С.Н. Селезнева

НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ НАХОЖДЕНИЯ ПОЛИНОМОВ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ СХЕМ С РАЗДЕЛЕННЫМИ ПЕРЕМЕННЫМИ[1]

Введение

Схемная сложность булевых и многозначных функций является одним из разделов теории сложности. Это понятие было введено C.E. Shannon [1]. Им было показано, что схемная сложность "`самой сложной"' булевой функции от n переменных равна $O(2^n/n)$. О.Б. Лупановым [2] было доказано, что схемная сложность (в базисе из конъюнкции, дизъюнкции и отрицания) "`самой сложной"' булевой функции от n переменных асимптотически равна $2^n/n$. Однако, если известна более детальная информация о рассматриваемых функциях, то оценка сложности может уточняться.

Важное место в теории сложности занимает задача оценки *индивидуальной* сложности функций. В работах [3-5] исследовалась схемная сложность операций сложения и умножения двоичных чисел. Отметим работы В.Б. Алексеева [6], А.А. Вороненко [7, 8], С.Н. Селезневой [9] о схемной сложности решения некоторых задач, касающихся булевых и многозначных функций в случае, когда функции заданы векторами своих значений.

Особую роль в теории сложности играет вопрос о нахождении точных оценок схемной сложности функций и, в частности, их нижних оценок. Отметим работы Н.П. Редькина [10], В.И. Резника [11], Е.П. Сопруненко [12], L.H. Harper, W.N. Hsieh, J.E. Savage [13], C.P. Schnorr [14], А.А. Разборова [15], в которых найдены нижние оценки схемной сложности некоторых функций.

В настоящей работе доказывается точная нижняя оценка сложности нахождения коэффициентов полинома булевой функции в классе схем с разделенными переменными.

Основные понятия

Пусть $B = \{0, 1\}$. Множество B^n, $n \geq 1$, назовем *n-мерным булевым кубом*. На кубе B^n введем частичный порядок: если $\alpha = (a_1, \dots, a_n)$ и $\beta = (b_1, \dots, b_n)$, то $\alpha \leq \beta$ при $a_1 \leq b_1$, …, $a_n \leq b_n$.

[1] Работа поддержана РФФИ, гранты 10-01-00768-а, 12-01-00706-а.

Весом |α| набора $\alpha = (a_1, \dots, a_n) \in B^n$ назовем число единиц в нем. *Тенью* набора $\alpha = (a_1, \dots, a_n) \in B^n$ назовем множество $S(\alpha) = \{\beta \in B^n \mid \beta \leq \alpha, |\beta| = |\alpha| - 1\}$. Множество $B_k^n = \{\alpha \in B^n \mid |\alpha| = k\}$ назовем *k-м слоем* куба B^n, $0 \leq k \leq n$.

Функция $f(x_1, \dots, x_n)$ называется *булевой*, если $f: B^n \to B$, $n = 0, 1, 2, \dots$. Множество всех булевых функций обозначим как P_2, множество всех булевых функций, зависящих от переменных $x_1, \dots, x_n$, обозначим как P_2^n. *Вектором значений* функции $f(x_1, \dots, x_n) \in P_2$ назовем вектор u_f длины 2^n ее значений на всевозможных наборах α из множества B^n.

Каждая булева функция $f(x_1, \dots, x_n) \in P_2$ задается *полиномом* (по модулю 2), или *алгебраической нормальной формой* (АНФ), т.е. формулой вида

$$\sum_{\sigma=(s_1,\dots,s_n)\in B^n} c_f(\sigma) \cdot {x_1}^{s_1} \cdot \dots \cdot {x_n}^{s_n},$$

где $c_f(\sigma) \in B$, $\sigma \in B^n$, – коэффициенты, а ${x_i}^{s_i}$ – степени, т.е. ${x_i}^1 = x_i$, ${x_i}^0 = 1$, и сложение и умножение рассматривается по модулю 2.

Наша задача состоит в следующем: с какой алгоритмической сложностью можно по вектору значений u_f произвольной булевой функции $f(x_1, \dots, x_n) \in P_2$ найти вектор u_{c_f} коэффициентов ее полинома?

В качестве алгоритмической модели рассмотрим схемы из функциональных элементов (СФЭ) в некотором базисе.

(*Ориентированным*) *графом* G называется пара (V, E), где V – множество *вершин*, а E – множество *дуг*, причем задано правило, по которому каждой дуге $e \in E$ ставится в соответствие пара вершин $(u, v) \in V \times V$. Если $e = (u, v) \in E$, то говорят, что дуга e *выходит* из вершины u и *входит* в вершину v. (*Ориентированным*) *путем* в графе $G = (V, E)$ называется такая последовательность его вершин

$$v_{i_0} v_{i_1}, \dots, v_{i_{l-1}} v_{i_l},$$

что $\left(v_{i_{lj-1}}, v_{i_j}\right) \in E$ для всех $j = 1, \dots, l$. Ориентированный путь называется (*ориентированным*) *циклом*, если $v_{i_l} = v_{i_0}$. Для вершины $v \in V$ ее *полустепенью захода* назовем число $b(v) = |\{(u, v) \in E\}|$, т.е. число дуг, входящих в вершину v.

Схемой из функциональных элементов (СФЭ) S в базисе (из функциональных элементов) $A \subseteq P_2$ называется ориентированный граф без ориентированных циклов $G = (V, E)$, в котором каждой вершине $v \in V$ приписаны пометки по правилам:

1) если $b(v) = 0$, то вершина v называется *входной* и ей приписывается какая-то булева переменная x_i;

2) если $b(v) \geq 1$, то вершина v называется *внутренней* и ей приписывается какая-то функция $f \in A$, зависящая от $b(v)$ переменных, причем дуги, входящие в вершину v, по какому-то правилу согласуются с переменными функции f;

3) какие-то из вершин (как входные, так и внутренние) называют *выходными* и им приписывают выходные переменные y_j.

Если в схеме S входным вершинам приписаны переменные $x_1, \dots, x_n$ и выходным вершинам приписаны переменные $y_1, \dots, y_m$, говорят, что схема S с *входами* $x_1, \dots, x_n$ и *выходами* $y_1, \dots, y_m$ и обозначают $S(x_1, \dots, x_n;\ y_1, \dots, y_m)$.

Сложностью $L(S)$ СФЭ S назовем число ее внутренних вершин, т.е. число функциональных элементов в ней.

В каждой вершине v СФЭ $S(x_1, \dots, x_n;\ y_1, \dots, y_m)$ реализуется некоторая булева функция. Если вершина v – входная, и ей приписана переменная x_i, то в ней реализуется функция $f_v(x_i)$, тождественно равная переменной x_i. Если вершина v – внутренняя, ей приписана функция $f \in A$, и в вершинах, из которых ведут дуги в эту вершину v, реализуются (согласованно с переменными функции f) функции $f_1, \dots, f_{b(v)}$, то в вершине v реализуется функция $f(f_1, \dots, f_{b(v)})$. Будем полагать, что СФЭ $S(x_1, \dots, x_n;\ y_1, \dots, y_m)$ реализует систему $F_S = \{f_{y_1}, \dots, f_{y_m}\}$ функций, реализующихся в выходных ее вершинах $y_1, \dots, y_m$.

СФЭ S с входами $x_1, \dots, x_n$ и выходами $y_1, \dots, y_m$ называется *схемой с разделенными переменными* (СФЭРП), если для любых i и j ориентированный путь от входа x_i к выходу y_j существует только в том случае, когда реализующаяся на выходе y_j функция *существенно* зависит от переменной x_i.

Пусть v – вершина в СФЭ $S(x_1, \dots, x_n;\ y_1, \dots, y_m)$. Рассмотрим все ориентированные пути из входов $x_1, \dots, x_n$ в вершину v. Пусть V' и E' – множества вершин и дуг, принадлежащих этим путям, $G' = (V', E')$ – соответствующий граф, и $S'(x_{i_1}, \dots, x_{i_r};\ v)$ – соответствующая СФЭ на графе G' с одним выходом v. Назовем эту СФЭ $S'(x_{i_1}, \dots, x_{i_r};\ v)$ *кустом*, растущим из вершины v.

Под (битовой) сложностью алгоритма будем понимать сложность соответствующей СФЭ.

Известен быстрый алгоритм построения по вектору значений булевой функции $f(x_1, \dots, x_n)$ ее полинома, описанный Г.П. Гавриловым, А.А. Сапоженко в 1977 г. в [16]. Он реализуется СФЭРП в базисе $A_{L_0} = \{x \oplus y\}$ со сложностью $n \cdot 2^{n-1}$.

В настоящей работе мы докажем нижнюю оценку поставленной задачи и покажем, что алгоритм из [16] является оптимальным по сложности в классе схем с разделенными переменными.

О точной оценке сложности нахождения полинома булевой функции в классе схем с разделенными переменными

Вначале определим СФЭ, решающую нашу задачу.

Определение. Обозначим как Π_n любую такую СФЭ с 2^n входами $u(\alpha)$, $\alpha \in B^n$, и 2^n выходами $v(\sigma)$, $\sigma \in B^n$, что если на входах $u(\alpha)$ появляются значения $f(\alpha)$ произвольной функции $f(x_1, \dots, x_n) \in P_2$, то на выходах $u(\sigma)$ выдаются значения $u_{c_f}(\sigma)$ коэффициентов ее полинома.

Известно [17], как выражаются коэффициенты полинома булевой функции через ее значения.

Теорема 1. ([17]) *Для каждой булевой функции $f(x_1, \dots, x_n) \in P_2$ каждый коэффициент $c_f(\sigma)$, $\sigma \in B^n$, ее полинома может быть найден по формуле*

$$c_f(\sigma) = \sum_{\tau \le \sigma} f(\tau).$$

Следствие 1.1. *В СФЭ Π_n на ее выходах v реализуется система LP_n булевых функций ее входов u, где*

$$LP_n = \left\{ \sum_{\tau \le \sigma} f(\tau) \mid \sigma \in B^n \right\}.$$

Сначала докажем нижнюю оценку сложности СФЭРП Π_n в базисе $A_{L_0} = \{x \oplus y\}$ из одного элемента сложения по модулю 2.

Нам будет нужна вспомогательная лемма.

Лемма 2. *Если $\alpha, \beta \in B^n$, $\alpha \neq \beta$, то*

$$|(\{\alpha\} \cup S(\alpha)) \cap (\{\beta\} \cup S(\beta))| \le 1.$$

Доказательство. Действительно, если наборы α и β из разных слоев куба B^n, то в пересечении указанных множеств может быть не более одного элемента (если один из наборов лежит в тени другого). Если наборы α и β из одного и того же слоя куба B^n, то в пересечении их теней также не более одного элемента. Т.к. их тени из одного слоя, а наборы одного слоя различаются не менее, чем в двух координатах. Лемма 2 доказана.

Теперь можно сформулировать и доказать основную теорему.

Теорема 3. *В базисе $A_{L_0} = \{x \oplus y\}$ сложность СФЭРП Π_n не меньше $n \cdot 2^{n-1}$.*

Доказательство. Пусть нам задана какая-то СФЭРП Π_n. Докажем индукцией по весу набора σ, что в СФЭРП Π_n для каждого набора $\sigma \in B^n$

можно найти не менее $|\sigma|$ элементов, причем так, что для разных наборов σ и τ соответствующие им элементы не пересекаются.

Базис индукции: $|\sigma| = 1$. Рассмотрим в СФЭРП Π_n куст, растущий из выхода $v(\sigma)$. На выходе $v(\sigma)$ реализуется функция $f(0, \dots, 0) \oplus f(\sigma)$, поэтому этот куст содержит хотя бы один элемент. Припишем выходному элементу этого куста пометку σ. Ясно, что если $\sigma \neq \tau$, $|\sigma| = |\tau| = 1$, то пометки σ и τ будут приписаны разным элементам в силу свойства схемы быть с разделенными переменными. Положим $\Pi_n^1 = \Pi_n$.

Индуктивный переход от $(k-1)$ к k, $2 \leq k \leq n$.

Рассмотрим СФЭРП Π_n^{k-1} с входами $u(\alpha)$, $|\alpha| \geq k-2$. Преобразуем ее: подадим на все входы $u(\beta)$, $|\beta| = k-2$, значение 0 и удалим из схемы все элементы, хотя бы на один вход которых пришел 0. Рассмотрим теперь выходы $v(\tau)$, $|\tau| = k-1$. На каждом из них реализуется тождественная функция своего единственного (в силу разделенности переменных схемы) входа. Если на пути от входа к выходу есть элементы, удалим их также.

Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq k-1$, как Π_n^k. Заметим, что по построению в СФЭРП Π_n^k нет элементов с пометками.

Пусть $|\sigma| = k$. Рассмотрим в СФЭРП Π_n^k куст, растущий из выхода $v(\sigma)$. На выходе $v(\sigma)$ реализуется функция

$$u(\sigma) \oplus \sum_{\tau \in S(\sigma)} u(\tau),$$

поэтому этот куст содержит не менее k элементов (в силу существенности всех переменных этой функции). Припишем всем элементам этого куста пометку σ.

Если $\sigma_1 \neq \sigma_2$, $|\sigma_1| = |\sigma_2| = k$, то пометки σ_1 и σ_2 будут приписаны разным элементам. В самом деле, пусть какой-то элемент s получил хотя бы две пометки, σ_1 и σ_2, $\sigma_1 \neq \sigma_2$. Рассмотрим куст, растущий из элемента s. Если он содержит только один вход, то его без ущерба для схемы можно удалить. Пусть он содержит хотя бы два входа $u(\tau_1)$ и $u(\tau_2)$, $\tau_1 \neq \tau_2$. Тогда, т.к.

$$|(\{\sigma_1\} \cup S(\sigma_1)) \cap (\{\sigma_2\} \cup S(\sigma_2))| \leq 1,$$

например, не верно, что $\tau_1 \leq \sigma_2$.

Тогда, с одной стороны, найдется ориентированный путь от входа $u(\tau_1)$ к элементу s. А с другой стороны, найдется ориентированный путь от элемента s к выходу $v(\sigma_2)$. Получаем противоречие с разделенностью переменных схемы.

Следовательно,

$$L(\Pi_n) \geq \sum_{k=1}^{n} \sum_{\sigma \in B_k^n} k = \sum_{k=1}^{n} k \cdot C_n^k = n \cdot 2^{n-1}.$$

Теорема 3 доказана.

Следствие 3.1. *Минимальная сложность СФЭРП* Π_n *в базисе* $A_{L_0} = \{x \oplus y\}$ *равна* $n \cdot 2^{n-1}$.

Доказательство. Минимальная сложность СФЭ Π_1 равна 1. Если построить СФЭРП Π_n по индукции по свойству

$$f(x_1, x_2 \ldots, x_n) = f(0, x_2, \ldots, x_n) \oplus \big(f(0, x_2, \ldots, x_n) \oplus f(1, x_2, \ldots, x_n)\big),$$

то выведем соотношение

$$L(\Pi_n) \leq 2L(\Pi_{n-1}) + 2^{n-1}.$$

Откуда получаем СФЭРП Π_n со сложностью $n \cdot 2^{n-1}$. Нижняя оценка получена в теореме 3. Следствие 3.1 доказано.

Теорема 4. *Минимальная сложность СФЭРП* Π_n *в базисе* $A = \{x\&y, x \vee y, \bar{x}\}$ *лежит в пределах от* $3n \cdot 2^{n-1}$ *до* $4n \cdot 2^{n-1}$.

Доказательство. Для получения нижней оценки воспользуемся доказательством теоремы 3. Докажем индукцией по весу набора σ, что в СФЭРП Π_n для каждого набора $\sigma \in B^n$ можно найти не менее $3 \cdot |\sigma|$ элементов конъюнкции и дизъюнкции, причем так, что для разных наборов σ и τ соответствующие им элементы не пересекаются.

Опишем, какие изменения нужно внести в доказательство теоремы 3.

Рассмотрим индуктивный переход от $(k-1)$ к k, $2 \leq k \leq n$. Сначала преобразуем СФЭРП Π_n^{k-1} с входами $u(\alpha)$, $|\alpha| \geq k-2$. А именно, подадим на все входы $u(\beta)$, $|\beta| = k-2$, значение 0, и по правилам булевой алгебры удалим из схемы все элементы, хотя бы на один вход которых пришла константа.

Рассмотрим теперь выходы $v(\tau)$, $|\tau| = k-1$. На каждом из них реализуется тождественная функция своего единственного (в силу разделенности переменных схемы) входа. Если на пути от входа к выходу есть элементы конъюнкции и дизъюнкции, удалим их также без ущерба для схемы.

Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq k-1$, как Π_n^k. Заметим, что по построению в СФЭРП Π_n^k нет элементов конъюнкции и дизъюнкции с пометками.

Пусть $|\sigma| = k$. Рассмотрим в СФЭРП Π_n^k куст, растущий из выхода $v(\sigma)$. Тогда для функции $v(\sigma)$, $\sigma \in B_k^n$, реализующей сумму по модулю 2

своих $(k+1)$ входов, требуется не менее $3(k+1)-3=3k$ элементов конъюнкции и дизъюнкции [14]. Припишем всем таким элементам пометку σ.

Поэтому

$$L(\Pi_n) \geq \sum_{k=1}^{n} \sum_{\sigma \in B_k^n} 3k = \sum_{k=1}^{n} 3k \cdot C_n^k = 3n \cdot 2^{n-1}.$$

Верхняя оценка выводится из доказательства следствия 3.1 и сложности 4 реализации линейной функции $x \oplus y$ в базисе из конъюнкции, дизъюнкции и отрицания [3]. Т.е. из соотношения

$$L(\Pi_n) \leq 2L(\Pi_{n-1}) + 2^{n-1}$$

получаем $L(\Pi_n) \leq 4n \cdot 2^{n-1}$. Теорема 4 доказана.

С.Н. Селезневой [9] доказано, что при составных k сложность в классе схем с разделенными переменными проверки по вектору длины $N = k^n$ значений k-значной функции $f(x_1, \dots, x_n)$ ее полиномиальности и в случае положительного ответа нахождения какого-то ее полинома равна $O(k^n)$. Таким образом, в булевом случае в классе схем с разделенными переменными соответствующая задача решается сложнее.

Отметим также, что разделенность переменных – существенное свойство схем. К.А. Зыковым [18] найдено семейство множеств линейных булевых функций, которые с классе схем с разделенными переменными имеют бóльшую сложность, чем в классе схем без ограничений.

Список литературы

1. Shannon C.E. A symbolic analysis of relay and switching circuits // Trans. AIEE, 1938, v. 57, p. 713-723.

2. Лупанов О.Б. Об одном методе синтеза схем // Изв. вузов. Радиофизика. 1958, т. 1, № 1, с. 120-140.

3. Редькин Н.\,П. О минимальной реализации двоичного сумматора // Проблемы кибернетики, вып. 38. М.: Наука, 1981, с. 181-216.

4. Карацуба А.А., Офман Ю.П. Умножение многозначных чисел на автоматах // Докл. АН СССР, 1962, т. 145, № 2, с. 293-294.

5. Schonhage A., Strassen V. Computing Archiv fur elektronisches Reshnen. 1971, v. 7, N 3-4, p. 281-292.

6. Алексеев В.Б. Ступенчатые билинейные алгоритмы и распознавание полноты в k-значных логиках // Изв. вузов. Матем., 1988, № 7, с. 19-27.

7. Вороненко А.А. О сложности распознавания монотонности // Матем. вопросы кибернетики, 1999, т. 8, с. 301-303.

8. Вороненко А.А. О методе разложения для распознавания принадлежности инвариантным классам // Дискрет. матем. (2002) 14, вып. 4, с. 110-116.

9. Селезнева С.Н. Быстрый алгоритм построения для k-значных функций полиномов по модулю k при составных k // Дискрет. матем. (2011) 23, вып. 3, с. 3-22.

10. Редькин Н.П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики, вып. 23, М.: Наука, 1970, с. 83-101.

11. Резник В.И. Реализация монотонных функций схемами из функциональных элементов // Докл. АН СССР, 1961, т. 139, № 3, с. 566-569.

12. Сопруненко Е.П. О минимальной реализации некоторых функций схемами из функциональных элементов // Проблемы кибернетики, вып. 15, М.: Наука, 1965, с. 117-134.

13. Harper L.H., Hsieh W.N., Savage J.E. A class of Boolean functions with linear combinational complexity // Theoret. Comput. Sci., 1975, v. 1, N 2, p. 161-183.

14. Schnorr C.P. Zwei lineare untere Schranken fur die Komplexitat Boolescher Funktionen. Computing // Archiv fur elektronischer Rechnen, 1974, v. 13, N 2, p. 155-171.

15. Разборов А.А. Нижние оценки монотонной сложности некоторых булевых функций // Докл. АН СССР, 1985, т. 281, № 4, с. 798-801.

16. Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977.

17. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

18. Зыков К.А. О сравнении сложности двух способов реализации некоторых линейных булевых преобразований // Дискрет. матем. (1996) 8, вып. 2, с. 152-159.