МЕТОДЫ ДИСКРЕТНОГО АНАЛИЗА
В СИНТЕЗЕ РЕАЛИЗАЦИЙ БУЛЕВЫХ ФУНКЦИЙ

Сборник трудов
1991 г. Института математики СО АН СССР Выпуск 51

УДК 519.714

НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ РЕАЛИЗАЦИИ ХАРАКТЕРИСТИЧЕСКИХ ФУНКЦИЙ ДВОИЧНЫХ КОДОВ БИНАРНЫМИ ПРОГРАММАМИ

Е.А.Окольнишникова

Введение

Рассматривается реализация булевых функций бинарными программами (определение приводится ниже). Получены нелинейные нижние оценки для сложности реализации последовательностей характеристических функций двоичных кодов с большим числом кодовых вершин и с растущим (с ростом n) кодовым расстоянием в классе бинарных программ и в классе формул в базисе $(\vee, \&, \neg)$ (теоремы 1 и 2). В частности, получена оценка $C \cdot n \cdot \ln n / \ln \ln n$ для характеристических функций кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов) с кодовым расстоянием $\ln n / \ln \ln n$ в классе бинарных программ (следствие 3 теоремы 1).

Пусть BP_K – класс бинарных программ, в которых каждый путь содержит не более K проверок одной и той же переменной. В работе показано, что при $K = C_1 \cdot \ln n / \ln \ln n$, где $0 < C_1 < 1$, существует двоичный линейный код, сложность реализации характеристической функции которого в классе BP_K не меньше чем $exp(n^{(1-C_1)/2})$. Сложность реализации той же функции в классе бинарных программ без ограничений не превышает $2n^2$ т.е. ограничение на количество проверок в цепи по каждой из переменных дает экспоненциальный относительно числа переменных рост сложности бинарной программы (теорема 3).

Работа состоит из 5 параграфов. В § I даны определения и обозначения. В § 2 приводится основная идея доказательства. В § 3 приводится нижняя оценка сложности реализации булевой функции в классе BP_k. Теоремы I и 2 даны в § 4, а теорема 3 – в § 5.

§ I. Определения и обозначения

Через $E(X)$ обозначим множество вершин n-мерного единичного куба, т.е. множество всех наборов значений двоичных переменных $X=\{x_1,\dots,x_n\}$. Назовем (n,M,d)-кодом такое подмножество из M наборов в $E(X)$, что координаты любых двух вершин различаются между собой по меньшей мере в d разрядах [I].

Напомним, что бинарная программа (б.п.) – это ориентированный граф без циклов, состоящий из входной вершины (у нее нет входящих дуг и имеется две выходящих), из внутренних вершин (у каждой из них не меньше одной входящей дуги и двух выходящих) и выходных вершин (у них нет выходящих дуг). Каждая внутренняя вершина, а также входная вершина помечены булевой переменной из множества $X=\{x_1,\dots,x_n\}$, выходная вершина – константой 0 или I. Поскольку из каждой вершины, за исключением выходных вершин, выходит 2 дуги, то в каждой из таких пар дуг припишем одной из дуг константу 0, а другой – I.

Пусть задан входной набор $\tilde{a}=(a_1,\dots,a_n)$, $a_i\in\{0,1\}$ для $i=1,\dots,n$. Б.п. $\mathcal{P}$ по набору $\tilde{a}$ вычисляет значение $\mathcal{P}(\tilde{a})$, равное 0 или I, следующим образом. Вычисление начинается во входной вершине. Если мы достигли вершины, которой приписана переменная x_i, то проверяем эту переменную; затем переходим к следующей вершине так: если $a_i=1$, – то по дуге, помеченной I; если $a_i=0$, – то по дуге, помеченной 0. Поскольку из каждой вершины, за исключением выходных, выходит одна дуга, помеченная 0, а другая – I, а б.п. – это ориентированный граф без циклов, то в конце концов мы достигнем выходной вершины, помеченной 0 или I. Это и будет значение $\mathcal{P}(\tilde{a})$.

Говорят, что б.п. $\mathcal{P}$ вычисляет булеву функцию (б.ф.) $f(X)$, если для любого набора $\tilde{a}=(a_1,\dots,a_n)$ значений входных переменных выполняется тождество $\mathcal{P}(\tilde{a}) = f(\tilde{a})$. Сложность $B(\mathcal{P})$ б.п. $\mathcal{P}$ определяется как число вершин вычисления б.п. $\mathcal{P}$ (под вершинами вычисления понимаются входная и внутренние вершины б.п.). Через $B(f)$ обозначим минимальную сложность б.п., реализующей б.ф. f.

Бинарную программу, в которой любой путь от входной вершины к выходной содержит не более k вершин, помеченных одной и той же переменной, будем называть k-программой. Сложность реализаций б.ф. f в классе k-программ (класс BP_k) обозначим через $B_k(f)$.

Поскольку ниже мы будем иметь дело только с бинарными программами и бинарными k-программами, то слово "бинарный" в ряде случаев будем опускать.

Введем понятие однородной k-программы. Будем говорить, что вершина a_i предшествует вершине a_j в б.п. $\mathcal{P}$, если существует путь, идущий от a_i к a_j. Бинарную k-программу назовем однородной, если для любой вершины и каждой переменной число проверок по этой переменной на любом пути, идущем от входа к рассматриваемой вершине, не зависит от пути (по разным переменным может быть разное число проверок). При этом число проверок по любой переменной для любого пути, идущего от входной вершины к выходной, должно быть равным k.

В ряде случаев б.п. удобно расcматривать как контактную схему с ограничениями на ее "топологию". Заменим в б.п., реализующей б.ф. f, каждую дугу, которой приписана константа I (соответственно 0), выходящую из вершины, помеченной переменной x_i, на контакт x_i (соответственно $\bar{x}_i$). Получим контактный (I,2)-полюсник, реализующий булевы функции f и $\bar{f}$.

Функцию, получающуюся из б.ф. $f(x_1,\dots,x_n)$ при подстановке констант $\tilde{a}$, $\tilde{a} \in E(X_1)$ вместо переменных $X_1 = \{x_{i_1}, x_{i_2}, \dots, x_{i_m}\}$ будем обозначать через $f/_{X_1=\tilde{a}}$. Как обычно, через N_f обозначим множество единиц б.ф. f.

Если $\alpha \in E(X)$, то элементарную конъюнкцию от переменных X, обращающуюся в единицу в вершине α, будем обозначать также через α.

§ 2. Основная идея доказательства

Кратко поясним основную идею метода получения нижних оценок сложности в классе бинарных программ, предложенную в настоящей работе. Пусть $\mathcal{P}$ – произвольная б.п., реализующая б.ф. $f(x_1, \ldots, x_n)$. Если для какой-то переменной x_i число проверок по этой переменной в некоторой цепи (пути) превышает K, то число вершин б.п. $\mathcal{P}$, помеченных переменной x_i, больше, чем K. Ясно, что при большом количестве таких переменных сложность $B(\mathcal{P})$ б.п. должна быть немалой. Если число таких переменных невелико, то, заменяя эти переменные константами, можно от б.п. $\mathcal{P}$ перейти к б.п. $\mathcal{P}'$, реализующей некоторую подфункцию б.ф. f и принадлежащей классу BP_K. В связи с этим представляет интерес получение нелинейных нижних оценок сложности реализации булевых функций и в. классе BP_K.

Для получения высоких нижних оценок в классе BP_K преобразуем бинарную K-программу $\mathcal{P}'$ в однородную K-программу $\mathcal{P}_0$, не слишком увеличивая сложность (лемма I). Рассмотрим путь в б.п. $\mathcal{P}_0$, соответствующий некоторой единице α б.ф. g. Разобьем этот путь на $\varphi(K)$ отрезков, при этом $\varphi(K)$ выбирается существенно большим, чем K. Так как $\mathcal{P}_0 \in BP_K$, то каждая из переменных будет встречаться не более чем на K отрезках пути. Будет показано, что можно выбрать m отрезков пути $(m \geq K)$ так, что число переменных, входящих только в выбранные отрезки, но не входящих в остальные отрезки, будет не очень мало. И аналогично, число переменных, не входящих в выбранные отрезки, но входящих только в остальные отрезки, будет также не очень мало (лемма 2). Поставим в соответствие вершине α, $\alpha \in N_g$, множество $\psi(\alpha)$ вершин б.п. $\mathcal{P}_0$, а именно концы выбранных отрезков (лемма 3). Пусть $K(\psi)$ – множество единиц б.ф. g, которым поставлено в соответствие одно и то же множество ψ вершин б.п. $\mathcal{P}_0$. В лемме 4 будут приведены ограничения, которые накладываются на множество $K(\psi)$. В частности, в § 4 будет показано, что для последовательности кодов с растущим кодовым расстоянием и большим числом кодовых вершин (например, для последовательности БЧХ-кодов с растущим кодовым расстоянием), $|K\psi|$ мало по сравнению с N_g. Поэтому для рассматриваемых в § 4 кодов велико число различных подмножеств вершин б.п., которым поставлены в соответствие единицы б.ф., и соответственно велико и число вершин программы.

§ 3. Получение нижних оценок сложности реализации булевых функций K-программами

Покажем, что любую K-программу можно преобразовать в однородную K-программу (реализующую ту же функцию), не слишком увеличивая сложность. Для этого в первоначальную K-программу будут введены фиктивные проверки переменных.

ЛЕММА I. Бинарную K-программу $\mathcal{P}$, реализующую б.ф. f от n переменных, можно преобразовать в реализующую ту же б.ф. однородную K-программу $\mathcal{P}_0$, у которой число вершин $B^q(\mathcal{P}_0)$, лежащих на расстоянии, кратном q, от входной вершины, удовлетворяет неравенству

$$B^q(\mathcal{P}) \le 2 \cdot \frac{Kn}{q} \cdot B(\mathcal{P}),$$

ДОКАЗАТЕЛЬСТВО.

I) Через $\ell_s(a_j)$ обозначим максимальное число проверок переменной x_s по всем путям, идущим от входной вершины к вершине a_j в б.п. $\mathcal{P}$. Ясно, что если вершина a_i предшествует вершине a_j, то для $s = 1, 2, \ldots, n$ имеем

$$\ell_s(a_i) \le \ell_s(a_j). \tag{I}$$

Предположим, что в б.п. $\mathcal{P}$ есть дуга (a_i, a_j), выходящая из вершины a_i и входящая в вершину a_j. Тогда направим соответствующий выход вершины a_i на фиктивные проверки переменных: $(\ell_1(a_j) - \ell_1(a_i))$ проверок переменной x_1, $(\ell_2(a_j) - \ell_2(a_i))$ – переменной x_2 - и т.д. (см. рис. I). Из (I) следует, что $\ell_s(a_j) - \ell_s(a_i) \ge 0$, поэтому такое преобразование возможно.

Проделаем эту процедуру со всеми дугами б.п. $\mathcal{P}$. В результате получим б.п. $\mathcal{P}_0$, и при этом кратность проверки переменной x_s по любому пути, идущему от входной вершины к выходной вершине E, будет равна $\ell_s(E)$. Добавим на выходе схемы $(\kappa - \ell_s(E))$ фиктивных проверок переменной x_s, $s = 1,2,\ldots$ $\ldots, n$. В итоге получим однородную κ-программу $\mathcal{P}_0$, реализующую ту же б.ф., что и б.п. $\mathcal{P}$.

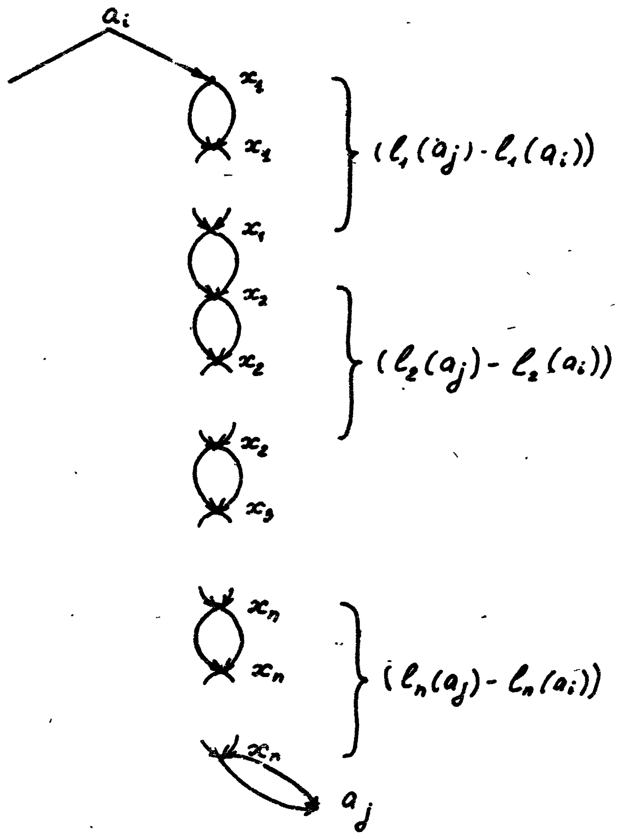

Рис. I

2) Вместо каждой дуги может быть вставлено самое большее $\kappa \cdot n$ фиктивных проверок переменных. Из них не больше чем $\kappa \cdot n / q$ находятся на расстоянии, кратном q, от входа, поэтому число вершин в $B^q(\mathcal{P}_0)$ в б.п. $\mathcal{P}_0$ не более чем в $\kappa \cdot n / q$ раз превосходит число дуг в б.п. $\mathcal{P}$. Остается учесть, что число вершин вычисления ровно в два раза меньше, чем число дуг б.п. Лемма доказана.

Пусть $\mathcal{P}$ – однородная κ-программа, реализующая б.ф. $f(x_1,\ldots,x_n)$. Так как на любом пути, идущем от входной вершины к выходной, встречаются все переменные, то любой путь реализует некоторую элементарную конъюнкцию (здесь удобно рассматривать б.п. как контактную схему с ограничением на топологию). Рассмотрим путь, соответствующий конкретной элементарной конъюнкции. Длина этого пути равна $\kappa\cdot n$. На этом пути выберем $(\varphi+1)$ вершину $a_0, a_1, \ldots, a_\varphi$, где вершина a_i предшествует вершине a_j при $0\le i\le j\le\varphi$. В качестве a_0 рассмотрим входную вершину, а в качестве a_φ – выход, помеченный I. При этом число дуг, расположенных между двумя соседними вершинами a_i и a_{i+1}, за исключением, возможно, двух последних, должно быть равно $\lceil \kappa\cdot n/\varphi\rceil$.

Пусть A_i, $i=0,1,\ldots,\varphi-1$, – множество тех переменных (без учета кратности), которые встречаются на данном пути от a_i к a_{i+1}; при этом переменная, которой помечена вершина a_i, относится к множеству A_i, но не относится к множеству A_{i+1}. Так как вершина a_φ – выходная, то ей не приписана никакая переменная. Выберем m вершин $a_{i_1}, a_{i_2},\ldots, a_{i_m}$ из множества $\{a_0, a_1,\ldots, a_{\varphi-1}\}$. Выбор этих вершин задает на выбранном пути m отрезков $(a_{i_1}, a_{i_1+1}), (a_{i_2}, a_{i_2+1}),\ldots,(a_{i_m}, a_{i_m+1})$. Пусть

$Q^1_{i_1,\ldots,i_m}$ – множество переменных, встречающихся <u>только на</u> выбранных отрезках;

$Q^2_{i_1,\ldots,i_m}$ – множество переменных, встречающихся <u>только вне</u> выбранных отрезков;

$Q^0_{i_1,\ldots,i_m}$ – множество переменных, встречающихся <u>как на</u> выбранных отрезках, <u>так</u> и <u>вне</u> их. Ясно, что множества $Q^1_{i_1,\ldots,i_m}$, $Q^2_{i_1,\ldots,i_m}$ и $Q^0_{i_1,\ldots,i_m}$ попарно не пересекаются.

ЛЕММА 2. **Существует такая последовательность вершин $(a_{i_1},\ldots,a_{i_m})$, что для порожденных ею множеств переменных имеют место оценки:**

$$|Q^1_{i_1,\ldots,i_m}| \ge n\cdot C^{m-\kappa}_{\varphi-\kappa}/C^m_\varphi;$$

$$|Q^{2}_{i_1,\ldots,i_m}| \geq n\cdot\left(1-\frac{km}{\varphi}\right)+n\cdot(k-1)\cdot C^{m-k}_{\varphi-k}\Big/ C^{m}_{\varphi}\ .$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим граф G (рис. 2), содержащий два множества вершин: n вершин, соответствующих переменным $x_1,\ldots,x_n$ и C^m_φ вершин, соответствующих всевозможным m-элементным подмножествам множества из φ отрезков. Вершину, соответствующую переменной x_i, соединим с вершиной, соответствующей подмножеству $\{i_1,\ldots,i_m\}$, в том и только том случае, когда $x\in Q^1_{i_1,\ldots,i_m}$, т.е. когда x_i входит в отрезки $A_{i_1},\ldots,A_{i_m}$, но не входит в остальные отрезки. Через ℓ_i обозначим число отрезков, в которые входит переменная x_i. Так как в любой цепи любая переменная встречается ровно k раз, то $\ell_i\leq k$. Поэтому вершина x_i соединена в графе G со всеми подмножествами, содержащими эти ℓ_i отрезков, а число таких подмножеств равно $C^{m-\ell_i}_{\varphi-\ell_i}$. Подсчет числа ребер в графе G показывает, что

$$\sum_{\{i_1,\ldots,i_m\}} Q^1_{i_1,\ldots,i_m} = \sum_{i=1}^{n} C^{m-\ell_i}_{\varphi-\ell_i}\ . \qquad (2)$$

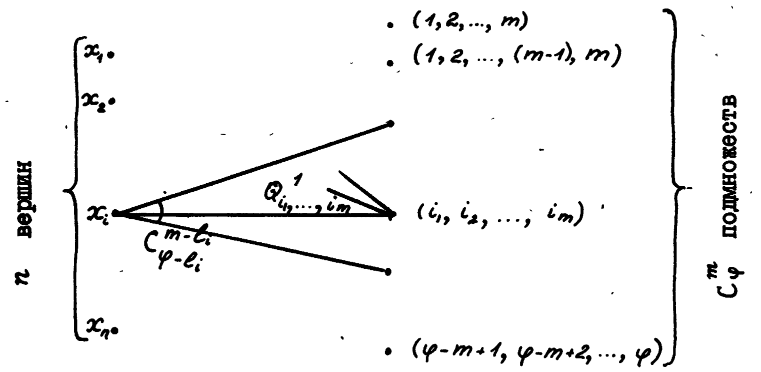

Рис. 2

Так как $C^{m-\ell_i}_{\varphi-\ell_i}\geq C^{m-k}_{\varphi-k}$ при $\ell_i\leq k$, то из (2) следует, что существует подмножество $(i_1,\ldots,i_m)$, для которого

$$|Q^1_{i_1,\dots,i_m}| \geq n \cdot C^{m-k}_{\varphi-k} / C^m_{\varphi} . \qquad (3)$$

Общее число переменных, входящих во множества $A_{i_1},\dots,A_{i_m}$, удовлетворяет неравенству

$$|A_{i_1} \cup \dots \cup A_{i_m}| \leq \lceil k \cdot n/\varphi \rceil \cdot m - (k-1) \cdot |Q^1_{i_1,\dots,i_m}| . \qquad (4)$$

Поскольку

$$|Q^2_{i_1,\dots,i_m}| = n - |A_{i_1} \cup \dots \cup A_{i_m}| ,$$

то из (4) и (3) следует, что

$$|Q^2_{i_1,\dots,i_m}| \geq n - \lceil k \cdot n/\varphi \rceil \cdot m + (k-1)\,|Q^1_{i_1,\dots,i_m}| \geq$$

$$\geq n \cdot \left(1 - \frac{km}{\varphi}\right) + (k-1) \cdot n \cdot C^{m-k}_{\varphi-k} / C^m_{\varphi} .$$

Лемма доказана.

Множество вершин $a_1,\dots,a_t$ назовем линейной последовательностью вершин, если в однородной б.п. $\mathcal{P}_0$ существует путь от входной вершины к выходной, проходящий через вершины $a_1,\dots,a_t$, и вершина a_i предшествует вершине a_j при $i < j$ и a_i не совпадает с a_j при $i \neq j$.

Пусть $a_1,\dots,a_{2l}$ – линейная последовательность вершин однородной бинарной k-программы $\mathcal{P}_0$. Пусть X – множество переменных, которыми помечены вершины б.п. $\mathcal{P}_0$. По аналогии с множествами $Q^1_{i_1,\dots,i_m}$, $Q^2_{i_1,\dots,i_m}$ и $Q^0_{i_1,\dots,i_m}$, определенными выше для путей б.п., определим для последовательности вершин $a_1,\dots,a_{2l}$ множества переменных $Q^j(a_1,\dots,a_{2l})$, $j \in \{0,1,2\}$. Рассмотрим путь в б.п. $\mathcal{P}_0$, проходящий через вершины $a_1,\dots,a_{2l}$. Пусть $Q^1(a_1,\dots,a_{2l})$ – множество переменных, которые встречаются только на отрезках пути $(a_1,a_2),(a_3,a_4),\dots,(a_{2l-3},a_{2l-2})$ и (a_{2l-1},a_{2l}), но не встречаются на остальных отрезках заданного пути. Обозначим входную вершину через a_0, выходную – через a_{2l+1}. Пусть $Q^0(a_1,\dots,a_{2l})$ – множество переменных, которые встречаются только на отрезках пути $(a_0,a_1),(a_2,a_3),\dots,(a_{2l-2},a_{2l-1})$ и (a_{2l},a_{2l+1}), но не встречаются на остальных отрезках пути. Пусть $Q^0(a_1,\dots,a_{2l})$ – множество всех остальных переменных, т.е.

$$Q^0(a_1,\dots,a_{2\ell}) = X \setminus (Q^1(a_1,\dots,a_{2\ell}) \cup Q^2(a_1,\dots,a_{2\ell})) .$$

При этом переменная, которой помечена вершина a_i, $i = 1,\dots,2\ell$, относится к отрезку (a_i, a_{i+1}), но не относится к отрезку (a_i, a_{i+2}). Ясно, что множества $Q^1(a_1,\dots,a_{2\ell}), Q^2(a_1,\dots,a_{2\ell})$, $Q^0(a_1,\dots,a_{2\ell})$ не пересекаются. Кроме того, в силу однородности б.п., эти множества не зависят от выбора пути, а зависят только от последовательности вершин.

ЛЕММА 3. Пусть $\mathcal{P}_0$ — однородная K-программа, реализующая б.ф. f от n переменных; φ, K, m — заданные значения параметров, где $K \le m \le \varphi$. Тогда каждой единице α б.ф. f можно в б.п. $\mathcal{P}_0$ поставить в соответствие такую последовательность вершин $\psi(\alpha) = \{a_1,\dots,a_{|\psi(\alpha)|}\}$, что

1) ее длина четна и не превышает $2m$.

2) любая из ее вершин находится на расстоянии, кратном $\lceil Kn/\varphi \rceil$ от входной вершины;

3) имеют место соотношения:

$$|Q^1(\psi/\alpha)| \ge n \cdot C^{m-K}_{\varphi-K} / C^m_\varphi ;$$

$$|Q^2(\psi/\alpha)| \ge n \cdot (1 - \frac{Km}{\varphi}) + n(K-1) \cdot C^{m-K}_{\varphi-K} / C^m_\varphi .$$

ДОКАЗАТЕЛЬСТВО. Докажем утверждение I леммы. Пусть в б.п. $\mathcal{P}_0$ на одном из путей, реализующих элементарную конъюнкцию α по лемме 2 выбрано m отрезков $(a_{i_1}, a_{i_1+1}), (a_{i_2}, a_{i_2+1}), \dots$ $\dots, (a_{i_m}, a_{i_m+1})$ таких, что мощности множеств $Q^1_{i_1,\dots,i_m}$ и $Q^2_{i_1,\dots,i_m}$ удовлетворяют неравенствам леммы 2. Без ограничения общности можно считать, что $i_1 < i_2 < \dots < i_m$. Рассмотрим упорядоченное множество концов выбранных отрезков

$$\omega(\alpha) = \{a_{i_1}, a_{i_1+1}, a_{i_2}, a_{i_2+1}, \dots, a_{i_m}, a_{i_m+1}\} .$$

В случае, когда конец одного отрезка $(a_{i_j}, a_{i_{j+1}})$ совпадает с началом другого отрезка $(a_{i_{j+1}}, a_{i_{j+2}})$, рассмотрим увеличенный отрезок $(a_{i_j}, a_{i_{j+2}})$ и из множества $\omega(\alpha)$ выбросим оба вхождения вершины $a_{i_{j+1}}$. Продолжая этот процесс дальше, можно от множества $\omega(\alpha)$ перейти к последовательности вершин $\psi(\alpha)$, в которой каждая вершина встречается не более одного раза. Утверждение I леммы доказано.

Утверждение 2 леммы следует из выбора вершин концов отрезков на пути, реализующем конъюнкцию α. Так как $\mathcal{P}_0$ – однородная программа, то из построения последовательности $\psi(\alpha)$ из множества $\omega(\alpha)$ следует, что $Q^i(\psi(\alpha)) = Q^i_{i_1,\dots,i_m}$, $i = 0, 1, 2$, а, значит, мощности этих множеств удовлетворяет неравенствам леммы. Утверждение 3 леммы тоже верно.

Лемма доказана.

Любой путь однородной K-программы реализует некоторую элементарную конъюнкцию. Через $T(\psi)$ обозначим дизъюнкцию всех элементарных конъюнкций, реализуемых всевозможными путями б.п., проходящими через последовательность вершин ψ.

ЛЕММА 4. Д.н.ф. $T(\psi)$ можно представить в виде

$$T(\psi) = \bigvee_{\tilde{\alpha} \in E(Q^0(\psi))} \mathcal{K}^{\tilde{\alpha}}(Q^0(\psi)) \cdot T^1_{\tilde{\alpha}}(Q^1(\psi)) \cdot T^2_{\tilde{\alpha}}(Q^2(\psi)),$$

где $\mathcal{K}^{\tilde{\alpha}}(Q^0(\psi))$ – конъюнкция, принимающая на наборе $\tilde{\alpha}$ переменных из множества $Q^0(\psi)$ значение I, а $T^1_{\tilde{\alpha}}$ и $T^2_{\tilde{\alpha}}$ – совершенные д.н.ф. от переменных из множеств $Q^1(\psi)$ и $Q^2(\psi)$ соответственно.

ДОКАЗАТЕЛЬСТВО. Зафиксируем набор значений $\tilde{\alpha}$ переменных из $Q^0(\psi)$. Пусть $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_p$ – конъюнкции из $T(\psi)$, содержащие множитель $\mathcal{K}^{\tilde{\alpha}}(Q^0(\psi))$, т.е.

$$\mathcal{K}_t = \mathcal{K}^{\tilde{\alpha}}(Q^0(\psi)) \& \beta_t(Q^1(\psi)) \& \gamma_t(Q^2(t)),$$

где $t \in \{1,\dots,p\}$. Для доказательства леммы достаточно показать, что для любых i и j, $i \in \{1,\dots,p\}$, $j \in \{1,\dots,p\}$, существует путь в б.п. $\mathcal{P}_0$, проходящий через последовательность вершин ψ и реализующий конъюнкцию $\mathcal{K}' = \mathcal{K}^{\tilde{\alpha}}(Q^0(\psi)) \cdot \beta_i(Q^1(\psi)) \cdot \gamma_j(Q^2(\psi))$.

Пусть $\psi = (b_1, b_2, \dots, b_{2l-1}, b_{2l})$. Рассмотрим путь S, идущий от входной вершины до вершины b_1 по пути, реализующему $\mathcal{K}_j$; от b_{2t-1} до b_{2t} – по пути, реализующему $\mathcal{K}_i$; от b_{2t} до b_{2t+1} – по пути, реализующему $\mathcal{K}_j$, где $t = 1, \dots, l$. Пусть на этом чередующемся пути реализуется конъюнкция $\mathcal{K}_0$. При этом те отрезки S, на которых мы идем по пути, реализующем $\mathcal{K}_i$, содержат переменные из $Q^0(\psi)$ и $Q^1(\psi)$, и поэтому их вклад в конъюнкцию $\mathcal{K}_0$ равен $\mathcal{K}^{\tilde{\alpha}} \& \beta_i (Q^1(\psi))$. Все остальные отрезки S, на которых мы идем по пути, реализующем $\mathcal{K}_j$, содержат переменные из $Q^0(\psi)$ и $Q^2(\psi)$, и поэтому их вклад в конъюнкцию $\mathcal{K}_0$ равен $\mathcal{K}^{\tilde{\alpha}}(Q^0(\psi)) \cdot \gamma_j (Q^2(\psi))$. Таким образом,

$$\mathcal{K}_0 = \mathcal{K}^{\tilde{\alpha}} \cdot \beta_i (Q^1(\psi)) \cdot \gamma_j (Q^2(\psi)),$$

т.е. путь S реализует конъюнкцию $\mathcal{K}_0$, равную $\mathcal{K}'$. Лемма доказана.

В лемме 3 каждой единице α б.ф. f поставлена в соответствие последовательность $\psi(\alpha)$ вершин б.п. $\mathcal{P}_0$. Через $\mathcal{K}(\psi)$ обозначим множество единиц б.ф. f, которым поставлена в соответствие последовательность ψ вершин б.п.

Для совершенной д.н.ф. $T(\psi)$ под $|T(\psi)|$ понимается число различных элементарных конъюнкций, входящих в эту д.н.ф. Ясно, что

$$|\mathcal{K}(\psi)| \leq |T(\psi)|. \tag{5}$$

Лемма 4 накладывает некоторые ограничения на структуру д.н.ф. $T(\psi)$, а значит, и на $|T(\psi)|$ и поэтому, по (5), на $|\mathcal{K}(\psi)|$.

Леммы 5 и 6 позволяют оценивать $|\mathcal{K}(\psi)|$ через величины, зависящие не от конкретной б.п., а от функции, реализуемой этой программой.

Рассмотрим б.ф. $H(X_1 \cup X_2)$, где $X_1 \cap X_2 = \emptyset$. Пусть $h_1(X_1)$ и $h_2(X_2)$ – такие б.ф. от переменных X_1 и X_2 соответственно, что $N_{h_1(X_1) \cdot h_2(X_2)} \subseteq N_{H(X_1 \cup X_2)}$. Положим

$$M_H(X_1, X_2) = \max_{h_1, h_2} (|N_{h_1}| \cdot |N_{h_2}|).$$

ЛЕММА 5. Для последовательности вершин ψ однородной K-программы $\mathcal{P}_0$, реализующей б.ф. $f(X)$, выполняются соотношения

$$|\mathcal{K}(\psi)| \le \sum_{\tilde{a}} M_{f/Q^0(\psi)=\tilde{a}}(Q^1(\psi), Q^2(\psi))$$

и

$$|\mathcal{K}(\psi)| \le \sum_{\tilde{a}} (\max_{\tilde{b}} N_{f/Q^0(\psi)=\tilde{a}, Q^1(\psi)=\tilde{b}} \cdot \max N_{f/Q^0(\psi)=\tilde{a}, Q^2(\psi)=\tilde{c}}),$$

где $\tilde{a} \in E(Q^0(\psi))$, $\tilde{b} \in E(Q^1(\psi))$, $\tilde{c} \in E(Q^2(\psi))$.

ДОКАЗАТЕЛЬСТВО. Оценим число конъюнкций в д.н.ф. $T(\psi)$. Получим

$$|T(\psi)| \le \sum_{\tilde{a}} |N_{T^1_{\tilde{a}}}(Q^1(\psi))| \cdot |N_{T^2_{\tilde{a}}}(Q^2(\psi))| \le$$

$$\le \sum_{\tilde{a}} M_{f/Q^0(\psi)=\tilde{a}} \cdot (Q^1(\psi), Q^2(\psi)).$$

Из этого факта и из (5) следует утверждение леммы.

Для б.ф. $f(X)$ определим величины $\mathcal{M}_1(f)$ и $\mathcal{M}_2(f)$ следующим образом:

$$\mathcal{M}_1 = \max_{Q^0, Q^1, Q^2} \sum_{\tilde{a}} \mathcal{M}_{f/Q^0=\tilde{a}}(Q^1, Q^2)$$

и

$$\mathcal{M}_2 = \max_{Q^0, Q^1, Q^2} \sum_{\tilde{a}} (\max_{\tilde{b}} N_{f/Q^0=\tilde{a}, Q^1=\tilde{b}} \cdot \max_{\tilde{c}} N_{f/Q^0=\tilde{a}, Q^2=\tilde{c}}), \qquad (6)$$

где максимум берется по всевозможным разбиениям множества переменных X на попарно-непересекающиеся множества Q^0, Q^1 и Q^2, такие, что мощности этих множеств удовлетворяют неравенствам

$$|Q^1| \ge |X| \cdot C^{m-k}_{\varphi-k} / C^m_\varphi \qquad (7)$$

и

$$|Q^2| \ge |X| \cdot (1 - \frac{km}{\varphi}) + |X| \cdot (k-1) \cdot C^{m-k}_{\varphi-k} / C^m_\varphi. \qquad (8)$$

При этом $\tilde{a} \in E(Q^0)$, $\tilde{b} \in E(Q^1)$, $\tilde{c} \in E(Q^2)$.

ЛЕММА 6. Для любой однородной κ-программы $\mathcal{P}_0$, реализующей б.ф. f, и произвольной последовательности вершин ψ этой б.п. выполняются соотношения

$$|\mathcal{K}(\psi)| \leq \mathcal{M}_1 \leq \mathcal{M}_2 .$$

ДОКАЗАТЕЛЬСТВО. Для любой последовательности ψ вершин б.п., которая поставлена в соответствие единице б.ф. f в б.п. $\mathcal{P}_0$, множества переменных $Q^0(\psi)$, $Q^1(\psi)$ и $Q^2(\psi)$ удовлетворяют требованиям, предъявляемым к множествам Q^0, Q^1 и Q^2 при определении величин $\mathcal{M}_1(f)$ и $\mathcal{M}_2(f)$. Поэтому из леммы 5 следует утверждение данной леммы.

Через $R(\mathcal{P})$ обозначим число различных последовательностей вершин б.п. $\mathcal{P}$, которые поставлены в соответствие единицам б.ф. f при заданных значениях параметров φ, m, κ. Пусть

$$R(f) = \min_{\mathcal{P}} R(\mathcal{P}), \tag{9}$$

где минимум берется по всем б.п., реализующим б.ф. f. Тогда

$$R(f) \geq \frac{|N_f|}{\mathcal{M}_1(f)} \geq \frac{|N_f|}{\mathcal{M}_2(f)} . \tag{10}$$

Из формулы Стирлинга при $m \leq n/2$, получаем

$$\frac{1}{\pi\sqrt{m}\, e^{3m^2/4n}} \cdot \left(\frac{ne}{m}\right)^m \leq C_n^m \leq \frac{1}{2}\left(\frac{ne}{m}\right)^m . \tag{11}$$

ЛЕММА 7. Сложность $B_\kappa(f)$ реализации б.ф. f бинарной κ-программой при $5 \leq \kappa \leq m \leq \varphi < \kappa n$ и $\kappa m < \varphi$ удовлетворяет соотношению

$$B_\kappa(f) \geq \frac{(R(f))^{1/(2m)} \cdot 2m}{e \cdot \varphi} ,$$

где $R(f)$ задается формулой (9).

ДОКАЗАТЕЛЬСТВО. Пусть κ-программа $\mathcal{P}$ реализует б.ф. f. Согласно лемме I, от б.п. $\mathcal{P}$ перейдем к однородной κ-программе $\mathcal{P}_0$, также реализующей б.ф. f. Пусть $\mathcal{L}_0$ – множество вершин K-программы $\mathcal{P}_0$, лежащих на расстоянии, кратном $\lceil Kn/\varphi \rceil$, от входной вершины. Все элементы последовательности $\psi(\alpha)$, поставленной в соответствие конъюнкции α, принадлежат множеству $\mathcal{L}_0$ по построению. Поэтому $R(\mathcal{P}_0)$, т.е. число различных последовательностей вершин $\mathcal{P}_0$, которые поставлены в соответствие единицам б.ф. f, удовлетворяют соотношению:

$$R(\mathcal{P}_0) \leq \sum_{i=0}^{m} C_{|\mathcal{L}_0|}^{2i} < \quad (\text{т.к. } m \leq \frac{\varphi}{K} \leq \frac{|\mathcal{L}_0|}{K} \leq \frac{|\mathcal{L}_0|}{5}) <$$

$$< 2 \cdot C_{|\mathcal{L}_0|}^{2m} < (\text{см.}(\mathrm{II})) < \frac{2(|\mathcal{L}_0| e)^{2m}}{2 \cdot (2m)^{2m}}$$

Отсюда

$$|\mathcal{L}_0| \geq \frac{(R(\mathcal{P}_0))^{1/(2m)} \cdot 2m}{e} . \qquad (12)$$

Так как $|\mathcal{L}_0| = B^{q}(\mathcal{P}_0)$ при $q = \lceil Kn/\varphi \rceil$ (см. лемму I), то из леммы I следует, что

$$B(\mathcal{P}) \geq \frac{2\lceil Kn/\varphi \rceil}{Kn} |\mathcal{L}_0| \geq \frac{2|\mathcal{L}_0|}{\varphi} \geq (\text{см.}(12)) \geq \frac{(R(\mathcal{P}_0))^{(1/2m)} m}{e \cdot \varphi} .$$

Поскольку $\mathcal{P}_0$ – произвольная K-программа, реализующая б.ф. f, то лемма справедлива.

Таким образом, нами получена нижняя оценка сложности реализации б.ф. в классе бинарных K-программ.

§ 4. Нижняя оценка сложности реализации последовательности характеристических функций двоичных кодов бинарными программами и формулами в базисе $(\vee, \&, \neg)$

Через $F_1, F_2, \dots, F_n, \dots$ обозначим последовательность характеристических функций для двоичных $(n, 2^{n-\ell_n}, d_n)$-кодов[ж)], где $d_n \geq 2 r_n + 1$, а

[ж)] В дальнейшем индекс n при ℓ_n, r_n и d_n в ряде случаев будет опускаться.

$$n^2/(r^2\cdot 2^{\ell/r})\to\infty,\quad \frac{r\cdot \ln(n^2/(r^2\cdot 2^{\ell/r}))}{\ln n}\to\infty. \tag{I3}$$

В теореме I будет показано, что последовательность $\{F_n\}$ имеет нелинейную относительно n сложность реализации бинарными программами. В следствии I будет дан вариант этой оценки. В следствиях 2 и 3 приведены нижняя и верхняя оценки сложности реализации последовательности характеристических функций БЧХ-кодов бинарными программами. Теорема 2 – аналог теоремы I в классе формул в базисе $(\vee, \&, \neg)$. Доказательство теоремы I и ее следствий будет дано в конце параграфа.

Зафиксируем константу C, $0<C<1$, и положим

$$K(n)=C\cdot\frac{\ln(n^2/(r^2\cdot 2^{\ell/r}))}{\frac{2\ln n}{r}+\ln\ln(n^2/(r^2\cdot 2^{\ell/r}))}. \tag{I4}$$

Ясно, что для последовательности б.ф. $\{F_n\}$ функция $K(n)\to\infty$ при $n\to\infty$.

ТЕОРЕМА I. Для сложности реализации последовательности б.ф. $\{F_n\}$ в классе бинарных программ имеет место оценка

$$B(F_n)\geqslant C\cdot K(n)\cdot n,$$

где $K(n)$ задается формулой (I4).

СЛЕДСТВИЕ I. Для последовательности $G_1, G_2, \ldots, G_n, \ldots$ характеристических функций двоичных $(n, 2^{n-\ell_n}, d_n)$ - кодов, удовлетворяющих условию

$$\frac{\ell_n}{r_n\cdot\ln(n/r_n)}\leqslant C_1<2,$$

где C_1 - константа, а $d_n\geqslant 2r_n+1$, имеет место оценка:

$$B(G_n)\geqslant C\cdot K_2(n)\cdot n,$$

где

$$K_2(n) = \begin{cases} C\cdot\dfrac{(2-C_1)\ln(n/\tau)}{\ln\ln(n/\tau)} & \text{при } \tau > \ln n/\ln\ln n; \\ C\cdot(2-C_1)\tau & \text{при } \tau < \ln n/\ln\ln n; \\ C\cdot\dfrac{(2-C_1)}{(1+2/C_0)}\cdot\dfrac{\ln n}{\ln\ln n} & \text{при } \tau = C\cdot\ln n/\ln\ln n. \end{cases}$$

СЛЕДСТВИЕ 2. Пусть H_τ - характеристическая функция БЧХ-кода [I] с параметрами (n, M, d), где $d \geq 2\tau+1$, $M \geq 2^n/(n+1)^\tau$. Если $n/\tau_n^2 \to \infty$ и $\tau_n \to \infty$ при $n \to \infty$, то для любой константы C, $0 < C < 1$ справедливы неравенства:

$$C\cdot n\cdot\frac{\ln(n/\tau^2)}{\frac{2\ln n}{\tau}+\ln\ln(n/\tau^2)} \leq B(H_\tau) \leq 2\tau n\cdot\ln n.$$

Из этого следствия непосредственно получаем

СЛЕДСТВИЕ 3. Для характеристической функции БЧХ-кода H_τ при $\tau = \ln n/\ln\ln n$ справедливы оценки:

$$n\cdot\frac{\ln n}{\ln\ln n} \leq B(H_\tau) \leq n\cdot\frac{\ln^2 n}{\ln\ln n}.$$

Через $L_{(\vee,\&,\neg)}(f)$ обозначим сложность реализации б.ф. f формулами в базисе $(\vee,\&,\neg)$. Известно [2], что $L_{(\vee,\&,\neg)}(f) \geq B(f)-1$. Поэтому из теоремы I немедленно следует

ТЕОРЕМА 2. Для сложности реализации последовательности б.ф. $\{F_n\}$ в классе формул в базисе $(\vee,\&,\neg)$ имеет место оценка

$$L_{(\vee,\&,\neg)}(F_n) \geq C\cdot K(n)\cdot n,$$

где $K(n)$ задается формулой (I4).

Переходим к доказательству теоремы I и ее следствий. Предварительно докажем лемму 8.

ЛЕММА 8. Если параметры n, τ, ℓ удовлетворяют соотношениям (I3) и $K(n)$ задается формулой (I4), то при

$n_1 = (1-C)\cdot n / C^{K}_{K^2+K}$; $n_2 = (1-C)n/(K+1)$, и достаточно больших n выполняются соотношения:

I) $K(n) < r$;

2) $\ln(C^{r}_{n_1}\cdot C^{r}_{n_2}) \geq r[\ln(n^2/r^2) - K\cdot\ln(K\cdot e^{3/2})]$.

ДОКАЗАТЕЛЬСТВО. Проверим первое сотношение. Так как $2^{\ell/r} > 1$, то при $n \to \infty$ из (I3) следует, что

$$n/r = \sqrt{n^2/(r^2\cdot 2^{\ell/r})}\cdot\sqrt{2^{\ell/r}} \to \infty . \qquad (I5)$$

Число вершин двоичного кода длины n с кодовым расстоянием d, $d \geq 2r+1$, не превышает $2^n/C^r_n$. Поэтому $2^{n-\ell} < 2^n/C^r_n$ и, значит, $2^{\ell} > C^r_n$, Тогда из (II) при достаточно больших n имеем

$$2^{\ell/r} \geq (C^r_n)^{1/r} > (n/r) . \qquad (I6)$$

Так как функция $\ln x/\ln\ln x$ монотонно возрастает при $x > 15{,}2$, то из (I5) и (I6) следует, что

$$K(n) < C\cdot\frac{\ln(n^2/(r^2\cdot 2^{\ell/r}))}{\ln\ln(n^2/(r^2\cdot 2^{\ell/r}))} < C\cdot\frac{\ln(n/r)}{\ln\ln(n/r)} . \qquad (I7)$$

Поэтому если $r \geq \ln n/\ln\ln n$, то $K(n) \leq Cr$. Если $r < \ln/\ln\ln n$, то при достаточно больших n

$$K(n) \leq \frac{Cr\ln(n^2/(r^2\cdot 2^{\ell/r}))}{2\ln n} < C\cdot r .$$

Первое соотношение доказано.

Для доказательства второго утверждения леммы проверим, что $r < n_1/2$. Из (II) следует, что

$$n_1 \geq \frac{2\cdot(1-C)n}{e^K(K+1)^K} . \qquad (I8)$$

Отсюда при достаточно больших n имеем:

$$\ln(n_1/2r) \geq \ln(1-C) + \ln n - K - K\ln(K+1) - \ln r \geq \quad \text{(по (17))} \geq$$

$$\geq \ln(1-C) + \ln(n/r) - 1 - C\cdot\frac{\ln(n/r)}{\ln\ln(n/r)}\cdot(\ln\ln(n/r) - \ln\ln\ln(n/r) + 1 +$$

$$+ \ln C) \geq (1-C)\cdot\ln(n/r) + C\cdot\frac{\ln(n/r)}{\ln\ln(n/r)}\cdot\frac{1}{2}\ln\ln\ln(n/r) + O(1).$$

Тогда из (15) получим

$$n_1/2r \to \infty \tag{19}$$

при $n \to \infty$.

Аналогичное соотношение имеем для n_2, т.е.

$$n_2/2r \to \infty \tag{20}$$

при $n \to \infty$. Тогда, по (11),

$$\ln(C_{n_1}^{r}\cdot C_{n_2}^{r}) \geq \ln\left(\frac{n_1\cdot n_2\cdot e^2}{r^2}\right)^r\cdot\frac{1}{\pi^2 r\cdot e^{3r^2/4n_1 + 3r^2/4n_2}} \geq$$

$$\geq r\cdot\left[\ln n_1 + \ln n_2 + 2 - 2\ln r - \frac{\ln\pi^2 r}{r} - \frac{3r}{4n_1} - \frac{3r}{4n_2}\right] \geq$$

(из (18)-(20) и так как $r \to \infty$, $K \to \infty$) $\geq$

$$\geq r\cdot[2\ln n - K - K\ln K - \ln K - 2\ln r - O(1)] \geq$$

$$\geq r\,[\ln n^2/r^2 - 1{,}5K - K\ln K].$$

Лемма доказана.

ДОКАЗАТЕЛЬСТВО теоремы I. Пусть $\mathcal{P}$ – б.п., реализующая б.ф. $F_n(X)$ от n переменных, а X_0 – множество переменных, каждая из которых приписана не меньше чем $K(n)$ вершинам б.п. $\mathcal{P}$. Если $|X_0| \geq C\cdot n$, то $B(F_n) \geq C\cdot K(n)\cdot n$ и теорема верна.

Допустим, что $|X_0| < C\cdot n$. Зафиксируем переменные из множества X_0 таким образом, чтобы для б.ф. $g(X\setminus X_0) = F_n/_{X_0=\tilde{a}}$ выполнялось соотношение

$$N_g \geq N_{F_n}\cdot 2^{-|X_0|}. \tag{21}$$

Тогда от б.п. $\mathcal{P}$, реализующей б.ф. $F_n(X)$, можно без увеличения сложности перейти к K-программе $\mathcal{P}'$, реализующей б.ф. $g(X \setminus X_0)$ от n' переменных,

$$n' > (1-C)\,n\,. \qquad (22)$$

При этом $B(F_n) \geq B_K(g) + |X_0| \cdot K(n)$, и для доказательства теоремы достаточно показать, что

$$B_K(g) \geq C \cdot K(n) \cdot |X \setminus X_0| = C \cdot K(n) \cdot n' \geq C \cdot (1-C) \cdot K(n) \cdot n\,. \qquad (23)$$

Положим $\varphi = K^2 + K$, $m = K$. Пусть подмножества Q^1, Q^2 и Q^0 множества переменных $(X \setminus X_0)$ удовлетворяют условиям (7),(8), т.е.

$$|Q^1| \geq \frac{n'}{C^K_{K^2+K}} > \frac{(1-C)\cdot n}{C^K_{K^2+K}} = n_1\,;\quad |Q^2| \geq \frac{n'K}{K^2+K} - \frac{(K-1)\cdot n'}{C^K_{K^2+K}} > \frac{(1-C)n}{(K+1)} = n_2$$

и $|Q^0| = n' - |Q^1| - |Q^2|$. Оценим сверху величину M_2 (см. (6)). Так как все единицы б.ф. $g|_{Q^0=\tilde{a},\,Q^2=\tilde{c}}$ лежат на расстоянии не меньше чем $(2r+1)$ друг от друга, то

$$N_{g|_{Q^0=\tilde{a},\,Q^2=\tilde{c}}} \leq \frac{2^{|Q^1|}}{C^r_{n_1} + \ldots + C^0_{n_1}} < \frac{2^{|Q^1|}}{C^r_{n_1}}$$

и аналогично

$$N_{g|_{Q^0=\tilde{a},\,Q^1=\tilde{b}}} < \frac{2^{|Q^2|}}{C^r_{n_2}}\,.$$

Поэтому имеем

$$M_2 \leq 2^{|Q^0|} \cdot \frac{2^{|Q^1|}}{C^r_{n_1}} \cdot \frac{2^{|Q^2|}}{C^r_{n_2}} < \frac{2^{n-|X_0|}}{C^r_{n_1} \cdot C^r_{n_2}}\,. \qquad (24)$$

Тогда

$$R(g) \geq (\text{см.}(10)) \geq \frac{N_g}{M_2} \geq (\text{см.}(24)) \geq \frac{N_g \cdot C^r_{n_1} \cdot C^r_{n_2}}{2^{n-|X_0|}} \geq$$

$$\geq \frac{2^{n-\ell} \cdot C^r_{n_1} \cdot C^r_{n_2}}{2^n} = C^r_{n_1} \cdot C^r_{n_2} \cdot 2^{-\ell}\,.$$

Отсюда и из леммы 8 следует, что

$$\ln R(q) \geqslant \tau \cdot [\ln (n^2/(\tau^2 \cdot 2^{\ell/\tau})) - \kappa \cdot \ln(\kappa \cdot e^{3/2})] . \tag{25}$$

Тогда при достаточно больших n получаем

$$\ln B_\kappa(q) - \ln [C \cdot (1-C) \cdot \kappa(n) \cdot n] \geqslant \quad \text{(по лемме 7)} \geqslant$$

$$\geqslant \ln \frac{(R(q))^{1/2\kappa} \cdot 2\kappa}{e \cdot (\kappa^2+\kappa)} - \ln (C \cdot (1-C) \cdot \kappa(n) \cdot n) \geqslant \quad \text{(из (25))} \geqslant$$

$$\geqslant \frac{\tau}{2\kappa} \cdot \kappa \cdot \ln (n^{2/\tau}) - \frac{6\tau}{2\kappa} \ln \kappa \geqslant \frac{\tau}{2\kappa}[\ln(n^2/(\tau^2 \cdot 2^{\ell/\tau})) - \kappa \cdot \ln(\kappa \cdot n^{2/\tau} \cdot e^2)] \geqslant$$

$\geqslant$(так как $\tau \geqslant \kappa$, по лемме 8) $\geqslant \frac{\tau}{2\kappa}[\ln (n^2/(\tau^2 \cdot 2^{\ell/\tau})) - \kappa \ln(\kappa \cdot e^{3/2})] -$

$$- \frac{\tau}{2\kappa} \cdot \kappa \cdot \ln (n^{2/\tau}) - \frac{6\tau}{2\kappa} \ln \kappa \geqslant \frac{\tau}{2\kappa} [\ln (n^2/(\tau^2 \cdot 2^{\ell/\tau})) - \kappa \cdot \ln(\kappa \cdot n^{2/\tau} \cdot e^2)] \geqslant$$

(подставляя $\kappa(n)$) $\geqslant \frac{\tau}{2\kappa} [\ln (n^2/(\tau^2 \cdot 2^{\ell/\tau})) -$

$$- C \cdot \frac{\ln (n^2/(\tau^2 \cdot 2^{\ell/\tau}))}{\ln (n^{2/\tau}) + \ln \ln (n^2/(\tau^2 \cdot 2^{\ell/\tau}))} \times [2 + \ln(n^{2/\tau}) + \ln \ln(n^2/(\tau^2 \cdot 2^{\ell/\tau})) +$$

$$+ \ln C - \ln \ln \ln(n^2/(\tau^2 \cdot 2^{\ell/\tau}))] \geqslant \frac{\tau}{2\kappa} [(1-C) \cdot \frac{\ln (n^2/(\tau^2 \cdot 2^{\ell/\tau}))}{\ln(n^{2/\tau}) + \ln \ln(n^2/(\tau^2 \cdot 2^{\ell/\tau}))} \times$$

$$\times \frac{1}{2} \ln \ln \ln (n^2/(\tau^2 \cdot 2^{\ell/\tau}))] \to \infty ,$$

т.е. формула (23) верна. Теорема доказана.

Следствие I вытекает непосредственно из теоремы I.

ДОКАЗАТЕЛЬСТВО следствия 2. В этом случае

$$\ell < \tau \cdot \log_2 (n+1) . \tag{26}$$

Проверим выполнение условий (I3). При $n \to \infty$, по условиям следствия 2, имеем

$$n^2/(\tau^2 \cdot 2^{\ell/\tau}) \sim n/\tau^2 \to \infty .$$

Если $r > \ln n$, то

$$\frac{r\cdot \ln (n^2/(r^2\cdot 2^{\ell/r}))}{\ln n} \geqslant \ln (n/r^2) \to \infty .$$

Если $r \leqslant \ln n$, то

$$\frac{r\cdot \ln (n^2/(r^2\cdot 2^{\ell/r}))}{\ln n} \sim \frac{r\cdot \ln (n/r^2)}{\ln n} \gtrsim \frac{r}{2} \to \infty ,$$

т.е. условия (13) выполняются. Тогда, по теореме I, справедлива нижняя оценка.

Код БЧХ - линейный, поэтому для его реализации достаточно рассмотреть конъюнкцию не более чем ℓ линейных функций. Известно, что сложность реализации любой линейной функции в классе б.п. не превышает $2n$. Из этого факта и из (26) следует верхняя оценка. Следствие доказано.

§ 5. Экспоненциальный рост сложности бинарной программы при ограничении на число проверок переменной в цепи

Пусть

$$\lambda_K(f) \geqslant B_K(f)/B(f) \quad \text{и} \quad \lambda_K(n) = \max \lambda_K(f),$$

где максимум берется по всем булевым функциям от n переменных.

ТЕОРЕМА 3. Для любой константы C, $0 < C < 1$, выполняется соотношение

$$\lambda_{C\cdot \ln n/\ln\ln n} \gtrsim \exp(n^{(1-C)/2}) .$$

ДОКАЗАТЕЛЬСТВО. Пусть $K(n) = C\cdot \ln n/\ln\ln n$. Рассмотрим последовательность характеристических функций БЧХ-кодов с параметрами $(n, 2^{n-\ell_n}, 2r_n+1)$, где $r_n = \lceil \sqrt{n/(K^K\cdot e^{3/2K} e^2)}\,\rceil$, $\ell_n \geqslant r\cdot \log_2 (n+1)$. Тогда

$$\ln r(n) = 1/2 [\ln n - K\ln K - 3/2 K - 2] =$$

$$= 1/2 [\ln n - C\cdot (\ln n/\ln\ln n)\times(\ln C + \ln n - \ln\ln n - 3/2) - 2] ,$$

т.е.

$$r(n) = n^{(1-c)/2} \exp\left[\frac{c}{2}\cdot\frac{\ln n}{\ln\ln n}\cdot\ln\ln\ln n - O\left(\frac{\ln n}{\ln\ln n}\right)\right]. \qquad (27)$$

Проверим выполнение условий следствия 2, а значит, и теоремы I. При $n\to\infty$ имеем $n/r^2 \sim K^K\cdot e^{3K/2+2} \to \infty$, $r\to\infty$. Используя (25), получим при достаточно больших n, что

$$\ln B_K(H_r) \geqslant \text{(по лемме 7)} \geqslant \frac{\ln R(H_r)}{2K} + \ln 2K - 1 - \ln(K^2+K) \geqslant$$

$$\geqslant \text{(по (25))} \geqslant \frac{r}{2K}\left[K\cdot\ln K + \frac{3}{2}K + 2 + \ln\frac{n}{n+1} - K\ln K - \frac{3}{2}K\right] - 2\ln K \geqslant$$

$$\geqslant \text{(по (27))} \geqslant n^{(1-c)/2}\cdot\exp\left[\frac{c}{2}\cdot\frac{\ln n}{\ln\ln n}\cdot\ln\ln\ln n - O\left(\frac{\ln n}{\ln\ln n}\right) - \frac{1}{2}\ln\ln n\right] - 2\ln K \geqslant 2\cdot\log_2 n\cdot n^{(1-c)/2}$$

Тогда

$$B_K(H_r) \geqslant n^2\cdot\exp(n^{(1-c)/2}).$$

Так как (по (26)), $B(H_r) \leqslant 2\cdot \ell_n\cdot n \leqslant 2rn\log_2(n+1) < n^2$, то теорема доказана.

Литература

I. MAC WILLIAMS F.J., SLOANE N.J.A. The theory of error-correcting codes,I,II. North-Holland publishing Co., Amsterdam-New York-Oxford, 1977. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. - М.: Связь. - 1979. - 744 с.

2. WEGENER I. Complexity of Boolean functions. John Wiley and Sons, and B.G.Teubner, Stuttgart. - 1987. - XI + 457 p.

Поступила в ред.-изд.отдел
22 мая 1991 г.