tag{1}$$

Разделим входные переменные (символы входного слова) на $2w$ блоков. В каждом блоке по $\lfloor \frac{n}{2w} \rfloor = a$ переменных. Кроме того, разделим переменные каждого блока на *маркерные*, *адресные* и *значащие*. Все переменные, стоящие на нечетных позициях, назовем *маркерными*. Если значение маркерной переменной равно 1, за ней идет значащая переменная, иначе — адресная. Первые $\lceil \log 2w \rceil = c$ переменных блока, стоящих на четных позициях, назовем *адресными* и оставшиеся $\frac{a}{2} - \lceil \log 2w \rceil = b$ переменных блока — *значащими*.

Обозначим через $x_0^p, \ldots, x_{b-1}^p$, $y_0^p, \ldots, y_{\lceil \log 2w \rceil}^p$ и $z_0^p, \ldots, z_{\frac{a}{2}}^p$ *значащие*, *адресные* и *маркерные* переменные p-го блока соответственно, для $p \in \{0, \ldots, 2w-1\}$.

Булева функция $\texttt{2-USAF}_\texttt{w}(X)$ вычисляется на основе следующих пяти функций:

1. Функция $Adr : \{0,1\}^n \times \{0, \ldots, 2w-1\} \to \{0, \ldots, 2w-1\}$ вычисляет адрес блока:
$$Adr(X, p) = \sum_{j=0}^{c-1} y_j^p \cdot 2^{c-j-1} (\mathrm{mod}\ 2w).$$

2. Функция $Ind : \{0,1\}^n \times \{0, \ldots, 2w-1\} \to \{-1, \ldots, 2w-1\}$ вычисляет номер блока по адресу:
$$Ind(X, i) = \begin{cases} p, & \text{где } p \text{ — минимальное число, т. ч. } Adr(X, p) = i, \\ -1, & \text{если не нашлось такого } p. \end{cases}$$

3. Функция $Val : \{0,1\}^n \times \{0, \ldots, 2w-1\} \to \{-1, \ldots, w-1\}$ вычисляет значение блока с адресом i:
$$Val(X, i) = \begin{cases} \sum\limits_{j=0}^{b-1} x_j^p (\mathrm{mod}\ w), & \text{где } p = Ind(X, i) \text{ для } p \geqslant 0, \\ -1, & \text{если } Ind(X, i) < 0. \end{cases}$$

Для вычисления $\texttt{2-USAF}_\texttt{w}(X)$ производится две итерации. Две функции $Step_1$ и $Step_2$ дают результат t-й итерации.

4. Функция $Step_1 : \{0,1\}^n \times \{0, \ldots, 1\} \to \{-1, w \ldots, 2w-1\}$ вычисляет первую часть t-й итерации:
$$Step_1(X, t) = \begin{cases} -1, & \text{если } Step_2(X, t-1) = -1, \\ Val(X, Step_2(X, t-1)) + w, & \text{иначе.} \end{cases}$$

5. Функция $Step_2 : \{0,1\}^n \times \{-1,\ldots,1\} \to \{-1,\ldots,w-1\}$ вычисляет вторую часть t-й итерации:

$$Step_2(X,t) = \begin{cases} -1, & \text{если } Step_1(X,t) = -1, \\ 2, & \text{если } t = -1, \\ Val(X, Step_1(X,t)), & \text{иначе.} \end{cases}$$

Отметим, что адрес текущего блока вычисляется на предыдущем шаге. Функция $\texttt{2-USAF}_\texttt{w}(X)$ вычисляется следующим образом:

$$\texttt{2-USAF}_\texttt{w}(X) = \begin{cases} 0, & \text{если } Step_2(X,1) \leqslant 0, \\ 1, & \text{иначе.} \end{cases}$$

Лемма 3. *Для целого $w = w(n)$, удовлетворяющего неравенству* (1)*, выполняется неравенство*

$$N^{id}(\texttt{2-USAF}_\texttt{w}) \geqslant w^{w-2}.$$

Лемма 4. *Существует* 2КДА A *размера* $23w + 2(1+3w)\log w + 6$*, распознающий язык, характеристической функцией которого является функция* $\texttt{2-USAF}_\texttt{w}$.

Используя приведенные верхние оценки, а также свойства функций $\texttt{2-SAF}_\texttt{w}$ и $\texttt{2-USAF}_\texttt{w}$, мы можем доказать теоремы 1, 2 и 3.

По лемме 3, лемме 4, и теореме 4 нетрудно показать, что $\texttt{2-USAF}_\texttt{d} \in \in \mathsf{2DFASIZE}(\lceil 32d \log d \rceil)$ и $\texttt{2-USAF}_\texttt{d} \notin \mathsf{2DFASIZE}(d-3)$.

Аналогично, по лемме 3, лемме 4, и теореме 5 имеем, что $\texttt{2-USAF}_\texttt{d} \in \in \mathsf{2NFASIZE}(\lceil 32d \log d \rceil)$ и $\texttt{2-USAF}_\texttt{d} \notin \mathsf{2NFASIZE}\left(\lfloor \sqrt{d-3} \rfloor\right)$.

По лемме 1, лемме 2 и теореме 6 получаем, что $\texttt{2-SAF}_\texttt{d} \in \mathsf{2PSIZE}\,(13d+4)$ и $\texttt{2-SAF}_\texttt{d} \notin \mathsf{2PSIZE}\left(\left\lfloor \frac{\sqrt{d+1}-2}{4(8+3\log t)} \right\rfloor\right)$.

Список литературы

1. Chrobak M. Finite automata and unary languages // Theoretical Computer Science. — 1986. — V. 47(0). — P. 149–158.
2. Kapoutsis C. A. Removing bidirectionality from nondeterministic finite automata // MFCS volume of Lecture Notes in Computer Science. — Springer, 2005. — V. 3618. — P. 544–555.
3. Khadiev K., Yakaryilmaz A. New Size Hierachies for Two-way Non-uniform Automata // Sixth Workshop on Non-Classical Models of Automata and Applications (NCMA 2014) Short Papers. — 2014. — P. 13–18.
4. Sakoda William J., Sipser Michael F. Nondeterminism and the size of two-way finite automata // Proceedings of the tenth annual ACM symposium on Theory of computing. — 1978. — P. 275–286.

5. Хадиев К. Р, Ибрагимов Р. Н. Иерархия для двухсторонних детерменированных и недетерменированных автоматов // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г.: Труды — М.: МАКС, 2015. — С. 252–254.

СИГМА-ПРЕДСТАВЛЕНИЯ АДДИТИВНОЙ ГРУППЫ ВЕЩЕСТВЕННЫХ ЧИСЕЛ НАД $\mathbb{HF}(\mathbb{R})$

Р. М. Короткова (Новосибирск)

Введение

В теории вычислимых моделей обычно изучаются следующие три группы вопросов:

1. Проблема существования вычислимых представлений;
2. Проблема числа вычислимых представлений;
3. Существование параметризаций для классов вычислимых моделей.

Данная работа относится ко второй группе вопросов, если вместо вычислимости рассматривать одно из ее обобщений. А именно, в работе изучается число Σ-представлений аддитивной группы вещественных чисел над $\mathbb{HF}(\mathbb{R})$.

1. Основные определения

Вычислимость на компьютере, в котором к встроенным типам данных добавлены настоящие вещественные числа (не приближения), хорошо моделируется в виде Σ-определимости над структурой $\mathbb{HF}(\mathbb{R})$, где $\mathbb{R}$ — поле вещественных чисел.

Напомним определение этой структуры (см. [1]). Ее основное множество определяется так:

$$\begin{aligned} HF_0(\mathbb{R}) &= \mathbb{R}, \\ HF_{n+1}(\mathbb{R}) &= HF_n(\mathbb{R}) \cup S_{\text{fin}}(HF_n(\mathbb{R})), \\ HF(\mathbb{R}) &= \bigcup_{n\in\omega} HF_n(\mathbb{R}). \end{aligned}$$

Такие структуры обычно рассматриваются в сигнатуре

$$\langle \in, U, +, \times, <, 0, 1, \varnothing \rangle,$$

где $+ : \{\langle x, y, z\rangle | x+y = z\}$, $\times : \{\langle x, y, z\rangle | x \times y = z\}$ — графики соответствующих операций на $\mathbb{R}$, $0 : \{0\}$ — ноль, $1 : \{1\}$ — единица, $\varnothing : \{\varnothing\}$ — пустое множество.

Аналогом вычислимой перечислимости в теории допустимых множеств является понятие Σ-определимости, т. е. определимости с помощью Σ-формул.

Напомним определение Σ-формул. Для начала надо определить Δ_0-формулы.

Определение 1 ([2])**.** В теории допустимых множеств Δ_0-*формулы* определяются рекурсивно следующим образом:

1. Любая атомарная формула есть Δ_0 формула;
2. Если Φ и Ψ — Δ_0-формулы, то $\neg\Phi$, $(\Phi \vee \Psi)$, $(\Phi \wedge \Psi)$, $(\Phi \to \Psi)$ тоже Δ_0-формулы;
3. Если x — переменная, t — терм, а Φ — Δ_0-формула, то $\exists x \in t\Phi$, $\forall x \in t\Phi$ тоже Δ_0-формулы;
4. Δ_0-формулами являются только формулы, полученные согласно пунктам 1–3.

Определение 2 ([2])**.** С помощью Δ_0-формул определим Σ-*формулы*:

1. Любая Δ_0-формула есть Σ-формула;
2. Если Φ и Ψ — Σ-формулы, то $(\Phi \vee \Psi)$ и $(\Phi \wedge \Psi)$ тоже Σ-формулы;
3. Если x — переменная, t — терм, а Φ — Σ-формула, то то $\exists x \in t\Phi$, $\forall x \in t\Phi$, $\exists x\Phi$ тоже Σ-формулы;
4. Других Σ-формул нет.

Ниже через $\varphi[\mathfrak{N}, \overline{p}]$ обозначено множество $\{x | \mathfrak{N} \models \varphi(x, \overline{p})\}$, где $\varphi(x, \overline{z})$ — формула языка теории допустимых множеств, а $\overline{p}$ — кортеж параметров.

Определение 3 ([3])**.** Будем говорить, что алгебраическая система

$$\mathfrak{A} = \langle A; P_0^{m_0}, \ldots, P_{k-1}^{m_{k-1}} \rangle$$

Σ-*определима* над $\mathbb{HF}(\mathfrak{M})$, если существуют конечный кортеж параметров $\overline{p} \in \mathbb{HF}(\mathfrak{A})$ и Σ-формулы $V(x, z)$, $E^+(x, y, z)$, $E^-(x, y, z)$, $P_0^+(x, z)$, $P_0^-(x, z)$, $\ldots$ $\ldots, P_{k-1}^+(x, z)$, $P_{k-1}^-(x, z)$, такие что:

1. Множества $E^+[\mathbb{HF}(\mathfrak{M}), \overline{p}]$ и $E^-[\mathbb{HF}(\mathfrak{M}), \overline{p}]$ образуют разбиение множества $V[\mathbb{HF}(\mathfrak{M}), \overline{p}]^2$;
2. Для всех $i < k$ множества $P_i^+[\mathbb{HF}(\mathfrak{M}), \overline{p}]$ и $P_i^-[\mathbb{HF}(\mathfrak{M}), \overline{p}]$ образуют разбиение множества $V[\mathbb{HF}(\mathfrak{M}), \overline{p}]^{m_i}$;

3. $E(x, y, \overline{p})$ определяет конгруэнцию на алгебраической системе

$$\mathfrak{B} = \langle V[\mathbb{HF}(\mathfrak{M}), \overline{p}]; P_0^+[\mathbb{HF}(\mathfrak{M}), \overline{p}], \ldots, P_{k-1}^+[\mathbb{HF}(\mathfrak{M}), \overline{p}]\rangle$$

(обозначаемую в дальнейшем E), и $\mathfrak{B}/E \cong \mathfrak{A}$.

Мы будем отождествлять группы $\langle \mathbb{R}^n, +\rangle$, $n \in \mathbb{N}$ с их естественными Σ-представлениями над $\mathbb{HF}(\mathbb{R})$, в которых $\mathbb{R}^n = \{\langle x_1, \ldots, x_n\rangle \mid x_1, \ldots, x_n \in \mathbb{R}\}$, а знак $+$ имеет стандартную интерпретацию: $\langle x_1, \ldots, x_n\rangle + \langle y_1, \ldots, y_n\rangle = \langle x_1 + y_1, \ldots, x_n + y_n\rangle$.

Приведем теперь точную формулировку основного результата работы.

2. Основной результат

Теорема 1. *Абелевы группы $\langle \mathbb{R}^n, +\rangle$ и $\langle \mathbb{R}^m, +\rangle$ изоморфны при любых $m, n \in \mathbb{N}$, но не Σ-изоморфны над $\mathbb{HF}(\mathbb{R})$ при $m \neq n$.*

Следствие 1. *Существует по крайней мере ω попарно не Σ-изоморфных представлений группы $\langle \mathbb{R}, +\rangle$.*

3. Некоторые представления группы $\langle \mathbb{R}, +\rangle$

Попутно с основной теоремой этой работы были доказаны некоторые другие результаты.

Далее $\mathbb{Q}$ — множество рациональных чисел.

Теорема 2. *Группа $\langle \mathbb{R}; +\rangle$ изоморфна группе $\langle \mathbb{R} \oplus \mathbb{Q}; +\rangle$, но не Σ-изоморфна ей.*

4. Заключение

Было показано, что существует счетное количество попарно не Σ-изоморфных представлений аддитивной группы $\langle \mathbb{R}, +\rangle$. При этом в доказательстве важную роль играли топологические соображения. Автор выдвигает гипотезу, состоящую в том, что:

Гипотеза. *Существует континуум попарно не Σ-изоморфных представлений аддитивной группы $\langle \mathbb{R}, +\rangle$.*

Список литературы

1. Ершов Ю. Л. Определимость и вычислимость // Новосибирск: Сибирская школа алгебры и логики, 1996.
2. Barwise J. Admissible Sets and Structures. Springer–Verlag, Berlin, Göttingen, Heidelberg, 1975.
3. Морозов А. С. О некоторых представлениях поля вещественных чисел // Алгебра и логика. — 2012. — Т. 51, вып. 1. — С. 96–128.
4. Федорчук В. В. Основы теории размерности, в сб. Итоги науки и техники. Современные проблемы математики. Фундаментальные направления // ВИНИТИ. М., 1988. — Т. 17. — С. 111–224.

ОБ УТОЧНЕНИИ ЗНАЧЕНИЙ ФУНКЦИОНАЛА СЛОЖНОСТИ КОНТАКТНЫХ СХЕМ ДЛЯ БУЛЕВЫХ ФУНКЦИЙ ОТ ПЯТИ ПЕРЕМЕННЫХ

С. А. Ложкин, М. С. Шуплецов, В. А. Коноводов, Б. Р. Данилов, В. В. Жуков, Н. Ю. Багров (Москва)

Введение

Построение минимальных и близких к ним схем в заданной модели дискретных управляющих систем является актуальной задачей математической кибернетики. Каталоги или библиотеки таких схем находят свое применение в различных алгоритмах логического синтеза цифровых схем (см., например, [1]). Первых каталоги минимальных контактных схем(КС), реализующих функции алгебры логики (ФАЛ) от малого числа переменных, появились еще в 1950-х гг. Так, например, в статье [2], в книге [3] и работе [4] приведены таблицы верхних оценок контактной сложности для всех типовых ФАЛ четырех переменных (всего 402 функции).

В [5] Г. Н. Поваровым с помощью построения схем было установлено, что одна ФАЛ из этих 402 требует не более 14 контактов, четыре ФАЛ — не более 13 контактов, а остальные — не более 12 контактов. Затем В. Л. ван дер Пуль [6] построил для первой из этих функций схему с 13 контактами. Ю. Л. Васильев [4], взяв за основу каталоги из работ Г. Н. Поварова [5], Игоннэ и Греа [7], указал минимальные значения всех функций от четырех переменных. Три ФАЛ имели сложность 12, и две — 13. Позднее в работе В. Ю. Сусова [8] каталог Ю. Л. Васильева был уточнен, и было доказано, что сложность 13 имеет только одна функция от четырех переменных.

В работе К. Шеннона [9] было доказано, что для реализации любой ФАЛ от 5 переменных в классе контактных схем достаточно 30 контактов. Позднее, Г. Н. Поваров [10] уточнил эту оценку до 28 контактов, используя метод каскадов и полученные ранее результаты для ФАЛ от четырех переменных. В. Ю. Сусовым [8] была найдена ФАЛ от 5 переменных, контактная сложность которой не меньше 19.

1. Основные определения и формулировка полученных результатов

Пусть $X = \{x_1, \ldots, x_n, \ldots\}$ — счетный алфавит входных переменных, и пусть $P_2(n)$ — множество всех ФАЛ от переменных $x_1, \ldots, x_n$. Обозначим через U^{K} класс (1,1)-КС от переменных из алфавита X. Сложностью $L(\Sigma)$ КС Σ, $\Sigma \in U^K$, называется общее число контактов в этой схеме, а сложностью $L(f)$

ФАЛ f, $f \in P_2(n)$, называется минимальная сложность КС Σ, реализующей ФАЛ f. Введем обычным образом функцию Шеннона $L(n)$ для сложности КС:

$$L(n) = \max_{f \in P_2(n)} L(f).$$

Основным результатом работы является следующая теорема.

Теорема 1. *Значение функции Шеннона для контактной сложности ФАЛ от* 5 *переменных удовлетворяет следующему неравенству*:

$$L(5) \leqslant 22.$$

Теорема была доказана в результате построения каталога минимальных и близких к ним КС [11], найденных в результате применения различных алгоритмов построения КС. Основные алгоритмы, которые позволили существенно понизить верхнюю оценку соответствующей функции Шеннона, описаны в разделах 2 и 3.

Стоит отметить, что при построения каталога все ФАЛ от пяти переменных были разбиты на классы эквивалентности относительно операций перестановки и инвертирования переменных, так как эти операции не меняют структуры КС, реализующей указанные ФАЛ и позволяют существенно сократить число рассматриваемых ФАЛ.

2. Алгоритмы построения контактных схем на основе модификаций метода каскадов

Метод каскадов [12] является довольно простым и в то же время довольно эффективным методом синтеза КС. Он связан с последовательным разложением заданных ФАЛ по булевым переменным и рекурсивным построением схемы, реализующей эти ФАЛ. При этом оригинальный метод каскадов предполагает единый глобальный порядок переменных, который используется при разложении и рекурсивном построении схемы. В данной работе вводится следующая модификация метода каскадов. На каждом этапе рекурсивного построения КС для ФАЛ f, существенно зависящей от переменных из множества $X(n) = (x_1, \ldots, x_n)$, переменная, по которой производится разложение, выбирается в результате решения следующей оптимизационной задачи:

$$x^* = \operatorname*{argmin}_{x \in X(n)} \left(L\left(f|_x\right) + L\left(f|_{\overline{x}}\right) \right),$$

где $f|_x$ и $f|_{\overline{x}}$ — остаточные ФАЛ, получаемые в результате подстановки вместо переменной x константы 1 и 0, соответственно.

Данная оптимизационная задача может быть решена полным перебором, но этот подход неприменим для ФАЛ с большим числом переменных из-за ее экспоненциальной сложности. В данной работе предлагают две следующих стратегии для приближенного решения указанной оптимизационной задачи.

Напомним, что для ФАЛ f ее булевой разностью (производной) по переменной x называется ФАЛ $\frac{\partial f}{\partial x} = f|_x \oplus f|_{\overline{x}}$. Назовем булевым градиентом $g(f,x)$ ФАЛ f по переменной x следующую числовую функцию:

$$g(f,x) = \sum_{\widetilde{\sigma} \in B^{n-1}} \frac{\partial f}{\partial x}(\widetilde{\sigma}),$$

где B^{n-1} — множество всех наборов из 0 и 1 длины $(n-1)$. Таким образом, на каждом этапе разложения выбирается такая переменная, на которой достигается максимум функции $g(f,x)$ (если таких переменных несколько, то переменная выбирается случайно среди всех переменных, обладающих указанным свойством).

Другая стратегия заключается в том, что функция $g(f,x)$ может быть использована для того, чтобы задать вероятность выбора переменной:

$$P(f,x) = \frac{g(f,x)}{\sum\limits_{x \in X} g(f,x)}.$$

В этом случае, переменная для разложения выбирается на основе указанной вероятности.

Экспериментально было показано, что указанные модификации позволяют для ряда ФАЛ построить КС с меньшим числом контактов, по сравнению со схемами, которые получаются в результате классического метода каскадов.

3. Алгоритм построения контактных схем на основе тупиковых ДНФ

Пусть задана ФАЛ f, $f \in P_2(n)$, существенно зависящая от n переменных $X(n)$. Характеристическим множеством ФАЛ f назовем множество наборов, на котором данная ФАЛ принимает значение 1. Зафиксируем некоторый порядок переменных $T = (x_{i_1}, \ldots, x_{i_n})$ и возьмем такую тупиковую ДНФ $\mathfrak{A} = K_1 \vee \ldots \vee K_m$, реализующую ФАЛ f, в каждой элементарной конъюнкции K_i, $i = 1, \ldots, m$, которой порядок следования переменных соответствует заданному порядку T. По ДНФ $\mathfrak{A}$ построим контактное дерево D с одним входом и m выходами с помощью операцию добавления очередной элементарной конъюнкции K_i, $i = 1, \ldots, m$, в уже построенное дерево D_{i-1}.

Пусть D_0 — тривиальное дерево, состоящее из входа (корня) и пусть в очередной рассматриваемой элементарной конъюнкции K_i первым вхождением является вхождение переменой x_k (или ее отрицания $\overline{x_k}$). Если существует ребро с пометкой x_k (соответственно $\overline{x_k}$), соединяющее корень дерева D_{i-1} с некоторым поддеревом D'_{i-1}, то результатом операции добавления элементарной конъюнкции K_i в дерево D_{i-1} является результат операции добавления элементарной конъюнкции K', получающейся удалением вхождения переменной x_k (переменной с отрицанием $\overline{x_k}$) из K, в поддерево D'_{i-1}. Если

такого ребра не существует, то присоединим к корню дерева D_{i-1} цепочку ребер с пометками, соответствующими вхождениям переменных в элементарную конъюнкция K_i, а концевую вершину этой цепочки объявим i-ым листом (выходом) D. Контактным деревом для тупиковой ДНФ $\mathfrak{A}$ назовем результат добавления всех элементарных конъюнкций $\{K_1, \ldots, K_m\}$ в дерево D_0.

Если все листья контактного дерева для тупиковой ДНФ T объединить в одну вершину, то получится контактная схема Σ с одним входом и одним выходом, реализующая функцию f. В общем случае сложность полученной контактной схемы довольно большая, поэтому контактные схемы такого вида не представляют особого интереса.

Из полученной контактной схемы Σ получим контактную схему Σ' путем склеивания одинаковых цепей из контактов, исходящих из выходной вершины схемы Σ, таких что всем внутренним вершинам цепи инцидентны только контакты из данной цепи. Операция склеивания цепей уменьшает сложность исходной схемы Σ и при этом результирующая схема Σ' может реализовывать функцию f, если только в ней не образовались дополнительные проводящие цепи. Таким образом, в ряде случаев, перебирая контактные деревья для всех тупиковых ДНФ заданной ФАЛ f и меняя порядок переменных $T = (x_{i_1}, \ldots, x_{i_n})$, можно получить контактную схему Σ', реализующую функцию f уже с меньшей сложностью.

Если после склеивания цепей схемы Σ получается схема Σ', которая реализуется ФАЛ f', отличную от ФАЛ f, то значит в схеме Σ' появились некоторые дополнительные проводящие цепи и $f \to f' \equiv 1$. В этом случае для построения искомой КС можно сначала уменьшить число единичных наборов исходной ФАЛ f, добавив одно или несколько вхождений переменных (переменных с отрицанием) в одну или несколько элементарных конъюнкций ее тупиковой ДНФ $\mathfrak{A}$. Таким образом, после построения контактного дерева и склеивания цепей может получиться так, что характеристическое множество функции, которую реализует полученная схема Σ', совпадет с характеристическим множество функции f, а значит схема Σ' будет реализовывать функцию f.

При построении схемы Σ' используются цепи, такие что всем ее внутренним вершинам инцидентны только контакты из данной цепи и никакие другие контакты схемы Σ. Это позволяло в ряде случаев избежать появления дополнительных проводящих цепей. Но при применении выше описанной техники можно склеивать любые цепи, так как они могут нужным образом расширить характеристическое множество.

Таким образом основные этапы алгоритма можно описать следующим образом:

1. Переберем все тупиковые ДНФ функции f (включая порядок вхождения переменных в элементарные конъюнкции).

2. Для каждой тупиковой ДНФ переберем всевозможные сужения характеристического множества.

3. Построим контактное дерево и, объединив его листовые вершины, получим некоторую КС.

4. Для полученной КС переберем все варианты склеивания цепей.

5. Из всех вариантов выберем КС, реализующую функцию f и имеющую минимальную сложность.

Работа выполнена при финансовой поддержке РФФИ, грант №15-01-07474.

Список литературы

1. Mishchenko A., Chatterjee S., Brayton R. DAG-aware AIG rewriting: A fresh look at combinational logic synthesis // Proc. DAC'06, 2006. Pp. 532–536.
2. Polya G. J. Symb. Logik, 5, № 3, p. 98, 1940.
3. Синтез электронных вычислительных и управляющих систем / Пер. с англ. под ред. Шестакова В. И. М.: ИЛ, 1954.
4. Васильев Ю. Л. Минимальные контактные схемы для булевых функций четырех переменных // ДАН СССР. — 1959. — Т. 127, №2.
5. Поваров Г. Н. Исследование контактных схем с минимальным числом контактов. Диссертация, ИАТ АН СССР, 1954.
6. Van der Poel W. L. Engine bijzondere onderwerpen uit de schakelalgebra. De Ingenieur (Utrecht), 1955. — V. 67, Nr. 1, blz. E. 9–14.
7. Higonnet R., Gréa R. Etude logique des circuits électriques et des systémes binairs. Paris, 1955.
8. Сусов В. Ю. Два алгоритма переборного типа для синтеза минимальных контактных схем и их реализация. Дипломная работа. ВМК МГУ. М., 1981.
9. Shannon C. E. The Synthesis of Two-Terminal Switching Circuits // Bell System Techn. Journ. — 1949. — V. 28, No. 1. — Pp. 59–98.
10. Поваров Г. Н. Математико-логическое исследование синтеза контактных схем с одним входом и k выходами. // Сб. Логические исследования, ИАН СССР. — М.: Наука, 1959.
11. Ложкин С.А., Шуплецов М.С., Коноводов В.А., Данилов Б.Р. База данных „Значения функционалов сложности и известные оптимальные схемы из функциональных элементов и контактные схемы для булевых функций" [Электронный ресурс] // http://mks2.cmc.msu.ru/.
12. Поваров Г. Н. Метод синтеза вычислительных и управляющих контактных схем // Автоматика и телемеханика. — 1957. — Т 18, №2. — С. 145–162.

ПОСТРОЕНИЕ ЛЕГКО ДЕКОДИРУЕМЫХ СУБДЕБРЕЙНОВЫХ МАТРИЦ С ОКНОМ 2×2

Д. А. Макаров (Москва)

В данной работе рассматриваются алгоритмы построения матриц, в которых каждая подматрица фиксированного размера отлична от других. В виду уникальности каждой из подматриц по их содержимому можно однозначно определить положение подматрицы в исходной матрице.

Основные определения

Определение. *Последовательностью де Брейна* [1] будем называть периодическую последовательность над множеством мощности c, в которой содержатся все возможные комбинации из n элементов этого множества ровно один раз за минимальный период.

Любые n подряд идущих элементов в последовательности будем называть *окном*. Несложно заметить, что минимальный период последовательности де Брейна для заданных n и c равен c^n.

Определение. *Окном* размера $n \times m$ *в матрице* размера $N \times M$ будем называть любую подматрицу состоящую из n подряд идущих строк и m подряд идущих столбцов:

$$\begin{pmatrix} a_{i,j} & a_{i,j+1} & \dots & a_{i,j+m-1} \\ a_{i+1,j} & a_{i+1,j+1} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{i+n-1,j} & \dots & \dots & a_{i+n-1,j+m-1} \end{pmatrix},$$

где $i \leqslant N - n$ и $j \leqslant M - m$.

Определение. *Матрицей де Брейна* с окном размера $n \times m$ над множеством мощности c будем называть матрицу, в которой все окна размера $n \times m$ различны, а их число в точности равно c^{nm}.

Для того, чтобы матрица могла быть матрицей де Брейна при заданных n, m и c необходимо, чтобы ее размеры удовлетворяли условию:

$$c^{nm} = (N - n + 1)(M - m + 1). \tag{1}$$

Из этого равенства следует, что размеры матрицы де Брейна не могут быть произвольными. Однако, матрица любого размера может быть заполнена так, что все окна размера $n \times m$ в ней будут различны.

Определение. Матрицы, в которых все окна размера $n \times m$ уникальны будем называть *субдебрейновыми*.

Обозначим $C(A)$ — число различных элементов в матрице A. Любая матрица размера $N \times M$ содержит не более, чем NM различных элементов. Значит $C(A) \leqslant NM$. С другой стороны равенство (1), позволяет оценить минимальное количество элементов, необходимое для построения субдебрейновой матрицы. Обозначим $C_{n,m}(N,M) = \min C(A)$, где минимум берется по всем субдебрейновым матрицам размера $N \times M$. Тогда

$$C_{n,m}(N,M) \geqslant \sqrt[nm]{(N-n+1)(M-m+1)}.$$

В данной работе будет рассматриваться алгоритм построения субдебрейновых матриц $N \times M$ с окном размера 2×2, в которых поиск местоположения по окну осуществляется за число арифметических операций, не зависящее от размера матрицы.

Субдебрейновы матрицы $N \times M$ с окном 2×2

Построим субдебрейнову матрицу над множеством мощности c (для удобства будем считать, что используется множество $\mathbb{Z}_c$), с окном размера 2×2. Пусть строки матрицы нумеруются от 0 до $N-1$, а столбцы от 0 до $M-1$. С помощью предлагаемого алгоритма будем получать субдебрейновы матрицы размера $2c \times 2(c-1)^2$.

Каждому столбцу с четным номером поставим в соответствие одно число от 0 до $(c-1)^2$ и переведем его в двухразрядное число в системе счисления по основанию $c-1$. Запишем эти числа в соответствующие им столбцы так, чтобы старший разряд числа был в каждой строчке с четным номером, а младший — с нечетным.

Все столбцы с нечетными номерами будут заполнены одинаково — в каждую строчку с четным номером поместим элемент $c-1$, в строчки с нечетными номерами поместим число от 0 до $c-1$. Пример построенной матрицы:

$$\begin{pmatrix}
0 & c-1 & 0 & c-1 & \dots & c-1 & c-2 & c-1 \\
0 & 0 & 1 & 0 & \dots & 0 & c-2 & 0 \\
0 & c-1 & 0 & c-1 & \dots & c-1 & c-2 & c-1 \\
0 & 1 & 1 & 1 & \dots & 1 & c-2 & 1 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & c-1 & 0 & c-1 & \dots & c-1 & c-2 & c-1 \\
0 & c-1 & 1 & c-1 & \dots & c-1 & c-2 & c-1
\end{pmatrix}$$

В любом окне 2×2 данной матрицы будет присутствовать хотя бы один элемент $c-1$. Столбец с элементом $c-1$ содержит в себе закодированный номер строки. Так же в любом окне данной матрицы будет находиться столбец без элемента $c-1$, который отвечает за номер столбца. Поиск местоположения в субдебрейновой матрице, полученной по данному алгоритму будет занимать не более 11 арифметических операций и операций сравнения.

Пусть требуется построить субдебрейнову матрицу размера $N \times M$. Применим предложенный алгоритм к множествам $\mathbb{Z}_{c_1}, \mathbb{Z}_{c_1+1} \dots \mathbb{Z}_{c_1+h}$. Над каждым

из множеств будет получена своя матрица $A_{c_1}, A_{c_1+1} \dots A_{c_1+h}$. Минимальное число c_1, необходимое для построения матрицыA_{c_1}, равно:

$$c_1 = \left\lceil \sqrt{0.5M} \right\rceil + 1.$$

По алгоритму, предложенному в [2], построим матрицу де Брейна U размера $1 \times M$, с окном размера 1×2. С помощью формулы $c_2 = \left\lceil \sqrt{M-1} \right\rceil$ определим размер множества $B = \{1, 2, \dots, c_2\}$, необходимого для построения U. Чтобы элементы матрицы U не пересекались с элементами множества $\mathbb{Z}_{c_1+h}$, к каждому элементу матрицы U прибавим число $t = c_1 + h - 1$.

Изначально все матрицы имеют разное количество столбцов. Для заполнения матрицы A будем использовать только первые M столбцов каждой матрицы. Расположим полученные матрицы в матрице A следующим образом:

$$\begin{pmatrix} A_{c_1} \\ U \\ A_{c_1+1} \\ U \\ \dots \\ U \\ A_t \\ U \end{pmatrix}$$

Вычислим число строк в матрице A, полученной с помощью матриц $A_{c_1}, \dots$ $\dots, A_t$ и U:

$$\sum_{k=c_1}^{t} (2k+1).$$

Каждая единичка в слагаемом соответствует матрице U. Преобразовав это выражение, получим $t(t+2) - {c_1}^2 + 1$. Наименьшее t, для которого выполняется неравенство $t^2 - 2t - {c_1}^2 + 1 \geqslant N$ равно $-1 + \left\lceil \sqrt{{c_1}^2 + N} \right\rceil$.

Общий размер используемого множества $C(A) = c_2 + t$. Таким образом

$$C(A) = \left\lceil \sqrt{M-1} \right\rceil + \left\lceil \sqrt{\left(\sqrt{0.5M} + 1\right)^2 + N} \right\rceil - 1.$$

Согласно нижней оценке $C_{2,2}(N, M) \geqslant \sqrt[4]{(N-1)(M-1)}$. Пусть M и N таковы, что для некоторого α выполняется условие: $M = \alpha N$, тогда при $N \to \infty$ полученное $C(A)$ асимптотически равно $\left(\sqrt{1 + 0.5\alpha} + \sqrt{\alpha}\right)\sqrt{N}$, а значение $C_{2,2}(N, \alpha N)$ асимптотически не меньше $\sqrt[4]{\alpha}\sqrt{N}$. Отсюда следует, что для матрицы A размера $N \times \alpha N$, заполненной по предложенному алгоритму, $C(A)$ по порядку равно $C_{2,2}(N, \alpha N)$.

Список литературы

1. de Bruijn N. G. A combinatorial problem // Koninklijke Nederlandse Akademie v. Wetenschappen. — 1946. — V. 49. — P. 758–764.
2. Макаров Д. А. О построении матриц де Брейна // Материалы IX молодежной школы по дискретной математике и ее приложениям. — Москва, 2013. — С. 72–76.

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ГЛАДКИХ КАКТУСОВ

А. К. Мелешко (Москва)

Кактусом называется связный граф, в котором нет ребер, лежащих более чем на одном простом цикле [1, с. 93]. Все блоки кактуса — ребра или простые циклы. *Гладкий граф* — это связный граф без висячих вершин [2].

Форд и Уленбек перечислили помеченные кактусы с заданным распределением числа вершин по циклам [3]. Из их результата следует формула для числа помеченных кактусов с заданным числом вершин, но она содержит суммирование по всем разбиениям целого числа. Более простые формулы получены в [4] и [5]. Рид перечислил помеченные гладкие графы с заданным числом вершин [6].

Теорема. *Пусть SG_n — число помеченных гладких кактусов с n вершинами, тогда при $n \geqslant 3$ верна формула*

$$SG_n = \sum_{m=3}^{n} \frac{(-1)^{n-m} n!}{(n-m)!} \sum_{r=1}^{[\frac{m-1}{2}]} \sum_{k=0}^{m-2r-1} \binom{m-k-r-2}{r-1} \frac{m^{n-m+k+r-2}}{k!r!2^r}.$$

Доказательство. Пусть V_n — число гладких связных графов с n помеченными вершинами, а C_n — число связных графов с n помеченными вершинами. В [7] из работы Рида [6] была получена формула

$$V_n = \sum_{m=0}^{n} (-1)^{n-m} \frac{n!}{m!(n-m)!} m^{n-m} A_m,$$

где $A_m = C_m - m^{m-2}$.

Пусть Ca_m — число помеченных кактусов. В [5] была доказана формула:

$$Ca_m = m^{m-2} + (m-1)! \sum_{r=1}^{[\frac{m-1}{2}]} \sum_{k=0}^{m-2r-1} \binom{m-k-r-2}{r-1} \frac{m^{k+r-1}}{k!r!2^r}.$$

Заметим, что в [5] была допущена опечатка в формуле для числа помеченных кактусов Ca_m : был пропущен биномиальный коэффициент. Подставив в A_m вместо C_m выражение для Ca_m, получим утверждение теоремы. Теорема доказана.

Автор благодарит Воблого В. А. за поставленную задачу и ценные замечания.

Список литературы

1. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977. 324 с.
2. Wright E. M. Enumeration of smooth labelled graphs // Proc. of the Royal Society of Edinburgh. — 1982. — P. 205–212.
3. Ford G. W., Uhlenbeck .G. E. Combinatorial problems in theory graphs // Proc. Nat. Acad. Sci. USA. — 1956. — V. 42. — P. 122–128.
4. Воблый В. А. Об одной формуле для числа помеченных связных графов // Дискретный анализ и исследование операций. — 2012. — Т. 19, N 4. — С. 48–59.
5. Воблый В. А., Мелешко А. К. Новая формула для числа помеченных кактусов с заданным числом вершин // Тез. докл. Межд. науч. конфер. Дискретная математика и их приложения. — Минск. — 2013. — С. 9–11.
6. Read R. C. Some unusual enumeration problems // Ann. New York Acad. Sci. — 1970. — V. 175. — P. 314–326.
7. Воблый В. А. Асимптотическое перечисление графов некоторых типов // Дис. канд. физ.-мат. наук: 01.01.09. — Москва, ВЦ АН. — 1985. — 85 с.

О НЕКОТОРЫХ СВОЙСТВАХ ЗАМКНУТЫХ КЛАССОВ, ПОРОЖДЕННЫХ КВАЗИОДНОСЛОЙНЫМИ ФУНКЦИЯМИ ТРЕХЗНАЧНОЙ ЛОГИКИ

А. В. Михайлович (Москва)

Известно [1], что все замкнутые классы булевых функций имеют конечный базис. В [2] показано, что для функций k-значной логики при всех $k \geqslant 3$ существуют как замкнутые классы со счетным базисом, так и классы, не имеющие базиса. Стоит отметить, что функции в этих примерах принимают только два значения, например, 0 и 1, причем если набор содержит хотя бы одну нулевую компоненту, то значение функции на этом наборе равно нулю. Кроме того, эти функции являются симметрическими. В [3–5] рассмотрены различные семейства классов, порожденных симметрическими функциями. Для этих классов

получены критерии базируемости и конечной порожденности. В данной работе рассматривается семейство классов, порожденных квазиоднослойными функциями принимающими значения из множества $\{0,1\}$. Все необходимые определения можно найти в [3].

Обозначим через R множество всех функций трехзначной логики, принимающих только значения из множества $\{0,1\}$ и равных нулю на единичном наборе и на всех наборах, содержащих хотя бы одну нулевую компоненту. Пусть $f(x_1,\dots,x_n) \in P_3$. Будем обозначать через N_f множество всех наборов из E_3^n, на которых функция f принимает значение 1. Пусть $\widetilde{\alpha} \in \{1,2\}^n$. Обозначим через $|\widetilde{\alpha}|$ число единиц в наборе $\widetilde{\alpha}$. Пусть $\widetilde{\alpha}$, $\widetilde{\beta} \in \{1,2\}^n$. *Расстоянием* $\rho(\widetilde{\alpha},\widetilde{\beta})$ между наборами $\widetilde{\alpha}$ и $\widetilde{\beta}$ будем называть число компонент, в которых эти наборы различаются. Определим *квазислой* следующим образом $\mathcal{L}(\widetilde{\alpha},d) = \left\{\widetilde{\beta} \in \{1,2\}^n \mid \rho(\widetilde{\alpha},\widetilde{\beta}) = d\right\}$. Функцию $f(x_1,\dots,x_n)$ из множества R будем называть *квазиоднослойной*, если существуют набор $\widetilde{\alpha} \in \{1,2\}^n$ и число $d \leqslant n$, такие, что $N_f = \mathcal{L}(\widetilde{\alpha},d)$. Обозначим этот набор и это число через $\widetilde{\alpha}_f$ и d_f соответственно. Множество всех квазиоднослойных функций из R обозначим через QS^1.

На множестве попарно неконгруэнтных, т. е. не получающихся друг из друга переименованием переменных без отождествления, функций из QS^1 определим отношение порядка. Будем говорить, что $f \preceq g$, если $f \in [\{g\}]$. Множество попарно неконгруэнтных функций из QS^1 называется цепью, если любые два элемента этого множества сравнимы относительно порядка $\preceq$. Пусть G — множество попарно неконгруэнтных функций из QS^1, H — цепь, $H \subseteq G$. Цепь H называется максимальной цепью множества G, если для любой цепи $H_1 \subseteq QS^1$, такой, что $H \subseteq H_1$, $H \neq H_1$, цепь H_1 не является подмножеством множества G. Функция $f \in H$ называется верхней гранью цепи H, если для любой функции $g \in H$ выполняется неравенство $g \preceq f$. Цепь называется ограниченной, если она имеет верхнюю грань.

Будем называть произвольную формулу *простой*, если у нее нет подформулы, отличной от переменных.

Лемма 1. *Пусть $f \in QS^1$. Тогда каждая простая подформула любой формулы, реализующей функцию f над QS^1, также реализует фукнцию f.*

Доказательство. Пусть простая подформула формулы над QS^1, реализующей фукцнию $f(x_1,\dots,x_n)$, в свою очередь реализует функцию $h(x_1,\dots,x_n)$. Тогда существует фукнция $g(x_1,\dots,x_m)$ из QS^1, такая, что $h(x_1,\dots,x_n) = g(x_{i_1},\dots,x_{i_m})$. Без ограничения общности будем считать, что имеет место $\widetilde{\alpha}_f = (1^{k_f},2^{n-k_f})$, $\widetilde{\alpha}_g = (1^{k_g},2^{m-k_g})$; среди $x_{i_1},\dots,x_{i_{k_g}}$ переменная x_1 встречается q_1 раз, переменная x_2 — q_2 раза, …, переменная x_n — q_n раз, среди $x_{i_{k_g+1}},\dots,x_{i_m}$ переменная x_1 встречается r_1 раз, переменная x_2 — r_2 раза, …, переменная x_n — r_n раз, $k_f \leqslant n - k_f$.

Пусть $\widetilde{\beta} \in \{1,2\}^n$. Обозначим через $\widetilde{\gamma}(\widetilde{\beta})$ набор $(\beta_{i_1}, \ldots, \beta_{i_m})$. Поскольку все функции из QS^1 равны нулю на наборах, содержащих хотя бы одну нулевую компоненту, то из соотношения $\widetilde{\beta} \in N_f$ следует, что $\widetilde{\gamma}(\widetilde{\beta}) \in N_g$.

Рассмотрим пару наборов из N_f, которые различаются только в j-й и k-й компонентах, $1 \leqslant j \leqslant n$, $1 \leqslant k \leqslant n$. Рассмотрим два случая.

1. Пусть $1 \leqslant j < k \leqslant k_f$ или $k_f + 1 \leqslant j < k \leqslant n$. Рассмотрим наборы $\widetilde{\beta}^1$, $\widetilde{\beta}^2 \in N_f$, такие, что $\beta_i^1 = \beta_i^2$ при всех $1 \leqslant i \leqslant n$, $i \neq j$, $i \neq k$, $\beta_j^1 = \beta_k^2 = 1$, $\beta_k^1 = \beta_j^2 = 2$. Нетрудно видеть, что $\rho(\widetilde{\alpha}_g, \widetilde{\gamma}(\widetilde{\beta}^1)) = \rho(\widetilde{\alpha}_g, \widetilde{\gamma}(\widetilde{\beta}^2))$. Поэтому $q_k - q_j = r_k - r_j$. А значит, $q_k - r_k = q_j - r_j$.

2. Пусть теперь $1 \leqslant j \leqslant k_f$ и $k_f + 1 \leqslant k \leqslant n$. Рассмотрим наборы $\widetilde{\beta}^1$, $\widetilde{\beta}^2 \in N_f$, такие, что $\beta_i^1 = \beta_i^2$ при всех $1 \leqslant i \leqslant n$, $i \neq j$, $i \neq k$, $\beta_j^1 = \beta_k^1 = 1$, $\beta_j^2 = \beta_k^2 = 2$. Нетрудно видеть, что $\rho(\widetilde{\alpha}_g, \widetilde{\gamma}(\widetilde{\beta}^1)) = \rho(\widetilde{\alpha}_g, \widetilde{\gamma}(\widetilde{\beta}^2))$. Поэтому $q_j + q_k = r_j - r_k$. А значит, $q_k - r_k = -(q_j - r_j)$.

Итак, в обоих случаях установлено, что разность $q_i - r_i$ зависит только от того, выполняется неравенство $i \leqslant k_f$ или $i > k_f$. Положим $\Delta = q_i - r_i$ при $1 \leqslant i \leqslant k_f$. Отметим, что $\Delta = r_i - q_i$ при $k_f + 1 \leqslant i \leqslant n$. Покажем, что $\Delta \neq 0$. Предположим, что $\Delta = 0$. Поскольку на наборах, содержащих хотя бы одну нулевую компоненту, функции из QS^1 равны нулю, то $N_f \subseteq N_h$. Рассмотрим набор $\widetilde{\beta} \in N_f$ и набор $\widetilde{\beta}'$, такой, что для некоторого i, $1 \leqslant i \leqslant n$, $\beta_i' = 3 - \beta_i$ и $\beta_j = \beta_j'$ для всех $j \neq i$. Из определения набора $\widetilde{\beta}'$ следует, что

$$|\rho(\widetilde{\gamma}(\widetilde{\beta}), \widetilde{\alpha}_g) - \rho(\widetilde{\gamma}(\widetilde{\beta}'), \widetilde{\alpha}_g)| = |q_i - r_i| = 0.$$

Следовательно, $\widetilde{\gamma}(\widetilde{\beta}') \in N_g$. А значит, $\widetilde{\beta}' \in N_h$. Таким образом показано, что набор, находящийся на расстоянии 1 от набора из N_f, содержится в N_h. Аналогичным образом за конечное число шагов для любого набора из $\{1,2\}^n$ можно показать, что он содержится в N_h, рассматривая вместо набора $\widetilde{\beta}$ некоторый набор, про который уже установлено, что он содержится в N_h. Следовательно, $(1^n) \in N_g$, что противоречит определению функции g. А значит, $\Delta \neq 0$.

Покажем теперь, что $N_h = N_f$. Очевидно, что $N_f \subseteq N_h$. Пусть $N_f \neq N_h$. Выберем произвольный набор $\widetilde{\sigma}$ из $N_h \backslash N_f$. Пусть набор $\widetilde{\beta}^1$ из N_f такой, что величина $\rho(\widetilde{\beta}^1, \widetilde{\sigma})$ минимальна. Поскольку $\rho(\widetilde{\gamma}(\widetilde{\beta}^1), \widetilde{\alpha}_g) = \rho(\widetilde{\gamma}(\widetilde{\sigma}), \alpha_g)$, то получаем, что $q_i - r_i = 0$ для всех i таких, что $\beta_i^1 \neq \sigma_i$. А значит, $\Delta = 0$. Получили противоречие. Следовательно, $N_h = N_g$. Лемма доказана.

Следствие 1. *Пусть* $f(x_1, \ldots, x_n), g(x_1, \ldots, x_m) \in QS^1$, $g(x_{i_1}, \ldots, x_{i_m})$ — *простая подформула некоторой формулы над* QS^1, *реализующей функцию* f. *Тогда* $n \leqslant m$.

Поскольку функции из множества QS^1 на наборах, содержащих хотя бы одну нулевую компоненту равны нулю, имеет место следствие.

Следствие 2. *Пусть* $f \in QS^1$. *Тогда каждая подформула любой формулы, реализующей функцию* f *над* QS^1, *также реализует фукнцию* f.

Теорема 1. *Пусть F — множество попарно неконгруэнтных функций из QS^1. Тогда выполняются следующие утверждения.*

1. *Класс $[F]$ конечный имеет базис тогда и только тогда, когда множество F конечно.*

2. *Класс $[F]$ имеет счетный базис тогда и только тогда, когда множество F бесконечно и каждая функция из F содержится в ограниченной максимальной цепи множества F.*

3. *Класс $[F]$ не имеет базиса тогда и только тогда, когда существует функция h из F, которая не содержится ни в какой ограниченной максимальной цепи множества F.*

Доказательство. 1. Очевидно, что если число неконгруэнтных функций в множестве F конечно, то $[F]$ имеет конечный базис. Пусть теперь класс $[F]$ имеет конечный базис $\mathfrak{A}$. Без ограничения общности будем считать, что $\mathfrak{A} \subseteq F$. Пусть n_0 — максимальное число существенных переменных у функций из $\mathfrak{A}$. Тогда в силу следствия 1 число существенных переменных у функций из $[\mathfrak{A}] \cap QS^1$ не превосходит n_0. Поскольку F — множество попарно неконгруэнтных функций и $F \subseteq [\mathfrak{A}]$, то множество F конечно.

2. Пусть класс $[F]$ имеет счетный базис $\mathfrak{A}$. Каждой функции f из $\mathfrak{A}$ сопоставим формулу Υ_f над F, реализующую функцию f. Пусть Φ — произвольная формула над $\mathfrak{A}$. Заменим в формуле Φ каждую из функций базиса $\mathfrak{A}$ на соответствующую ей подформулу над F. Полученную формулу над F обозначим через $\pi(\Phi)$.

Пусть $g \in F$, Φ_g — формула над $\mathfrak{A}$, реализующая функцию g. Из леммы 1 следует, что все простые подформулы формулы $\pi(\Phi_g)$ имеют вид $g'(x_{i_1}, ..., x_{i_p})$, где $g \preceq g'$. Следовательно, для любой функции g из F существует функция f из $\mathfrak{A}$, такая, что простые подформулы формулы Υ_f имеют вид $g'(x_{i_1}, \ldots, x_{i_p})$, где $g \leqslant g'$. Из следствия 2 получаем, что любая подформула формулы $\pi(\Phi_g)$ реализует функцию g. А значит, существует функция $f_g \in \mathfrak{A}$, такая, что $g \in [\{f_g\}]$.

Предположим, что существует функция h, которая не содержится ни в какой ограниченной максимальной цепи множества F. Пусть Φ_h — формула над $\mathfrak{A}$, реализующая функцию h. Пусть $f_h(x_{i_1}, \ldots, x_{i_p})$ — простая подформула формулы Φ_h, такая что $h \in [\{f_h\}]$. Покажем, что $f_h \in [\mathfrak{A} \backslash \{f_h\}]$. Рассмотрим формулу Υ_{f_h}. Пусть $g(\Psi_1, \ldots, \Psi_m)$ — подформула формулы Υ_{f_h}, $\Psi_1, \ldots, \Psi_m$ — формулы над F, $g \in F$. Рассмотрим два случая.

Пусть $g(\Psi_1, \ldots, \Psi_m)$ — простая подформула. Тогда, как показано выше, функция g не содержится ни в какой ограниченной максимальной цепи множества F. Пусть $g(x_1, \ldots, x_m) \prec g'(x_1, \ldots, x_r)$, причем $g' \in F$ и $r > 2p$. Используя следствие 1, получаем, что $g' \in [\mathfrak{A} \backslash \{f\}]$. Следовательно, $g \in [\mathfrak{A} \backslash \{f\}]$.

Пусть теперь формула $g(\Psi_1, \ldots, \Psi_m)$ не является простой. Пусть также $h \not\preceq g$ (случай $h \preceq g$ сводится к рассмотренному выше). Тогда существует функция $f_g \in \mathfrak{A}$ такая, что $g \in [\{f_g\}]$ и $h \notin [\{f_g\}]$. Следовательно,

$f_h \notin [\{\mathfrak{A}\backslash\{f_h\}]$. Это противоречит определению базиса. А значит, не существует функции, которая не содержится ни в какой ограниченной максимальной цепи множества F.

Покажем теперь, что если каждая функция из множества F содержится в некоторой ограниченной максимальной цепи множества F, то класс $[F]$ имеет базис. Пусть $\mathfrak{A} \subseteq F$ — множество всех (попарно неконгруэнтных) функций, являющихся верхними гранями ограниченных максимальных цепей множества F. Очевидно, что все функции из $\mathfrak{A}$ попарно несравнимы. Поскольку каждая функция из множества F содержится в некоторой ограниченной максимальной цепи множества F, то $[\mathfrak{A}] = [F]$. Далее покажем, что для любой функции $g(x_1, \ldots, x_p) \in \mathfrak{A}$ выполняется соотношение $g \notin [\mathfrak{A}\backslash\{g\}]$. Предположим, что это не так. Пусть формула $\Phi(x_1, \ldots, x_p)$ над $\mathfrak{A}\backslash\{g\}$ реализует функцию g. Пусть некоторая простая подформула формулы Φ имеет вид $f(x_{i_1}, \ldots, x_{i_n})$, $f \in \mathfrak{A}\backslash\{g\}$. Тогда в силу леммы 1 выполняется соотношение $g \preceq f$. Получили противоречие с тем, что все функции множества $\mathfrak{A}$ несравнимы. Следовательно, $g \notin [\mathfrak{A}\backslash\{g\}]$, т. е. $\mathfrak{A}$ — базис класса F. Таким образом, достаточность для п.2 доказана.

3. Следует из пп.1 и 2.

Данное научное исследование (№ 14-01-0144) выполнено при поддержке Программы «Научный фонд НИУ ВШЭ» в 2014/2015 гг.

Список литературы

1. Post E. L. The two-valued iterative systems of mathematical logic // Annals of Math. Studies. — Princeton Univ. Press, 1941.
2. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.
3. Михайлович А. В. О замкнутых классах функций многозначной логики, порожденных симметрическими функциями // Математические вопросы кибернетики. Вып. 18. — М. : Физматлит, 2013. — С. 123–212.
4. Михайлович А. В. О замкнутых классах функций в P_3, порожденных периодическими симметрическими функциями // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2013. — № 1. — С. 208–212.
5. Михайлович А. В. О классах функций трехзначной логики, порожденных симметрическими функциями с ограниченным числом слоев // Прикладная дискретная математика. — 2015. — № 1. — С. 17–26.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ В ОДНОМ БЕСКОНЕЧНОМ БАЗИСЕ

О. В. Подольская (Москва)

Базисом называется произвольное функционально полное множество булевых функций. Базис называется бесконечным, если содержит функции, существенно зависящие от сколь угодно большого числа переменных (см., например, [4]).

Сложностью схемы называется количество функциональных элементов в этой схеме, а сложностью функции — сложность минимальной схемы, реализующей эту функцию. Для функции f будем обозначать ее сложность через $L(f)$. Подробнее с понятиями схемы и сложности можно ознакомиться, например, в [1].

Антицепью булева куба называется множество попарно несравнимых наборов булева куба. Будем называть слоем булева куба $\{0,1\}^n$ с номером t, где $t \in \{0,1,\ldots,n\}$, множество всех наборов, содержащих t единичных компонент. Ясно, что всякий слой является антицепью.

Булевы функции, принимающие значение 1 лишь на антицепях булева куба, называются антицепными. Множество антицепных функций от любого числа переменных образует бесконечный базис. Этот базис называется базисом антицепных функций и обычно обозначается через AC, см. [2, 3].

Функцией четности p_n от n переменных называется булева функция $x_1 + \ldots + x_n \pmod 2$. Функцией голосования m_n от n переменных называется булева функция, равная 1 лишь на наборах, в которых количество единичных компонент не менее $n/2$.

Функция называется симметрической, если ее значение не изменяется при произвольной перестановке ее переменных. Далее, говоря о симметрических функциях, будем иметь в виду симметрические булевы функции. В частности, функции четности и голосования являются симметрическими.

Всякая симметрическая функция задается слоями, т. е. для того, чтобы задать симметрическую функцию, достаточно сказать, на каких слоях она равна 1. Для симметрической функции f от n переменных через $k(f)$ будем обозначать количество различных слоев булева куба $\{0,1\}^n$, на которых f равна 1.

Рассматривается задача о сложности реализации симметрических функций схемами из функциональных элементов в базисе антицепных функций.

Изучение задачи о реализации булевых функций схемами в базисе антицепных функций началось с работ О. М. Касим-Заде [2, 3]. В [2] была установлена верхняя оценка $n+1$ сложности произвольной булевой функций от n

переменных. Также в [2] для функции четности от n переменных была получена нижняя оценка порядка $n^{1/3}$, а затем в [3] для этой же функции была получена более сильная нижняя оценка — порядка $\sqrt{n/\ln n}$.

В работе автора [5] последнюю оценку удалось улучшить и доказать для функции четности от n переменных нижнюю оценку сложности порядка $\sqrt{n}$, а также доказать такую же по порядку нижнюю оценку сложности функции голосования от n переменных и почти всех булевых функций от n переменных (имеется в виду, что доля булевых функций, для которых рассматриваемая оценка не выполнена, среди всех булевых функций от n переменных, стремится к нулю при n стремящемся к бесконечности).

В [6] доказана верхняя оценка n сложности произвольной булевой функции от n переменных. С использованием той же идеи в [7] доказана верхняя оценка сложности произвольной симметрической функции f от n переменных, $f \not\equiv 0$: $L(f) \leqslant \min(k(f), n - k(f) + 2)$. Также в [7] изложен новый метод, с помощью которого доказана нижняя оценка сложности произвольной симметрической функции f от n переменных: $L(f) \geqslant \min(k(f), n - k(f) + 2)$. Тем самым в [7] доказано следующее утверждение.

Теорема 1. *Для произвольной симметрической функции f, отличной от константы 0, выполнено равенство $L(f) = \min(k(f), n - k(f) + 2)$.*

Сложность функции f, такой что $f \equiv 0$, равна 1. Таким образом установлена сложность реализации схемами в базисе AC всех симметрических функций.

Из теоремы 1 несложно выводится следующее утверждение.

Теорема 2. *Для функции четности и функции голосования от n переменных, $n \geqslant 2$, выполнены равенства $L(p_n) = \lfloor \frac{n+1}{2} \rfloor$, $L(m_n) = \lfloor \frac{n}{2} \rfloor + 1$.*

Учитывая, что в соответствии с [6], любая функция от n переменных реализуется со сложностью не больше n, из теоремы 2, в частности, следует, что указанная верхняя оценка по порядку не улучшаема.

Работа выполнена при поддержке РФФИ (проект № 14-01-00598-а) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.
2. Касим-Заде О. М. О сложности схем в одном бесконечном базисе // Вестник Московского университета, Сер. 1. Математика. Механика. — 1994. — № 6. — С. 40–44.

3. Касим-Заде О. М. О сложности реализации булевых функций схемами в одном бесконечном базисе // Дискретный анализ и исследование операций. — 1995. — Т. 2, вып. 1. — С. 7–20.
4. Касим-Заде О. М. Об одном методе получения оценок сложности схем над бесконечными базисами // Математические вопросы кибернетики. Вып. 11. — 2002. — С. 247–254.
5. Подольская О. В. О нижних оценках сложности схем в базисе антицепных функций // Вестник Московского университета, Сер. 1. Математика. Механика. — 2013. — № 2. — С. 17–23.
6. Подольская О. В. Об оценках сложности схем в одном бесконечном базисе // Материалы IX Молодежной научной школы по дискретной математике и ее приложениям (16–23 сентября 2013 г.). — Москва, 2013. — С. 97–100.
7. Подольская О. В. Сложность реализации симметрических булевых функций схемами в базисе антицепных функций // Дискретная математика. — 2015. — Т. 27, вып. 3. — С. 95–107.

ОЦЕНКИ ДЛИН ТЕСТОВ ДЛЯ КОНТАКТОВ

К. А. Попков (Москва)

Введение

Рассматриваются задачи проверки исправности и распознавания состояний контактов с использованием экспериментов, заключающихся в составлении из заданных контактов произвольных двухполюсных контактных схем с последующим «прозваниванием» этих схем, т. е. нахождением булевых функций, реализуемых составляемыми схемами. Описания физических принципов работы релейно-контактных схем и тех явлений, которые наблюдаются при работе таких схем, можно найти, например, в монографиях [1, 2]. Суть общепринятых математических моделей контактной схемы и тех элементов (т. е. контактов), из которых строятся эти схемы, с исчерпывающей полнотой и ясностью представлена в [3]; именно такая математическая модель является объектом исследования и рассматривается ниже.

Опишем постановку задачи, как это сделано в [4]. Представим, что имеются N контактов ($N \geqslant 1$), занумерованных числами от 1 до N, из которых N_1 контактов с номерами от 1 до N_1 являются замыкающими, а N_2 контактов с номерами от $N_1 + 1$ до N — размыкающими, где $N_2 = N - N_1$ (N_1 или N_2 может быть равно 0). В исправном состоянии каждый замыкающий контакт, рассматриваемый как простейшая контактная схема, реализует между своими концами (полюсами схемы) булеву функцию x_i, а размыкающий контакт — булеву функцию $\overline{x_i}$, где x_i — отвечающая данному контакту переменная. Число

замыкающих контактов (N_1), и соответственно, число размыкающих контактов (N_2) предполагаются известными. В неисправном состоянии каждый контакт реализует между своими концами одну из булевых констант, т. е. 0 (при обрыве контакта) или 1 (при замыкании контакта). Предполагается, что среди данных N контактов не более k контактов могут быть неисправны, где k — заданное натуральное число, $k \leqslant N$. Можно составлять любые двухполюсные контактные схемы из данных контактов и наблюдать выдаваемые схемами значения на любых наборах значений переменных.

Задача заключается в том, чтобы протестировать контакты, т. е. для каждого из них определить, исправен данный контакт или неисправен (задача проверки), и, в дополнение к этому, определить тип неисправности каждого неисправного контакта (задача диагностики), используя при тестировании по возможности меньшее число схем.

Предполагается, что в процессе экспериментирования исправные контакты остаются исправными, неисправные контакты — неисправными и тип неисправности каждого неисправного контакта сохраняется.

1. Основные определения и вспомогательные утверждения

Диагностическим тестом назовем такой набор двухполюсных контактных схем $S_1, \ldots, S_l$, составленных из заданных контактов, что по набору функций, реализуемых этими схемами, можно однозначно определить состояние каждого из N контактов. Число l назовем *длиной* этого теста.

Проверяющим тестом назовем такой набор двухполюсных контактных схем $S_1, \ldots, S_l$, составленных из заданных контактов, что по набору функций, реализуемых этими схемами, можно однозначно определить исправность или неисправность каждого из N контактов. Число l назовем *длиной* этого теста.

Отметим, что проверяющий тест, в отличие от диагностического, не обязан определять тип неисправности (обрыв или замыкание) каждого неисправного контакта.

Введем функции $L_c(N_1, N_2, k)$ и $L_d(N_1, N_2, k)$, равные длинам самого короткого, соответственно, проверяющего и диагностического тестов для N_1 замыкающих и N_2 размыкающих контактов, среди которых не более чем k неисправных. Пусть $L_c(N, k) = L_c(N, 0, k)$ и $L_d(N, k) = L_d(N, 0, k)$.

Введенные определения полностью согласуются с соответствующими определениями из [4] при замене $L_d(N_1, N_2, k)$ на $L(N_1, N_2, k)$.

Ранее (см. утверждение 2 в [4]) были доказаны равенства $L_d(N_1, N_2, k) = L_d(N_1 + N_2, 0, k) = L_d(N, 0, k) = L_d(N, k)$. Совершенно аналогично можно доказать равенства $L_c(N_1, N_2, k) = L_c(N_1 + N_2, 0, k) = L_c(N, 0, k) = L_c(N, k)$. Из выписанных равенств следует, что для нахождения значений $L_c(N_1, N_2, k)$ и $L_d(N_1, N_2, k)$ достаточно знать только $L_c(N, k)$ и $L_d(N, k)$. Поэтому далее, без ограничения общности, будем считать, что все заданные контакты замыкающие.

Отметим, что, поскольку любой диагностический тест, очевидно, является проверяющим, для любых N и k выполняется соотношение $L_d(N,k) \geqslant L_c(N,k)$.

В качестве тривиального диагностического (и проверяющего) теста (длины N), очевидно, можно взять множество из N контактных схем, каждая из которых представляет собой один из заданных контактов.

2. Ранее полученные результаты

В [4] доказано, что при выполнении условий $N \geqslant 36$ и $2k\lceil\sqrt{k}\rceil \leqslant N$ справедливо неравенство $L_d(N,k) \leqslant k+1$. В [5] получены равенства

$$L_c(N,1) = L_d(N,1) = \begin{cases} 1, & \text{если } N = 1 \text{ или } N \geqslant 5, \\ 2, & \text{если } N \in \{2,3,4\}. \end{cases}$$

3. Формулировки основных теорем

Пусть N и k зафиксированы. Введем следующую последовательность чисел: $r_1 = \lfloor\sqrt{N}\rfloor$, $r_{i+1} = \left\lfloor\sqrt{N - \sum\limits_{j=1}^{i} r_j}\right\rfloor$ для $i \geqslant 1$, если $\sum\limits_{j=1}^{i} r_j < N$.

Теорема 1. *Если t — такое натуральное число, что все числа $r_1, \ldots, r_t$ определены и $\sum\limits_{i=1}^{t} r_i \leqslant k-1$, то $L_c(N,k) \geqslant t+1$ и $L_d(N,k) \geqslant t+1$.*

Следствие. *Для любых N и k справедливы неравенства $L_c(N,k) \geqslant \frac{k}{\lfloor\sqrt{N}\rfloor}$ и $L_d(N,k) \geqslant \frac{k}{\lfloor\sqrt{N}\rfloor}$.*

Теорема 2. *Пусть $k < N$ и $r = \left\lfloor\frac{k-1}{N-k}\right\rfloor$. Тогда имеет место $L_c(N,k) \geqslant r + L_c(N - r(N-k), k - r(N-k))$ и $L_d(N,k) \geqslant r + L_d(N - r(N-k), k - r(N-k))$.*

Следствие 1. *Если $k < N$, то $L_c(N,k) \geqslant \frac{k}{N-k}$ и $L_d(N,k) \geqslant \frac{k}{N-k}$.*

Следствие 2. *При всех $N \geqslant 2$ справедливы равенства $L_c(N,N-1) = L_d(N,N-1) = L_c(N,N) = L_d(N,N) = N$.*

Доказательства указанных теорем и следствий приведены в [6].

Автор выражает глубокую благодарность своему научному руководителю профессору Н. П. Редькину за постановку задачи и внимание к работе.

Список литературы

1. Гаврилов М. А. Теория релейно-контактных схем. — М.-Л., 1950.
2. Колдуэлл С. Логический синтез релейных устройств. — М.: ИЛ, 1962.
3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

4. Попков К. А. Диагностика состояний контактов // Дискретная математика. — 2013. — Т. 25, вып. 4. — С. 30–40.
5. Попков К. А. О единичных тестах для контактов // Вестник Московского университета. Серия 1. Математика. Механика. — 2015. — №5. — С. 13–18.
6. Попков К. А. Оценки длин проверяющих и диагностических тестов для контактов // Известия вузов. Поволжский регион. Физико-математические науки. — 2015. — №2. — С. 108–121.

О СЛОЖНОСТИ И ГЛУБИНЕ ФОРМУЛ ДЛЯ MOD-ФУНКЦИЙ

И. С. Сергеев (Москва)

Введение

В настоящей заметке рассматриваются сложность и глубина реализации функций многократного сложения по модулю m — MOD-функций — формулами в стандатном базисе $B_0 = \{\vee, \wedge, {}^-\}$ и в базисе B_2 всех бинарных булевых функций.

Через MOD_n^m обозначим булев (n, m)-оператор сложения n одноразрядных чисел по модулю m. Компоненты оператора, называемые MOD-функциями, определяются как

$$\mathrm{MOD}_n^{m,r}(x) = \left(\sum_{i=1}^{n} x_i \equiv r \bmod m \right),$$

$r = 0, \ldots, m-1$, где $x = (x_1, \ldots, x_n)$.

Понятия формулы, глубины и сложности см. в [1, 7]. Сложность и глубину реализации булевого оператора f формулами над базисом B обозначим через $L_B(f)$ и $D_B(f)$ соответственно.

Универсальный способ реализации MOD-функций заключается в вычислении арифметической суммы $C_n = x_1 + \ldots + x_n$ и применении простых соотношений

$$L_B(\mathrm{MOD}_n^{m,r}) \preceq n^{o(1)} L_B(C_n), \qquad D_B(\mathrm{MOD}_n^{m,r}) \leqslant D_B(C_n) + o(\log n),$$

справедливых в произвольном полном базисе B (знак $\preceq$ означает неравенство по порядку).

Сложность и глубина оператора C_n удовлетворяют неконструктивно выводимым оценкам

$$L_{B_0}(C_n) \preceq n^{3,91},\ L_{B_2}(C_n) \preceq n^{2,84},\ D_{B_0}(C_n) \lesssim 4,14 \log n,\ D_{B_2}(C_n) \lesssim 3,02 \log n$$

и конструктивным оценкам

$$L_{B_0}(C_n) \preceq n^{4{,}47},\ L_{B_2}(C_n) \preceq n^{3{,}03},\ D_{B_0}(C_n) \lesssim 4{,}87\log n,\ D_{B_2}(C_n) \lesssim 3{,}34\log n$$

(знак $\lesssim$ означает асимптотическое неравенство; основание у двоичных логарифмов здесь и далее опускается) [2, 3].

Для конкретных MOD-функций известны лучшие оценки. Основной интерес представляет случай простых нечетных модулей m. Вопрос о сложности линейных функций ($m = 2$) фактически закрыт [4]; сложность MOD-функций с составным модулем m определяется сложностью MOD-функций с модулями простых делителей числа m, см. [6, 8].

Известные нижние оценки имеют вид $L_{B_0}(\mathrm{MOD}_n^m) = \Omega(n^2)$ (следует из [4]) и $L_{B_2}(\mathrm{MOD}_n^m) = \Omega(n\log n)$ при $m > 2$ [6]. Оценки глубины получаются применением стандартного для бинарных базисов соотношения $D_B(f) \geqslant \log L_B(f)$.

Нетривиальные верхние оценки для некоторых значений m получены в [5, 6, 8, 9] (приводятся ниже).

1. Обзор известных результатов

Для вывода оценок в базисе B_0 используются следующие простые формулы [5]:

$$\mathrm{MOD}_{n_1+n_2}^{m,r}(x) = \bigvee_{k=0}^{m-1} \mathrm{MOD}_{n_1}^{m,k}(x^1)\cdot \mathrm{MOD}_{n_2}^{m,r-k}(x^2), \tag{1}$$

$$\mathrm{MOD}_{n_1+n_2}^{m,r}(x) = \bigwedge_{k=0}^{m-1} \left(\mathrm{MOD}_{n_1}^{m,k}(x^1) \vee \overline{\mathrm{MOD}_{n_2}^{m,r-k}(x^2)}\right), \tag{2}$$

где $x = (x^1, x^2)$, $|x^i| = n_i$. Из них непосредственно вытекают оценки

$$L_{B_0}(\mathrm{MOD}_n^m) \preceq n^{1+\log m}, \qquad D_{B_0}(\mathrm{MOD}_n^m) \lesssim \lceil 1+\log m\rceil \cdot \log n. \tag{3}$$

Комбинируя (1) и (2), в [5] получены уточнения оценки глубины в специальных случаях:

$$D_{B_0}(\mathrm{MOD}_n^3) < 2{,}89\log n + O(1), \qquad D_{B_0}(\mathrm{MOD}_n^5) < 3{,}48\log n + O(1).$$

В базисе B_2 справедливы более короткие формулы [8]:

$$\mathrm{MOD}_{n_1+n_2}^{m,r}(x) = \bigwedge_{k=1}^{m-1} \left(\mathrm{MOD}_{n_1}^{m,k}(x^1) \sim \mathrm{MOD}_{n_2}^{m,r-k}(x^2)\right),$$

где «$\sim$» означает булеву операцию эквивалентности. Поэтому справедливы оценки

$$L_{B_2}(\mathrm{MOD}_n^m) \preceq n^{1+\log(m-1)}, \qquad D_{B_2}(\mathrm{MOD}_n^m) \lesssim \lceil 1+\log(m-1)\rceil \cdot \log n. \tag{4}$$

В работе [9] предложено использовать изоморфизм между $(\mathbb{Z}_{2^k-1}, +)$ и мультипликативной группой $GF(2^k)^*$. Сложение по модулю $m \mid 2^k - 1$ заменяется умножением в поле $GF(2^k)$, элементы которого представляются двоичными матрицами размера $k \times k$. Получаются оценки

$$L_{B_2}(\mathrm{MOD}_n^m) \preceq n^{1+\log k}, \qquad D_{B_2}(\mathrm{MOD}_n^m) \lesssim \lceil 1 + \log k \rceil \cdot \log n. \tag{5}$$

2. Новые результаты

Определим расширенную кодировку группы $(\mathbb{Z}_m, +)$, состоящую из функций

$$\mathrm{MOD}_n^{m,S}(x) = \left(\sum_{i=1}^{n} x_i \bmod m \in S \right),$$

где $S \subset \mathbb{Z}_m$. Будем искать формулы вида

$$\mathrm{MOD}_n^{m,S}(x) = \bigvee_{k=1}^{t} \mathrm{MOD}_{n_1}^{m,A_k}(x^1) \cdot \mathrm{MOD}_{n_2}^{m,B_k}(x^2). \tag{6}$$

Множеству S поставим в соответствие $(m,m)-$матрицу I_m^S, строки и столбцы которой занумерованы числами из $\mathbb{Z}_m$, а элементы определяются как $I_m^S[i,j] = (i + j \in S)$. Тогда формула (6) отвечает покрытию матрицы I_m^S сплошь единичными подматрицами (прямоугольниками) со строками A_k и столбцами B_k.

Из (1) вытекает тривиальное тождество

$$\mathrm{MOD}_{n_1+n_2}^{m,S}(x) = \bigvee_{k=0}^{m-1} \mathrm{MOD}_{n_1}^{m,k}(x^1) \cdot \mathrm{MOD}_{n_2}^{m,S-k}(x^2), \tag{7}$$

отвечающее покрытию матрицы отдельными строками. Ранг тривиального покрытия (число покрывающих матриц) равен m. Однако можно указать матрицы I_m^S с рангом минимального покрытия (или OR-рангом) $\mathrm{rk}_\vee(I_m^S) < m$.

Стандартным примером циклической матрицы малого ранга является матрица с нулевой циклической диагональю (см., например, [7]). Ранг такой матрицы асимптотически равен $\log m$. При малых m и $|S| = m - 1$ имеем $\mathrm{rk}_\vee(I_5^S) = 4$, $\mathrm{rk}_\vee(I_7^S) = 5$. Используя (7) с соответствующими покрытиями в комбинации с (1), (2), (6), устанавливается

Теорема 1. *Справедливы оценки*:

$$L_{B_0}(\mathrm{MOD}_n^5) \preceq n^{3,22}, \qquad L_{B_0}(\mathrm{MOD}_n^7) \preceq n^{3,63},$$

$$D_{B_0}(\mathrm{MOD}_n^5) < 3,35 \log n + O(1), \qquad D_{B_0}(\mathrm{MOD}_n^7) < 3,87 \log n + O(1).$$

В некоторых случаях эффективный способ построения формул возможен при разбиении набора переменных на три части.

Пусть $x = (x^1, x^2, x^3)$, $|x^i| = n_i$, $|x| = n$. Введем сокращенное обозначение $F_i^r = \mathrm{MOD}_{n_i}^{3,r}(x^i)$. Справедлива формула

$$\mathrm{MOD}_n^{3,r}(x) = (F_1^0 \vee F_2^0 \vee F_3^r)(F_1^1 \vee F_2^1 \vee F_3^{r+1})(F_1^2 \vee F_2^2 \vee F_3^{r+2}) \vee \\ \vee (F_1^0 \vee F_2^2 \vee F_3^{r+1})(F_1^1 \vee F_2^0 \vee F_3^{r+2})(F_1^2 \vee F_2^1 \vee F_3^r), \quad (8)$$

которую можно переписать в виде

$$\mathrm{MOD}_n^{3,r}(x) = (F_1^0 \vee F_2^0 \vee F_3^r)(F_1^1 \vee F_2^1 \vee F_3^{r+1})(F_1^2 \vee F_2^2 \vee F_3^{r+2}) \vee \\ \vee F_1^0 \cdot F_2^0 \cdot F_3^r \vee F_1^1 \cdot F_2^1 \cdot F_3^{r+1} \vee F_1^2 \cdot F_2^2 \cdot F_3^{r+2}. \quad (9)$$

В случае $m = 7$ удобные формулы строятся, отталкиваясь от представления из [9]. Положим $T = \{0, 1, 2, 5\} \subset \mathbb{Z}_7$. Введем обозначение $F_i^r = \mathrm{MOD}_{n_i}^{7,T+r}(x^i)$. Тогда выполняется тождество

$$\mathrm{MOD}_n^{7,T+r}(x) = \bigoplus_{k=0}^{6} F_1^k \cdot F_2^k \cdot \overline{F_3^{3+r-2k}}. \quad (10)$$

Используя (8), (9) и (10), доказывается

Теорема 2. *Справедливы оценки*:

$$D_{B_0}(\mathrm{MOD}_n^3) < 2,8 \log n + O(1), \qquad D_{B_2}(\mathrm{MOD}_n^7) < 2,93 \log n + O(1).$$

Лучшие результаты о сложности и глубине операторов MOD_n^m сведены в таблицу.

m	L_{B_0}	L_{B_2}	D_{B_0}	D_{B_2}
3	$n^{2,59}$, (3)	n^2 [6, 9], (4, 5)	$2,8 \log n$, т. 2	$2 \log n$ [8], (4, 5)
5	$n^{3,22}$, т. 1	$n^{2,84}$ (неконстр.) n^3 [9], (4, 5)	$3,35 \log n$, т. 1	$3 \log n$, (4, 5)
7	$n^{3,63}$, т. 1	$n^{2,59}$ [9], (5)	$3,87 \log n$, т. 1	$2,93 \log n$, т. 2

Работа выполнена при поддержке РФФИ, проект № 14-01-00671а.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Сергеев И. С. Верхние оценки сложности формул для симметрических булевых функций // Известия высших учебных заведений. Математика. — 2014. — №5. — С. 38–52.
3. Сергеев И. С. Верхние оценки глубины симметрических булевых функций // Вестник МГУ. Серия 15. Вычислительная математика и кибернетика. — 2013. — №4. — С. 39–44.
4. Храпченко В. М. Об одном методе получения нижних оценок сложности π-схем // Математические заметки. — 1971. — Т. 10(1). — С. 83–92.
5. Chin A. On the depth complexity of the counting functions // Information Processing Letters. — 1990. — V. 35. — P. 325–328.
6. Fischer M. J., Meyer A. R., Paterson M. S. $\Omega(n \log n)$ lower bounds on length of Boolean formulas // SIAM Journal on Computing. — 1982. — V. 11(3). — P. 416–427.
7. Jukna S. Boolean function complexity. — Berlin, Heidelberg: Springer-Verlag, 2012.
8. McColl W. F. Some results on circuit depth. Report №18. — Coventry: Univ. of Warwick, 1977.
9. van Leijenhorst D. C. A note on the formula size of the "mod k" functions // Information Processing Letters. — 1987. — V. 24. — P. 223–224.

СОБСТВЕННЫЕ ФУНКЦИИ С МИНИМАЛЬНЫМ НОСИТЕЛЕМ ДИСТАНЦИОННО-РЕГУЛЯРНЫХ ГРАФОВ СТЕПЕНИ $k = 3$

Е. В. Сотникова (Новосибирск)

Введение

Пусть $V = \{v_1, \ldots, v_n\}$ — непустое конечное множество из n элементов, называемых *вершинами*, а E — множество неупорядоченных пар вершин v_iv_j, называемых *ребрами*. Тогда упорядоченная пара $G = (V, E)$ называется *неориентированным графом*. Две вершины v_i, v_j являются *смежными* или *соседними*, если они соединены ребром, то есть $v_iv_j \in E$. *Путем* P в графе называется последовательность различных вершин и ребер такая, что для каждой вершины существует ребро, соединяющее ее со следующей вершиной в последовательности, иными словами $P = (v_0, v_0v_1, v_1, v_1v_2, v_2, \ldots, v_{m-1}, v_{m-1}v_m, v_m)$. *Длина* пути определяется как количество ребер в нем. Граф называется *связным*, если между любой парой вершин существует как минимум один путь.

Пусть каждая вершина графа имеет одинаковое число соседей, равное k, тогда граф называется *регулярным*, а число k его *степенью*. Для любых двух

вершин $v, u \in V$ определим *расстояние* $d(u, v)$ между ними как длину кратчайшего пути между этими двумя вершинами. Наибольшее из расстояний между вершинами в связном графе называется *диаметром* графа D. Множество вершин, находящихся на расстоянии i от v будем обозначать за $G_i(v)$. Связный граф G называется *дистанционно-регулярным*, если он регулярный степени k и существует такое множество констант $\{b_0, \ldots, b_{D-1}, b_D = 0, c_0 = 0, c_1, \ldots, c_D\}$, что для любых двух вершин $v, u \in V$ на расстоянии $i = d(v, u)$ множество $G_{i-1}(v)$ содержит в точности c_i соседей u, а множество $G_{i+1}(v)$ содержит в точности b_i соседей u. Числа $b_i, c_i, a_i = k - b_i - c_i$, где $i \in \{0, \ldots, D\}$, не зависят от выбора вершин и называются *массивом пересечений* графа G.

Определим матрицу смежности A порядка n графа G следующим образом:

$$A_{ij} = \begin{cases} 1, \text{ если } v_i v_j \in E \\ 0, \text{ если } v_i v_j \notin E \end{cases}$$

Обозначим за $\Lambda = \{\lambda_1, \ldots, \lambda_t\}$ множество всех собственных значений матрицы A. В силу неориентированности графа матрица A является симметричной, поэтому все ее собственные значения вещественные. Поставим каждой вершине v_i в соответствие некоторое вещественное число $f(v_i)$. Вектор $f = (f(v_1), \ldots, f(v_n))$ будем называть функцией на вершинах графа. Если для ненулевой функции f имеет место соотношение $Af = \lambda f$, то такая функция называется *собственной функцией* графа G, соответствующей собственному значению λ. *Носителем* $\mathrm{supp}(f)$ функции является множество всех координантых позиций с ненулевыми значениями, другими словами $\mathrm{supp}(f) = \{i \mid f(v_i) \neq 0\}$.

Данное исследование посвящено дистанционно-регулярным графом степени $k = 3$ и нахождению их собственных функций с минимальными по мощности носителями. Известно [1], что с точностью до изоморфизма таких графов 13: K_4, $K_{3,3}$, граф Петерсена, граф куба, граф Хивуда, граф Паппа, граф Коксетера, граф Татта-Коксетера, граф додекаэдра, граф Дезарга, граф Фостера, 12-клетка Татта, граф Бигса-Смита. Для 10 из них для каждого собственного значения найдены мощности минимальных носителей, а также приведена классификация подграфов, которые могут являться минимальными носителями соответствующих собственных функций.

Основные результаты

Пусть f — собственная функция дистанционно-регулярного графа G, соответствующая некоторому собственному числу λ. Выберем произвольную вершину v с ненулевым значением. Без ограничения общности будем считать, что $f(v) = 1$ (если нет, то произведем нормировку, разделив вектор на $|f(v)|$). Обозначим через $W_i^f(v)$ сумму значений функции в вершинах, находящихся на расстоянии i от v, другими словами $W_i^f(v) = \sum\limits_{u \in G_i(v)} f(u)$. Для дистанционно-

регулярных графов значение $W_i^f(v)$ с точностью до нормировки не зависит от выбора вершины, причем справедливо следующее рекуррентное соотношение:

$$W_0^f = 1,$$

$$W_1^f = \lambda,$$

$$W_i^f = \frac{\lambda W_{i-1}^f - b_{i-2}W_{i-2}^f - a_{i-1}W_{i-1}^f}{c_i}, \text{ где } i = 2, \ldots, D.$$

Множество $\{W_0^f, W_1^f, \ldots, W_D^f\}$ называется *весовым распределением* собственной функции f. Хорошо известен следующий факт:

Лемма 1. *Справедлива следующая оценка на мощность носителя собственной функции*: $|\mathrm{supp}(f)| \geqslant \sum\limits_{i=0}^{D} |W_i^f|$.

Таким образом, вычислив весовое распределение, мы получаем нижнюю оценку на размер минимального носителя. Однако достигаться она будет не всегда. Проиллюстрируем это следующим примером.

Рассмотрим граф Петерсена. Он состоит из 10 вершин и 15 ребер. Множество его собственных значений с указанием кратностей выглядит следующим образом: $\Lambda = \{-2^{(4)}, 1^{(5)}, 3^{(1)}\}$. Вычислим весовое распределение: $W_0 = 1$, $W_1 = \lambda$, $W_2 = \lambda^2 - 3$. Для $\lambda = 1$ и $\lambda = -2$ имеем одинаковое значение границы весового распределения: $\sum\limits_{i=0}^{2} |W_i| = 4$. Таким образом получаем следующую оценку на мощность носителя $|\mathrm{supp}(f)| \geqslant 4$. При $\lambda = 1$ в указанной оценке достигается равенство. Минимальный носитель в таком случае представляет собой подграф, состоящий из двух непересекающихся ребер uv и xy, причем вершины, принадлежащие разным ребрам не смежны друг с другом (см. рис. 1).

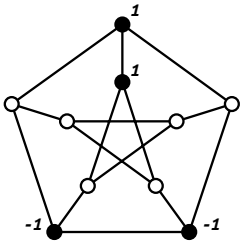

Рис. 1: Граф Петерсена, $\lambda = 1$.

Однако при $\lambda = -2$ вышеуказанная граница уже не достигается. В этом случае мощность минимального носителя равна 6. На рис. 2 представлены

структуры, которые может принимать носитель минимальной мощности, соответствующий $\lambda = -2$.

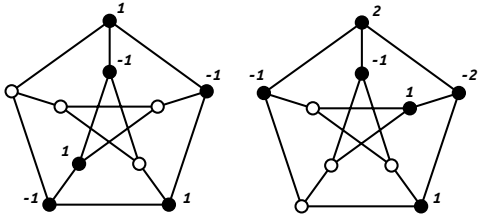

Рис. 2: Граф Петерсена, $\lambda = -2$.

В таблице ниже представлены мощности минимальных носителей, соответствующих различным собственным значениям. Стоит отметить, что поскольку рассматриваемые графы являются регулярными степени 3, то число $k = 3$ будет максимальным собственным значением с собственным вектором, состоящим из одних единиц (с точностью до нормировки). Таким образом размер минимального носителя для $\lambda = 3$ (а в случаях двудольных графов и для $\lambda = -3$) всегда будет равен порядку графа n.

Граф	**Собственные значения**	**Минимальный носитель**
K_4	$\{-1^{(3)}, 3^{(1)}\}$	$\{2, 4\}$
$K_{3,3}$	$\{0^{(4)}, \pm 3^{(1)}\}$	$\{2, 6\}$
Cube	$\{\pm 1^{(3)}, \pm 3^{(1)}\}$	$\{4, 8\}$
Petersen	$\{-2^{(4)}, 1^{(5)}, 3^{(1)}\}$	$\{6, 4, 10\}$
Heawood	$\{\pm\sqrt{2}^{(6)}, \pm 3^{(1)}\}$	$\{6, 14\}$
Pappus	$\{0^{(4)}, \pm\sqrt{3}^{(6)}, \pm 3^{(1)}\}$	$\{6, 8, 18\}$
Dodecahedral	$\{-2^{(4)}, 0^{(4)}, 1^{(5)}, \pm\sqrt{5}^{(3)}, 3^{(1)}\}$	$\{12, 8, 8, 16, 20\}$
Desargues	$\{\pm 1^{(5)}, \pm 2^{(4)}, \pm 3^{(1)}\}$	$\{8, 12, 20\}$
Coxeter	$\{(-1 \pm \sqrt{2})^{(6)}, -1^{(7)}, 2^{(8)}, 3^{(1)}\}$	$\{16, 12, 14, 28\}$
Tutte-Coxeter	$\{0^{(10)}, \pm 2^{(9)}, \pm 3^{(1)}\}$	$\{6, 14, 30\}$

Исследование выполнено за счет гранта Российского научного фонда (проект №14-11-00555)

Список литературы

1. Biggs N. L., Boshier A. G., Shawe-Taylor J. Cubic distance-regular graphs // J. London Math. Soc. — 1986. — 33(2). — Pp. 385–394.

КЛАССЫ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ, ЗАМКНУТЫЕ ОТНОСИТЕЛЬНО ОПЕРАЦИЙ СУПЕРПОЗИЦИИ И ОБРАЩЕНИЯ

Д. Е. Стародубцев (Москва)

Введение

Работа относится к теории функциональных систем. Исследуются замкнутые классы функций k-значной логики [3, 5]. Известно, что семейство замкнутых классов булевых функций имеет счетную мощность [6, 7], а семейство замкнутых классов функций k-значной логики при $k \geqslant 3$ имеет мощность континуума [3, 4]. В ряде работ (см., например, обзор [2]) рассматриваются различные усиления операции суперпозиции, что позволяет получить более «просто» устроенную решетку классов функций, замкнутых относительно новых операций. Данная работа также относится к этому направлению исследований. На множестве функций k-значной логики наряду с операцией суперпозиции вводится операция обращения, которая в некотором смысле является обратной к операции отождествления переменных. Получено описание всех классов функций, замкнутых относительно операций суперпозиции и обращения. Для классов булевых функций аналогичная задача была решена в 2011 г. в работе [1].

Описание замкнутых классов

Пусть $k \geqslant 3$. Обозначим через E_k множество $\{0, 1, \ldots, k-1\}$, через P_k — множество всех функций k-значной логики. На множестве функций k-значной логики определим операцию *обращения* следующим образом. Для $n \geqslant 2$ обозначим через A_n множество наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_k^n$, таких, что $\alpha_n = \alpha_i$ для некоторого $i \in \{1, \ldots, n-1\}$. Рассмотрим функцию $f(x_1, \ldots, x_n) \in P_k$. Будем говорить, что функция $g(x_1, \ldots, x_{n+1})$ получена из функции f с помощью операции обращения, если для всех наборов $(\alpha_1, \ldots, \alpha_{n+1})$ из множества A_{n+1} выполняется $g(\alpha_1, \ldots, \alpha_{n+1}) = f(\alpha_1, \ldots, \alpha_n)$. Заметим, что если функция $g(x_1, \ldots, x_{n+1})$ получена из функции $f(x_1, \ldots, x_n)$ при помощи операции обращения, то f можно получить из g путем отождествления переменной x_{n+1} с любой из переменных $x_1, \ldots, x_n$. Через $\Delta(f)$ будем обозначать множество всех функций g, которые получаются из f операцией обращения. Через $[F]$ будем обозначать замыкание множества функций F относительно операции суперпозиции; через $[F]_\Delta$ — замыкание F относительно операций суперпозиции и обращения. Через T_i будем обозначать множество всех функций из P_k, сохраняющих константу i; через A_ρ — множество всех функций из P_k, сохраняющих отношение ρ на множестве E_k. Пусть F — множество функций

из P_k, тогда через $F(n)$ будем обозначать множество всех функций из F, зависящих от n переменных.

Утверждение 1. *Пусть $s(x) \in P_k$. Пусть $I \subseteq E_k$ — такое множество значений, что $s(x) \in T_i$ для всех $i \in I$ и $s(x) \notin T_j$ для всех $j \in E_k \setminus I$. Тогда для любой одноместной функции*[1] *$f(x) \in \bigcap\limits_{i \in I} T_i$ выполняется $f(x) \in [\{s(x)\}]_\Delta$.*

Доказательство. Рассмотрим функцию $g(x, y)$, определенную следующим образом:

$$g(x,y) = \begin{cases} s(x), & \text{если } x = y; \\ f(x), & \text{если } x \neq y \text{ и } s(x) = y; \\ 0, & \text{иначе.} \end{cases}$$

Заметим, что $g(x, y) \in \Delta\big(s(x)\big)$, так как на наборах вида (a, a) функция принимает значение $s(a)$ и тем самым удовлетворяет определению операции Δ. Покажем, что $f(x) = g\big(x, g(x, x)\big)$. По определению функции g для любых $a \in E_k$ имеем $g\big(a, g(a, a)\big) = g\big(a, s(a)\big)$. Теперь если $a = s(a)$, то $g\big(a, s(a)\big) = s(a) = a = f(a)$; если $a \neq s(a)$, то применение функции s к первому аргументу дает в точности второй аргумент, поэтому получаем $g\big(a, s(a)\big) = f(a)$. Таким образом $f(x) \in [\{s(x)\}]_\Delta$. Утверждение доказано.

Утверждение 2. *Пусть $s(x) \in P_k$. Пусть $I \subseteq E_k$ — такое множество значений, что $s(x) \in T_i$ для всех $i \in I$ и $s(x) \notin T_j$ для всех $j \in E_k \setminus I$. Тогда для любой двухместной функции $f(x, y) \in \bigcap\limits_{i \in I} T_i$ выполняется $f(x, y) \in [\{s(x)\}]_\Delta$.*

Доказательство. Рассмотрим функцию $g(x) = f(x, x)$. Для всех $i \in I$ верны соотношения $g(x) \in T_i$. По утверждению 1 имеем $g(x) \in [\{s(x)\}]_\Delta$. По определению операции обращения получаем, что $f(x, y) \in \Delta\big(g(x)\big)$, поэтому $f(x, y) \in [\{s(x)\}]_\Delta$. Утверждение доказано.

Теорема 1. *Пусть $s(x) \in P_k$. Пусть $I \subseteq E_k$ — такое множество значений, что $s(x) \in T_i$ для всех $i \in I$ и $s(x) \notin T_j$ для всех $j \in E_k \setminus I$. Тогда $[\{s(x)\}]_\Delta = \bigcap\limits_{i \in I} T_i$.*

Доказательство. Известно, что если отношение ρ унарное, то множество A_ρ порождается функциями из A_ρ, зависящими не более чем от двух переменных (см., например, [2]). По утверждению 2 имеем $(\bigcap\limits_{i \in I} T_i)(2) \subset [\{s(x)\}]_\Delta$. Следовательно, $[\{s(x)\}]_\Delta = \bigcap\limits_{i \in I} T_i$. Теорема доказана.

Следствие. *Пусть ρ — унарное отношение на E_k. Тогда $A_\rho = [A_\rho(1)]_\Delta$.*

[1] Здесь и далее будем считать, что при $I = \varnothing$ множество $\bigcap\limits_{i \in I} T_i$ совпадает с P_k.

Доказательство. Известно, что $A_\rho = [A_\rho(2)]$. По утверждению 2 любая двухместная функция из A_ρ принадлежит замыканию функции $s(x)$, поэтому из порождающей системы для A_ρ, содержащей все функции $f(x_1, \ldots, x_n) \in A_\rho$, для которых $n \leqslant 2$, все двухместные функции можно удалить. Утверждение доказано.

Теорема 2. *Пусть $A \subseteq P_k$. Пусть множество $I \subseteq E_k$ выбрано так, что для любого $i \in I$ всякая функция $f \in A$ принадлежит T_i, а для любого $j \in E_k \setminus I$ существует функция $f \in A$, не принадлежащая T_j. Тогда $[A]_\Delta = \bigcap\limits_{i \in I} T_i$.*

Доказательство. Соотношение $[A]_\Delta \subseteq \bigcap\limits_{i \in I} T_i$ следует из того, что по условию теоремы любая функция из A принадлежит $\bigcap\limits_{i \in I} T_i$, и для любого $i \in E_k$ множество T_i является замкнутым относительно операций суперпозиции и обращения классом. Докажем обратное включение. Если $I = E_k$, то любая функция из A сохраняет все константы и, следовательно, для любой функции f из A по теореме 1 выполняется соотношение $T_0 \cap T_1 \cap \cdots \cap T_{k-1} = [\{f\}]_\Delta \subseteq [A]_\Delta$.

Пусть теперь $I \neq E_k$. Для каждого $j \in E_k \setminus I$ рассмотрим функцию $f_j \in A \setminus T_j$. Для каждой функции f_j положим $g_j(x) = f_j(x, \ldots, x)$. Пусть $I = \{i_1, \ldots, i_m\}$, $E_k \setminus I = \{j_1, \ldots, j_n\}$. Будем считать, что элементы $i_1, \ldots, i_m$ упорядочены между собой естественным образом; то же предположение сделаем относительно элементов $j_1, \ldots, j_m$. Упорядочим элементы из E_k следующим образом: $i_1 < \cdots < i_m < j_1 < \cdots < j_n$. Обозначим через $\min^\circ(x, y)$ функцию, равную меньшему из значений аргументов относительно этого упорядочения. Заметим, что $\min, \min^\circ \in \Delta\big(e(x)\big)$, так как $\min(a, a) = \min^\circ(a, a) = a$ для любого $a \in E_k$. По утверждению 1 для любой одноместной функции $s(x)$ имеем $e(x) \in [\{s(x)\}]_\Delta$, поэтому $\min, \min^\circ \in [\{g_j\}]_\Delta$ для любого $j \in E_k \setminus I$ и, следовательно, $\min^\circ \in [A]_\Delta$.

Для каждой функции $g_j(x)$ введем следующие две функции:

$$h_j(x) = \begin{cases} x, & \text{если } g_j(x) = x; \\ 0, & \text{иначе;} \end{cases}$$

$$h_j^\circ(x) = \begin{cases} x, & \text{если } g_j(x) = x; \\ i_1, & \text{иначе.} \end{cases}$$

По утверждению 1 выполнены соотношения $h_j, h_j^\circ \in \Delta(g_j)$ и, следовательно, $h_j, h_j^\circ \in [A]_\Delta$.

Пусть $I \neq \varnothing$. Положим $r^\circ(x) = \min\limits^\circ\limits_{j \in E_k \setminus I} h_j^\circ(x)$. Для всех $i \in I$ имеем $g_i \in T_i$, $h_i^\circ \in T_i$, то есть $h_i^\circ(i) = i$. Значит, $r^\circ(x) \in \bigcap\limits_{i \in I} T_i$. Заметим, что $g_{j_1}(j_1) \neq j_1$, поэтому $h_{j_1}^\circ(j_1) = i_1$. Так как i_1 является минимальным значением относительно

соответствующего упорядочения элементов из E_k, то $r^\circ(j_1) = i_1$. Рассуждая аналогичным образом для $j_2, \ldots, j_n$, получаем, что $r^\circ(j_2) = \cdots = r^\circ(j_n) = i_1$. Так как $i_1 \notin \{j_1, \ldots, j_n\}$, то $r^\circ(x) \notin T_j$ для всех $j \in E_k \setminus I$. Применяя теперь теорему 1 к функции $r^\circ(x)$, получаем, что $\bigcap\limits_{i\in I} T_i = [\{r^\circ(x)\}]_\Delta \subseteq [A]_\Delta$.

Рассмотрим случай $I = \varnothing$. Положим теперь $r(x) = \min\limits_{j\in E_k} h_j(x)$. Заметим, что для всех $j \in E_k$ выполняется $g(j) \neq j$, поэтому $h_j(j) = 0$ и $r(j) = 0$. Получаем, что $r(x) \in T_0$ и $r(x) \notin T_j$ для всех $j \in E_k \setminus \{0\}$. По теореме 1 имеем $[\{r(x)\}]_\Delta = T_0$. Рассмотрим теперь класс $[\{r(x), g_0(x)\}]_\Delta$. Так как $[\{r(x)\}]_\Delta = T_0$, то $T_0 \subset [\{r(x), g_0(x)\}]_\Delta$. Так как $g_0(x) \notin T_0$, то $[\{r(x), g_0(x)\}]_\Delta \not\subset T_0$. Так как T_0 является предполным классом для замыкания относительно суперпозиции, то он является таковым и для рассматриваемого замыкания. Отсюда следует, что $P_k = [\{r(x), g_0(x)\}]_\Delta \subseteq [A]_\Delta$.

Тем самым доказано обратное включение для искомого равенства. Теорема доказана.

Теорема 3. *Семейство классов в P_k, замкнутых относительно операций суперпозиции и обращения исчерпывается следующим списком*: P_k, $\bigcap\limits_{i\in I} T_i$ *для всевозможных* $I \subseteq E_k$.

Доказательство. Рассмотрим произвольный замкнутый относительно операций суперпозиции и обращения замкнутый класс A. Возьмем произвольную функцию $f \in A$. Положим $f'(x) = f(x, \ldots, x)$. По утверждению 1 имеем $e(x) \in \Delta\big(f'(x)\big)$, по теореме 2 получаем, что $T_0 \cap \cdots \cap T_{k-1} \subseteq A$. Таким образом, $T_0 \cap \cdots \cap T_{k-1}$ — наименьший непустой замкнутый класс.

Докажем теперь, что замкнутые классы, содержащие $T_0 \cap \cdots \cap T_{k-1}$, есть $\bigcap\limits_{i\in I} T_i$ для некоторого $I \subset E_k$ или P_k. Рассмотрим произвольный замкнутый класс B, содержащий $T_0 \cap \cdots \cap T_{k-1}$. Предположим, что B не совпадает ни с одним из перечисленных классов. Тогда легко видеть, что найдется такое множество $J \subseteq E_k$, что $\bigcap\limits_{i\in J} T_i \subset B$, но для всех $J' \subset E_k$, таких, что $|J'| = |J|-1$, имеем $\bigcap\limits_{i\in J'} T_i \not\subset B$.

Рассмотрим произвольную функцию $g \in B \setminus \bigcap\limits_{i\in J} T_i$. Обозначим функцию $g(x, \ldots, x)$ через $g'(x)$. Пусть $I \subseteq E_k$ — такое множество, что $g'(a) = a$ при $a \in I$ и $g'(a) \neq a$ при $a \notin I$. Рассмотрим также произвольную функцию f' из $\bigcap\limits_{i\in J} T_i \setminus \bigcup_{i\in E_k\setminus J} T_i$. Разобьем E_k на четыре непересекающихся множества: положим $I_1 = I \cap J$; $I_2 = J \setminus I$; $I_3 = I \setminus J$; $I_4 = E_k \setminus (I \cup J)$. Так как $g' \notin \bigcap\limits_{i\in J} T_i$, имеем $I_2 \neq \varnothing$. Для $i \in I_1$ имеем $f' \in T_i$ и $g' \in T_i$; для $i \in I_2$ имеем $f' \in T_i$ и $g' \notin T_i$; для $i \in I_3$ имеем $f' \notin T_i$ и $g' \in T_i$; для $i \in I_4$ имеем $f' \notin T_i$ и $g' \notin T_i$. Применив теперь теорему 2 к множеству функций $\{f', g'\}$, получаем

$\bigcap\limits_{i\in I_1} T_i = [\{f', g'\}] \subseteq B$ (если I_1 пусто, снова считаем $\bigcap\limits_{i\in I_1} T_i = P_k$). Возьмем теперь произвольный элемент a из I_2, положим $J' = J \setminus \{a\}$. Тогда получим, что $\bigcap\limits_{i\in J'} T_i \subseteq \bigcap\limits_{i\in I_1} T_i \subset B$, что противоречит выбору множества J.

Таким образом, предположение неверно, любой замкнутый класс, содержащий $T_0 \cap \cdots \cap T_{k-1}$, есть $\bigcap\limits_{i\in I} T_i$ для некоторого $I \subset E_k$ или класс P_k. Теорема доказана.

Работа выполнена при поддержке РФФИ, проект № 14-01-00598 («Вопросы синтеза, сложности и контроля управляющих систем») и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Мартынова Н. Т. Вопросы полноты для некоторых функциональных систем булевых функций. — Дипломная работа. МГУ им. М. В. Ломоносова. — Москва, 2011.
2. Угольников А. Б. О некоторых задачах в области многозначных логик // Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, МГУ, 1–6 февраля, 2010 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 18–34.
3. Яблонский С. В. Введение в дискретную математику. — М.: Высш. шк., 2001.
4. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Докл. АН СССР. — 1959. — Т. 127, №1. — С. 44–46.
5. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Berlin: Springer, 2006.
6. Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, №3. — P. 163–185.
7. Post E. L. The two-valued iterative systems of mathematical logic // Annals of Math. Studies. Princeton Univ. Press. — 1941. — V. 5.

ОЦЕНКИ НА ЧИСЛО БУЛЕВЫХ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ ИНИЦИАЛЬНЫМ БУЛЕВЫМ АВТОМАТОМ С ТРЕМЯ КОНСТАНТНЫМИ СОСТОЯНИЯМИ

Л. Н. Сысоева (Москва)

Введение

В данной работе рассматривается задача о порождении булевых функций инициальными булевыми автоматами с тремя константными состояниями и n входами, то есть такими автоматами с тремя состояниями, что в любом из них функция выхода совпадает с одной из булевых функций $0(x_1, x_2, \ldots, x_n)$ или $1(x_1, x_2, \ldots, x_n)$, $n \geqslant 1$. Ранее в [1] автором рассматривалась аналогичная задача для инициального булевого автомата с двумя константными состояниями и n входами, $n \geqslant 1$. Было получено точное значение $(\frac{5}{8} \cdot 2^{2^n})$ максимальной мощности множества булевых функций от n фиксированных переменных, которые могут быть реализованы одним инициальным булевым автоматом с двумя константыми состояниями. В данной работе, построен пример инициального булевого автомата с тремя константными состояниями реализующего $2^{2^n} - 2^{2^{n-1}} - 1$ различных булевых функций от n фиксированных переменных. Таким образом, в отличие от случая инициальных автоматов с двумя состояниями, среди инициальных булевых автоматов с тремя константными состояниями существуют автоматы, доля функций $f(x_1, x_2, \ldots, x_n)$, реализуемых которыми, стремится к 1 с ростом n. Также получена верхняя оценка числа булевых функций от n фиксированных переменных, реализуемых инициальным булевым автоматом с тремя константными состояниями.

1. Определения и обозначения

Введем необходимые определения. Через $P_2(n)$ обозначается множество всех булевых функций, зависящих только от переменных $x_1, x_2, \ldots, x_n$, $n \geqslant 1$. Под *булевым автоматом* будем понимать автомат $V = (A, B, Q, F, G)$ с произвольным числом входов, входным алфавитом $A = \{0, 1\}$, выходным алфавитом $B = \{0, 1\}$, алфавитом состояний Q, функцией перехода G и функцией выхода F. Определения автомата и инициального автомата можно найти в [2, 3]. Пусть n — число входов автомата V. Без ограничения общности будем полагать, что входы автомата V занумерованы от 1 до n, и на i-ый вход автомата V подается значение булевой переменной x_i. Тем самым можно считать, что в каждый момент времени на вход автомата V подается некоторый двоичный набор значений переменных $x_1, x_2, \ldots, x_n$, и для любого состояния $q \in Q$ функция выхода $F(q, x_1, x_2, \ldots, x_n)$ является булевой функцией от перемен-

ных $x_1, x_2, \ldots, x_n$. Булев автомат V будем называть *автоматом с константными состояниями*, если для любого $q \in Q$ функция $F(q, x_1, x_2, \ldots, x_n)$ является константной булевой функцией $0(x_1, x_2, \ldots, x_n)$ или $1(x_1, x_2, \ldots, x_n)$. Нетрудно видеть, что такой автомат является частным случаем автомата Мура.

Пусть $V_{q_1} = (\{0,1\}, \{0,1\}, Q, F, G, q_1)$ — инициальный булев автомат с начальным состоянием q_1 и n входами, входным алфавитом $A = \{0,1\}$, выходным алфавитом $B = \{0,1\}$, алфавитом состояний Q, функцией перехода G и функцией выхода F. Пусть $C = (\widetilde{\beta}_1, \widetilde{\beta}_2, \ldots, \widetilde{\beta}_{2^n})$ — упорядоченная последовательность всех двоичных наборов длины n, $n \geqslant 1$. Будем говорить, что *автомат V_{q_1} с последовательностью C реализует булеву функцию f*, если при последовательной подаче на вход V_{q_1} наборов из C в первые 2^n моментов времени, в каждый момент $t = 1, 2, \ldots, 2^n$ на выходе V_{q_1} выдается значение $f(\widetilde{\beta}_t)$. Будем также говорить, что V_{q_1} *реализует функцию f*, если для некоторой последовательности наборов C автомат V_{q_1} с последовательностью C реализует f. Обозначим через $P(V_{q_1})$ множество всех булевых функций из $P_2(n)$, реализуемых автоматом V_{q_1}.

Под 0-состоянием инициального булевого автомата V будем понимать состояние с функцией выхода $0(x_1, x_2, \ldots, x_n)$, а под 1-состоянием — состояние с функцией выхода $1(x_1, x_2, \ldots, x_n)$. Без ограничения общности мы будем рассматривать инициальные булевы автоматы, содержащие хотя бы одно 0-состояние и хотя бы одно 1-состояние, при этом начальным состоянием является 0-состояние. Рассматриваемые автоматы очевидным образом разбиваются на два подмножества: множество всех инициальных булевых автоматов с тремя константными состояниями и n входами, содержащих ровно одно 1-состояние, обозначаемое через $\mathfrak{V}_3^0(n)$, $n \geqslant 1$, и множество всех инициальных булевых автоматов с тремя константными состояниями и n входами, содержащих ровно одно 0-состояние, являющееся начальным, обозначаемое через $\mathfrak{V}_3^1(n)$, $n \geqslant 1$. Автоматы из множеств $\mathfrak{V}_3^0(n)$ и $\mathfrak{V}_3^1(n)$ можно схематично изобразить с помощью диаграмм, изображенных на рис. 1 и рис. 2, где A, B, K, M, T, $E \subseteq \{0,1\}^n$. В кружочках написаны символы, соответствующие функции выхода в этом состоянии, а на стрелках — множества всех наборов, при подаче которых на вход автомата автомат из состояния, из которого идет стрелка, переходит в состояние, на которое указывает стрелка. Звездочкой помечено начальное состояние автомата.

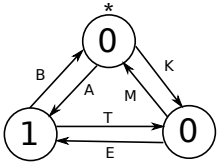

Рис. 1.

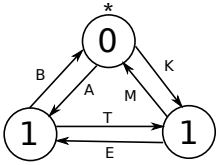

Рис. 2.

2. Нижняя оценка для числа функций, реализуемых инициальными автоматами

Утверждение 1. *Для любого $n \geqslant 1$ существует инициальный булев автомат V с тремя константными состояниями, такой, что $|P(V)| = 2^{2^n} - 2^{2^{n-1}} - 1$.*

Доказательство. Рассмотрим инициальный автомат V из $\mathfrak{V}_3^0(n)$, определяемый множествами $A = B = M = T = \varnothing$, K и E, такими, что $K \cap E = \{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, где $\widetilde{\varkappa}_1, \widetilde{\varkappa}_2$ — некоторые двоичные наборы длины n, $|K| = |E| = 2^{n-1} + 1$ и $K \cup E = \{0,1\}^n$. Такой автомат V не может реализовать функцию f из $P_2(n)$, если функция f принимает значение 1 на всех наборах множества K или принимает значение 1 на всех наборах множества E, а также если она принимает значение 1 на всех булевых наборах длины n, кроме одного набора $\widetilde{\varkappa}_i$, где $i \in \{0,1\}$. Докажем, что все другие функции из $P_2(n)$ реализуются данным автоматом.

Пусть дана функция $f \in P_2(n)$, такая, что $f(\widetilde{\varkappa}_1) = f(\widetilde{\varkappa}_2) = 0$. Определим последовательность подаваемых наборов следующим образом: сначала подаем все наборы из множества $E\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, на которых функция f принимает значение 0, затем набор $\widetilde{\varkappa}_1$, потом все наборы из множества $K\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, на которых функция f принимает значение 0, далее набор $\widetilde{\varkappa}_2$ и наконец все наборы, на которых функция f принимает значение 1. Автомат V с такой последовательностью подаваемых наборов будет реализовать функцию f.

Пусть дана функция $f \in P_2(n)$, такая, что $f(\widetilde{\varkappa}_i) = 0$ и $f(\widetilde{\varkappa}_j) = 1$, где $i, j \in \{1,2\}, i \neq j$. В этом случае существует набор $\widetilde{\varkappa} \in K\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, такой, что $f(\widetilde{\varkappa}) = 0$ или набор $\widetilde{\varepsilon} \in E\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, такой, что $f(\widetilde{\varepsilon}) = 0$. Без ограничения общности будем считать, что существует набор $\widetilde{\varkappa} \in K\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, такой, что $f(\widetilde{\varkappa}) = 0$. Определим последовательность подаваемых наборов следующим образом: сначала подаем все наборы из множества $E\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, на которых функция f принимает значение 0, затем набор $\widetilde{\varkappa}$, потом все наборы из множества $K\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2, \widetilde{\varkappa}\}$, на которых функция f принимает значение 0, далее набор $\widetilde{\varkappa}_i$ и наконец все наборы, на которых функция f принимает значение 1. Автомат V с такой последовательностью подаваемых наборов будет реализовать функцию f.

Пусть дана функция $f \in P_2(n)$, такая, что $f(\widetilde{\varkappa}_1) = f(\widetilde{\varkappa}_2) = 1$. В этом случае существует набор $\widetilde{\varkappa} \in K\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, такой, что $f(\widetilde{\varkappa}) = 0$ и набор $\widetilde{\varepsilon} \in E\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2\}$, такой, что $f(\widetilde{\varepsilon}) = 0$. Определим последовательность подаваемых наборов следующим образом: сначала подаем все наборы из множества $E\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2, \widetilde{\varepsilon}\}$, на которых функция f принимает значение 0, затем набор $\widetilde{\varkappa}$, потом все наборы из множества $K\backslash\{\widetilde{\varkappa}_1, \widetilde{\varkappa}_2, \widetilde{\varkappa}\}$, на которых функция f принимает значение 0, далее набор $\widetilde{\varepsilon}$ и наконец все наборы, на которых функция f принимает значение 1. Автомат V с такой последовательностью подаваемых наборов будет реализовать функцию f.

Оценим количество функций, которые не могут быть реализованы автоматом V:

$$2^{2^n} \cdot \left(\frac{1}{2^{|K|}} + \frac{1}{2^{|E|}} - \frac{1}{2^{|K \cup E|}}\right) + 2 = 2^{2^n} \cdot \left(\frac{1}{2^{2^{n-1}+1}} + \frac{1}{2^{2^{n-1}+1}} - \frac{1}{2^{2^n}}\right) + 2 =$$

$$= \frac{1}{2} \cdot 2^{2^{n-1}} + \frac{1}{2} \cdot 2^{2^{n-1}} + 1 = 2^{2^{n-1}} + 1.$$

Значит, автомат V может реализовать $2^{2^n} - 2^{2^{n-1}} - 1$ различных булевых функций от n переменных.

3. Верхняя оценка для числа функций, реализуемых инициальными автоматами

Верна следующая теорема.

Теорема 1. *Для любого $n \geqslant 5$ и любого инициального булевого автомата V с тремя константными состояниями $|P(V)| \leqslant 2^{2^n} - \frac{3}{4} \cdot 2^{n-3}$.*

Ее доказательство разбивается на два случая. Сформулируем их в виде независимых утверждений.

Теорема 2. *Для любого $n \geqslant 5$ и любого автомата V из множества $\mathfrak{V}_3^0(n)$ верно $|P(V)| \leqslant 2^{2^n} - 2^{n-2} - 1$.*

Теорема 3. *Для любого $n \geqslant 1$ и любого автомата V из множества $\mathfrak{V}_3^1(n)$ верно $|P(V)| \leqslant 2^{2^n} - \frac{3}{4} \cdot 2^{n-3}$.*

Доказательства этих теорем состоят из рассмотрения большого количества различных случаев и, в силу громоздкости, не приведены в данной работе. Сформулируем некоторые свойства автоматов из множеств $\mathfrak{V}_3^0(n)$ и $\mathfrak{V}_3^1(n)$, используемые при доказательстве этих теорем.

В отличие от случая для инициального булева автомата с двумя константными состояниями, для автомата с тремя константными состояниями максимальная мощность множества реализуемых автоматом функций не может достигаться для любого n при фиксированной мощности множеств A, B, K, M, T, E. В частности, верны следующие два утверждения, доказательства которых аналогичны, поэтому приведем лишь одно из них.

Утверждение 2. *Для любого $n \geqslant 1$ и автомата V из множества $\mathfrak{V}_3^0(n)$ верно $|P(V)| \leqslant \min\left(2^{2^n} - 2^{2^n - |A \cup K|} + 1, 2^{2^n} - 2^{2^n - |A \cup E|} + 1\right)$.*

Доказательство. Автомат V не может реализовать функцию $f \in P_2(n)$, которая принимает значение 1 на всех наборах множества $A \cup K$ или принимает значение 1 на всех наборах множества $A \cup E$. В случае, когда хотя бы одно из множеств $A \cup E$, $A \cup K$ является пустым, в силу того, что автомат V в этом случае может реализовать только константу 0, верно равенство

$$\min\left(2^{2^n} - 2^{2^n - |A \cup K|} + 1, 2^{2^n} - 2^{2^n - |A \cup E|} + 1\right) = 1.$$

Утверждение 3. *Для любого* $n \geqslant 1$ *и автомата* V *из множества* $\mathfrak{V}_3^1(n)$, *верно* $|P(V)| \leqslant \min\left(2^{2^n} - 2^{2^n-|A\cup K|} + 1, 2^{2^n} - 2^{2^n-|B\cup M|-1}\right)$.

При доказательстве приведенных теорем важную роль играют следующие утверждения. Пусть $f(x_1, x_2, \ldots, x_n)$ — некоторая булева функция от n переменных, и D — некоторое подмножество множества всех булевых наборов длины n. Обозначим через D_f^0 подмножество множества D, состоящее из всех таких наборов $\widetilde{\beta}$, для которых выполнено равенство $f(\widetilde{\beta}) = 0$, а через D_f^1 — подмножество множества D, состоящее из всех таких наборов $\widetilde{\beta}$, для которых выполнено равенство $f(\widetilde{\beta}) = 1$.

Утверждение 4. *Для любого* $n \geqslant 1$, *любого автомата* V *из множества* $\mathfrak{V}_3^0(n)$ *и любой реализуемой им булевой функции* $f(x_1, x_2, \ldots, x_n)$ *выполнено* $|(A \cap E)_f^0| - 1 \leqslant |(B \cup T)_f^1| \leqslant |(A \cup E)_f^0|$.

Утверждение 5. *Для любого* $n \geqslant 1$, *любого автомата* V *из множества* $\mathfrak{V}_3^1(n)$ *и любой реализуемой им булевой функции* $f(x_1, x_2, \ldots, x_n)$ *выполнено* $|(A \cup K)_f^0| - 1 \leqslant |(B \cup M)_f^1|$.

Работа выполнена при поддержке РФФИ, проект № 14-01-00598 («Вопросы синтеза, сложности и контроля управляющих систем») и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

В заключение автор выражает искреннюю признательность Р. М. Колпакову и О. С. Дудаковой за постановку задачи и обсуждение результатов работы.

Список литературы

1. Сысоева Л. Н. Максимальное число булевых функций, порождаемых инициальным автоматом с двумя константными состояниями // IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г.: Труды / Отв. ред. В.Б. Алексеев, Д.С. Романов, Б.Р. Данилов. — М.: МАКС Пресс, 2015. — С. 239–241.
2. Яблонский С. В. Введение в дискретную математику. — М. : Высшая школа, 2006. — 384 с.
3. Конспект лекций О. Б. Лупанова по курсу “Введение в математическую логику” / Отв. ред. А. Б. Угольников. — М. : Изд-во ЦПИ при механико-математическом факультете МГУ имени М. В. Ломоносова, 2007. — 191 с.

ОБ ОДНОЙ РЕКУРСИВНОЙ КОНСТРУКЦИИ ПЛАТОВИДНЫХ БУЛЕВЫХ ФУНКЦИЙ С ПЕРЕСЕКАЮЩИМИСЯ НОСИТЕЛЯМИ СПЕКТРА

Е. В. Хинко (Москва)

Введение

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и поднимается в работах многих российских и зарубежных авторов. Например, в работах [3] и [5] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работах [4] и [6] построены соответствующие конструкции функций.

В работе [1] Ю. В. Таранниковым построены рекурсивные конструкции устойчивых функций с высокой нелинейностью, имеющие пары квазилинейных покрывающих переменных.

В данной работе представлена обеспечивающая рост устойчивости рекурсивная конструкция платовидных булевых функций с шагом числа переменных 3 и приведены примеры начальных функций. К похожей теме уже обращался К. В. Захаров, исследовавший в работе [2] рекурсивные конструкции бент-функций (которые можно считать подмножеством платовидных) с шагом 2 переменных.

Принципиальное отличие представленной конструкции от многих построенных ранее в том, что рассматривается случай порождающих функций с пересекающимися спектрами.

1. Основные определения и факты

Рассмотрим булеву функцию f от n переменных.

Определение 1. Коэффициентом Уолша называется следующее выражение:

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x)+<x,u>},$$

где $< x, u >$ — стандартное скалярное произведение наборов.

Определение 2. Булева функция $f : V_n \to F_n^2$ называется платовидной, если $W_f(u) \in \{0, \pm 2^c\}$ $\forall u \in V_n$.

Определение 3. Булева функция $f : V_n \to F_n^2$ называется корреляционно-иммунной порядка m, если $W_f(u) = 0$ $\forall u : 1 \leqslant wt(u) \leqslant m$. Далее будем обозначать это $f \in CI(m)$.

Определение 4. Булева функция $f : V_n \to F_n^2$ называется m-устойчивой, если $f \in CI(m)$ и является уравновешенной.

Утверждение (равенство Парсеваля). *Имеет место равенство:*

$$\sum_{u \in V_n} W_f^2(u) = 4^n.$$

2. Постановка задачи

Пусть имеются восемь платовидных булевых функций от n переменных $f_n^{a_{ij}}(x_1, x_2, \ldots, x_n), a_{ij} \in \{1, 2, 3, 4, 5, 6, 7, 8\}$, среди которых возможно есть совпадающие с точностью до взятия отрицания; добавим три переменные x_{n+1}, x_{n+2} и x_{n+3}. Для новых функций от $n+3$ переменных будем использовать обозначения $f_{n+3}^s(x_1, x_2, \ldots, x_n, a_1, a_2, a_3)$, $s = \overline{1,8}$.

Связь между функциями от n и $n+3$ переменных можно записать в виде системы из 8 уравнений. Краткое представление системы:

$$f_{n+3}^s = (\sigma_{s1} g_{s1} \,|\sigma_{s2} g_{s3} \,|\sigma_{s3} g_{s3} \,|\sigma_{s4} g_{s4} \,|\sigma_{s5} g_{s5} \,|\sigma_{s6} g_{s6} \,|\sigma_{s7} g_{s7} \,|\sigma_{s8} g_{s8}), \qquad (1)$$

где $s = \overline{1,8}$,

$$\sigma_{ij} g_{ij} = \begin{cases} f_n^{a_{ij}}, \sigma_{ij} = 1, \\ \overline{f_n^{a_{ij}}}, \sigma_{ij} = -1. \end{cases}$$

Целью проделанной работы являлся подбор таких соотношений σ_{ij} и порождающих функций, чтобы полученные новые функции от $n+3$ переменных:

а) сохраняли платовидность;

б) обеспечивали рост устойчивости функций;

в) конструкция могла воспроизводиться рекурсивно.

Кроме того, строятся порождающие функции, удовлетворяющие найденным соотношениям.

3. Краткий обзор хода работы и полученные результаты

3.1. Идея конструкции. Из равенства Парсеваля следует, что число ненулевых коэффициентов Уолша у каждой из порождающих функций $f_n^{i_j}$, $j \in \overline{1,8}$, равно 4^{n-c}. Из этого легко видеть, что значение максимума модуля коэффициентов Уолша у новых функций от $n+3$ переменных может увеличиться в 4 или 8 раз.

Непосредственно проверяется, что коэффициенты Уолша преобразуются в соответствии со следующей матрицей, т. е. каждый коэффициент функции от $n+3$ переменных это линейная комбинация с коэффициентами ± 1 коэффициентов Уолша функций $f_n^{i_j}$, $j \in \overline{1,8}$:

$$\begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{pmatrix}. \tag{2}$$

Эта матрица называется *матрицей Адамара-Сильвестра* порядка 8.

Идея конструкции заключается в следующем. Рассмотрим 8 порождающих функций от n переменных, среди которых k, $k \leqslant 8$, различных. Мы хотим построить k различных функций от $n+3$ переменных. В нашем случае $k = 4$.

Требуем от порождающих функций m-устойчивость, платовидность (с одинаковым значением модуля ненулевых коэффициентов Уолша) и соблюдение некоторых условий ((К1)–(К3)). Все эти свойства мы хотим сохранить и у новых функций от большего числа переменных, для того чтобы обеспечить рекурсивность конструкции.

Сама конструкция строится с помощью матрицы (2). Посмотрим на матричную запись системы и подставим в каждое уравнение вместо набора знаков сигм строку матрицы (2) или противоположную ей, т. е. если i-й элемент s-й строки матрицы (2) равен $+$, возьмем $\sigma_{si} = +1$, а если $-$, то $\sigma_{si} = -1$ или ровно наоборот: если для всех i i-й элемент s-й строки матрицы (2) равен $+$, возьмем $\sigma_{si} = -1$, а если $-$, то $\sigma_{si} = +1$. Таким образом, с помощью строки матрицы (2) и 8 функций от n переменных зададим функцию от $n+3$ переменных.

3.2. Описание конструкции. Рассмотрим 8 порождающих функций $f_n^{i_j}, j = \overline{1,8}$, среди которых 4 пары совпадающих с точностью до взятия отрицания. Другими словами, рассмотрим 4 функции (обозначим их f_n^1, f_n^2, f_n^3, f_n^4), удовлетворяющие следующим условиям:

(К1) Каждый двоичный набор $\overrightarrow{u} \in V_n$ содержится в спектре в точности нуля, двух или всех четырех функций.

(К2) Мощности всевозможных попарных пересечений спектров порождающих функций $f_n^i, i = \overline{1,4}$, совпадают, а мощность пересечения спектров всех 4 функций $f_n^i, i = \overline{1,4}$, равна четверти мощности спектра каждой функции.

(К3) Для каждого набора $\overrightarrow{u} \in V_n$, содержащегося в спектре всех 4 функций $f_n^i, i = \overline{1,4}$, коэффициенты Уолша трех функций одного знака, а коэффициент Уолша четвертой — другого знака.

В записи системы (1) порождающих функций 8, в конструкции они объединены в 4 пары совпадающих следующим образом:

Функциям $f_n^{i_j}, j = \overline{1,2}$, (см. систему (1)) соответствует f_n^1; $f_n^{i_j}, j = \overline{3,4}$, соответствуют f_n^2; $f_n^{i_j}, j = \overline{5,6}$, соответствуют f_n^3; $f_n^{i_j}, j = \overline{7,8}$, соответствуют f_n^4.

Таким образом, порождающих функций формально 8, но различных среди них лишь 4.

Определение 5. Строки из знаков сигм, определяющие конструкцию, назовем *базовыми* для данной конструкции и будем нумеровать S^1–S^4.

Зададим функции с помощью строк из знаков сигм. Базовые строки S^1 и S^2 двух функций соответствуют строкам 2 и 6 основной матрицы, а базовые строки S^3 и S^4 двух оставшихся функций инвертированным строкам 4 и 8 основной матрицы.

Запишем соответствие функций от $n+3$ переменных и строк из σ_{ij}:
$f^1_{n+3} : S^1 = (+-+-+-+-)$ (строка 2),
$f^2_{n+3} : S^2 = (+-+--+-+)$ (строка 6),
$f^3_{n+3} : S^3 = (-++--+-+)$ (инвертированная строка 4),
$f^4_{n+3} : S^4 = (-++-+--+)$ (инвертированная строка 8).
В явном виде эти функции записываются так (например, f^1_{n+3}):

$$f^1_{n+3}(\overrightarrow{x}, x_{n+1}, x_{n+2}, x_{n+3}) = f^1_n(\overrightarrow{x}) \cdot (x_{n+1} \cdot x_{n+2} + x_{n+1} + x_{n+2} + 1) +$$
$$+ f^2_n(\overrightarrow{x}) \cdot (x_{n+1} \cdot x_{n+2} + x_{n+2}) + f^3_n(\overrightarrow{x}) \cdot (x_{n+1} \cdot x_{n+2} + x_{n+1}) +$$
$$+ f^4_n(\overrightarrow{x}) \cdot x_{n+1} \cdot x_{n+2} + x_{n+3} = (\text{упростим запись}) =$$
$$= A(f^1_n(\overrightarrow{x}), f^2_n(\overrightarrow{x}), f^3_n(\overrightarrow{x}), f^4_n(\overrightarrow{x}), x_{n+1}, x_{n+2}, x_{n+3}) + x_{n+3},$$

где $\overrightarrow{x}$ — это вектор длины n;

Выполнение для функций $f^i_{n+3}, i = \overline{1,4}$, условий (К1)–(К3) было проверено. При проверке выполнения условий (К1) и (К2) использовалась следующая лемма.

Лемма 1. *Для каждого набора* $\overrightarrow{a} \in V_n \setminus W_n : \sum\limits_{i=1}^{4} |W_{f^i_n}(\overrightarrow{a})| \neq 0$ *выполняется* $\#\{W_{f^i_n}(\overrightarrow{a}\, x_{n+1}x_{n+2}x_{n+3}) : W_{f^i_n}(\overrightarrow{a}\, x_{n+1}x_{n+2}x_{n+3}) \neq 0\} \in \{0, 2\}$, *где* W_n — *пересечение носителей спектров всех* 4 *порождающих функций* $f^i_n, i \in \overline{1,4}$.

Выполнение условия (К3) следует из представленной ниже теоремы.

Теорема 1. *Соотношение положительных и отрицательных коэффициентов Уолша новых функций* $f^i_{n+3}, i = \overline{1,4}$, *на наборах от* $n+3$ *переменных с четными номерами, соответствующих* $\overrightarrow{a} \in V_n$, *суть*:

1) *для* f^1_{n+3} *и* f^2_{n+3} *при соотношении коэффициентов Уолша порождающих функций на наборе* $\overrightarrow{a} \in V_n$ *«три положительных — один отрицательный» и для* f^3_{n+3} *и* f^4_{n+3} *при соотношении «один положительный — три отрицательных»*:

если $W_{f^2_n}(\overrightarrow{a})$, $W_{f^3_n}(\overrightarrow{a})$ *или* $W_{f^4_n}(\overrightarrow{a})$ *отрицательный (положительный), то на* $\overrightarrow{a}\, x_{n+1}x_{n+2}1$ *три положительных и один отрицательный коэффицент*

Уолша, а если $W_{f_n^1}(\overrightarrow{a}) < 0$ (*соответственно,* > 0) — *три отрицательных и один положительный*;

2) *для* f_{n+3}^3 *и* f_{n+3}^4 *при соотношении коэффициентов Уолша порождающих функций на наборе* $\overrightarrow{a} \in V_n$ *«три положительных — один отрицательный» и для* f_{n+3}^1 *и* f_{n+3}^2 *при соотношении «один положительный — три отрицательных»*:

если $W_{f_n^2}(\overrightarrow{a})$, $W_{f_n^3}(\overrightarrow{a})$ *или* $W_{f_n^4}(\overrightarrow{a})$ *отрицательный (положительный), то на* $\overrightarrow{a}x_{n+1}x_{n+2}1$ *три отрицательных и один положительный коэффициент Уолша, а если* $W_{f_n^1}(\overrightarrow{a}) < 0$ (*соответственно,* > 0) — *три положительных и один отрицательный.*

Теорема 2 (итоговая). *Заданная в разделе* 3.2 *с помощью базовых строк* S^1–S^4 *конструкция с шагом числа переменных 3 платовидных m-устойчивых булевых функций при выполнении начальных условий* (К1)–(К3):

1) *рекурсивна, т. е. сохраняет начальные условия, что позволяет применять ее многократно*;

2) *обеспечивает рост устойчивости функций на 1.*

Пример. Зададим 4 функции $f_n^i, i = \overline{1,4}$, от $n = 3$ переменных их спектрами:

0 4 4 0 4 0 0 -4 ($f_{n=3}^1 = x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3$);

0 4 0 -4 4 0 4 0 ($f_{n=3}^2 = x_1 \cdot x_3 + x_2 \cdot x_3 + x_1$);

0 4 4 0 0 -4 4 0 ($f_{n=3}^3 = x_1 \cdot x_2 + x_1 \cdot x_3 + x_2$);

0 -4 0 4 0 4 0 4 ($f_{n=3}^4 = x_1 \cdot x_2 + x_1 + x_2 + x_3$).

Заметим, что для любого $\overrightarrow{u} \in V_3, W_{f_3^i}(\overrightarrow{u}) \in \{0, \pm 2^2\}$, т. е. начальные функции платовидны. Они также 0-устойчивы и удовлетворяют свойствам (К1)–(К3).

Применение вышеизложенной конструкции дает следующие 4 функции от 6 переменных:

$f_{n=3+3=6}^1 = (x_1 \cdot x_2 + x_1 \cdot x_3) \cdot (x_4 \cdot x_6 + x_4 + x_6 + 1) + (x_2 \cdot x_6 + x_2 \cdot x_3) \cdot (x_4 + 1) + {}$
$+ x_5 \cdot (x_1 \cdot x_2 + x_2 \cdot x_4 + x_3 \cdot x_4 + x_1) + x_6$;

$f_{n=3+3=6}^2 = (x_1 \cdot x_2 + x_1 \cdot x_3) \cdot (x_4 \cdot x_6 + x_4 + x_6 + 1) + (x_2 \cdot x_6 + x_2 \cdot x_3) \cdot (x_4 + 1) + {}$
$+ x_5 \cdot (x_1 \cdot x_2 + x_2 \cdot x_4 + x_3 \cdot x_4 + x_1) + x_4 + x_6$;

$f_{n=3+3=6}^3 = (x_1 \cdot x_2 + x_1 \cdot x_3) \cdot (x_4 \cdot x_6 + x_4 + x_6 + 1) + (x_2 \cdot x_6 + x_2 \cdot x_3) \cdot (x_4 + 1) + {}$
$+ x_5 \cdot (x_1 \cdot x_2 + x_2 \cdot x_4 + x_3 \cdot x_4 + x_1) + x_6 + 1$;

$f_{n=3+3=6}^4 = (x_1 \cdot x_2 + x_1 \cdot x_3) \cdot (x_4 \cdot x_6 + x_4 + x_6 + 1) + (x_2 \cdot x_6 + x_2 \cdot x_3) \cdot (x_4 + 1) + {}$
$+ x_5 \cdot (x_1 \cdot x_2 + x_2 \cdot x_4 + x_3 \cdot x_4 + x_1) + x_4 + x_6$;

Из теоремы 2 следует, что $W_{f_6^i} \in \{0, \pm 2^4\}$, т. е. новые функции платовидны и 1-устойчивы. Они также удовлетворяют свойствам (К1)–(К3).

Список литературы

1. Тарасников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 91–148.

2. Захаров К. В. О порождении бент-функций рекурсивными конструкциями. Дипломная работа. Москва, 2008.
3. Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001. Proceedings, Lecture Notes in Computer Science. — V. 2247. — Springer-Verlag, 2001. — P. 254–256.
4. Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics. — V. 6. — Elsevier Science, 2001.
5. Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity // Proceeding of Indocrypt 2000, Lecture Notes in Computer Science. — V. 1977. — Springer-Verlag, 2000. — P. 19–30.
6. Tarannikov Yu. New constructions of resilient Boolean functions with maximal nonlinearity // Fast Software Encryption. 8th International Workshop, FSE 2001, Yokohama, Japan, April 2–4, 2001. Revised Papers, Lecture Notes in Computer Science. — V. 2355. — 2002. — P. 66–77.

ДЛЯ ЗАМЕТОК

Подписано в печать 17.11.2015. Формат 60 × 84/16. Усл. печ. л. 4,9. Тираж 100 экз. Заказ М-7.
ИПМ им. М. В. Келдыша РАН. 125047, Москва, Миусская пл., 4