

УДК 519.714.4 + 519.725

ОБ ОДНОМ МЕТОДЕ ПОЛУЧЕНИЯ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ НЕДЕТЕРМИНИРОВАННЫМИ ВЕТВЯЩИМИСЯ ПРОГРАММАМИ*)

Е. А. Окольнішнікова

Предложен метод получения нижних оценок сложности реализации булевых функций недетерминированными ветвящимися программами. Получена нелинейная нижняя оценка $\Omega(n \log n / \log \log n)$ для сложности реализации характеристических функций кодов Рида—Маллера такими программами.

Введение

Получение нижних оценок для сложности реализации последовательностей булевых функций — важное направление в теории управляющих систем. В последнее время интенсивно исследуются ветвящиеся программы. В статье рассматривается реализация булевых функций недетерминированными ветвящимися программами. Получена нелинейная нижняя оценка сложности реализации характеристических функций кодов Рида—Маллера в этом классе схем.

Наилучшей известной нижней оценкой сложности реализации функций такими программами является оценка $\Omega(\frac{n^{3/2}}{\log n})$, полученная П. Пудлаком [11] с помощью метода Нечипорука [2]. Кроме того, на недетерминированные ветвящиеся программы переносятся известные оценки для сложности реализации булевых функций контактно-вентильными схемами, в частности оценка $\Omega(n \log \log \log^* n)$, полученная А. А. Разборовым для сложности реализации ряда симметрических булевых функций, включая функцию голосования MAJ_n , для контактно-вентильных схем [5].

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 00-01-00874) и Федеральной целевой программы «Интеграция» (проект АО-110).

Наилучшей известной нижней оценкой для сложности реализации функций детерминированными ветвящимися программами является оценка $\Omega(\frac{n^2}{\log^2 n})$, полученная П. Пудлаком [11] с помощью метода Нечипорука [2].

Для некоторых симметрических булевых функций, в частности для функции голосования, П. Пудлак [10] получил нижнюю оценку $\Omega(n \log \log n / \log \log \log n)$ в классе детерминированных ветвящихся программ. Впоследствии эта оценка была усилена до оценки $\Omega(n \log n) (\log \log n)^{-1}$ для сложности реализации некоторых симметрических булевых функций, в том числе для функции голосования MAJ_n и для элементарной симметрической функции от n переменных, которая принимает значение 1 на наборах, содержащих $\lfloor n/2 \rfloor$ единиц [6].

В [3] были получены оценки сложности реализации характеристических функций двоичных кодов с большим числом кодовых вершин и растущим (по n) кодовым расстоянием в классе детерминированных ветвящихся программ. В частности, получена нижняя оценка $\Omega(n \log n / \log \log n)$ для характеристических функций кодов Боуза—Чоудхури—Хоквингема (БЧХ) с кодовым расстоянием $\log n / \log \log n$. Эти коды широко используются в теории кодирования и ее приложениях, тем не менее вопрос об конструктивности их задания остается.

В настоящей статье рассматривается реализация булевых функций недетерминированными и детерминированными ветвящимися программами. Приведены нелинейные нижние оценки сложности реализации булевых функций ветвящимися программами, исходя из сложности покрытий множества единиц булевой функции функциями определенного вида (теорема 4), в частности исходя из числа единиц булевой функции в гранях куба определенной размерности (теорема 5). Применение этих результатов позволило получить нелинейные нижние оценки $\Omega(n \log n / \log \log n)$ сложности реализации характеристических кодов Риды—Маллера недетерминированными программами.

Оценки были получены некоторой модификацией метода из [3, 8]. Этот метод сводит получение нижних оценок сложности реализации булевых функций ветвящимися программами без ограничений к получению нижних оценок сложности реализации подфункций рассматриваемой функции в классе ветвящихся программ с ограничениями на число проверок каждой переменной в любой цепи (ветвящиеся k -программы).

В настоящее время известны два метода [3, 7] получения нижних оценок сложности реализации функций ветвящимися k -программами. В [3, 8] были получены экспоненциальные нижние оценки сложности реализации булевых функций детерминированными ветвящимися k -программами при $k(n) = O(\log n / \log \log n)$. Впоследствии этот метод был

распространен на недетерминированные ветвящиеся программы [9, 4]; в [7] были получены экспоненциальные нижние оценки для сложности реализации булевых функций недетерминированными ветвящимися k -программами при $k(n) = O(\log n)$. В настоящей работе при получении нижних оценок сложности реализации подфункций рассматриваемой функции используется метод из [3, 8].

При получении результата существенно используются результаты из [13] по обобщенным весам Хемминга для линейных кодов.

В § 1 изложена общая идея доказательства и приведено некоторое обоснование того, почему при получении нижних оценок сложности ветвящихся k -программ мы отдали предпочтение методу из [3, 8]. В § 2 содержатся определения и предварительные сведения. В § 3 доказывается основной результат (теорема 1), позволяющий сводить получение нижних оценок сложности реализации булевых функций программами без ограничений к получению нижних оценок сложности реализации подфункций рассматриваемой функции программами с ограничениями (ветвящиеся k -программы). В § 4 рассматривается метод получения нижних оценок сложности для ветвящихся k -программ, приводятся основные теоремы, позволяющие получать нижние оценки сложности реализации функции программами без ограничений. В § 6 применяется результат из [13] по обобщенным весам Хемминга для подсчета числа единиц характеристической функции кода Рида—Маллера, лежащих в гранях куба определенной размерности. Это позволяет в § 6 получить нелинейные нижние оценки сложности реализации характеристических функций кодов Рида—Маллера недетерминированными ветвящимися программами.

§ 1. Идея метода получения нижних оценок

Идея метода получения нелинейных нижних оценок для ветвящихся программ без ограничений [3, 8] заключается в следующем. Пусть \mathcal{P} — произвольная ветвящаяся детерминированная программа, реализующая булеву функцию $f(x_1, x_2, \dots, x_n)$. Если число проверок переменной x_i в некоторой цепи (пути) от входной вершины к выходной превышает $k(n)$, где $k(n) \rightarrow \infty$ при $n \rightarrow \infty$, и число таких переменных не очень мало, то сложность ветвящейся программы не может быть малой. Если число таких переменных мало, то эти переменные можно «забить» константами, что позволит от первоначальной схемы \mathcal{P} перейти к схеме \mathcal{P}' с ограничениями на число проверок каждой переменной в цепи, т. е. рассмотреть реализацию некоторой подфункции функции f ветвящейся $k(n)$ -программой.

Этот подход позволяет свести получение нижних оценок сложности реализации булевой функции программой без ограничений к получению нижних оценок сложности реализации подфункций рассматриваемой булевой функции схемами с ограничениями, а именно ветвящимися $k(n)$ -программами.

Можно отметить, что предложенные в [3, 7, 9, 12] методы для получения высоких нижних оценок сложности реализации булевых функций ветвящимися k -программами схожи. Пусть \mathcal{P} — ветвящаяся программа, реализующая булеву функцию f от n переменных. Каждой единице булевой функции f (т. е. набору, на котором функция равна 1) ставится в соответствие путь в \mathcal{P} . Этот путь делится на «равные» части, и каждому такому пути ставится в соответствие или подмножество вершин [3, 9], или некоторое подмножество дуг ветвящейся программы [7, 12], позволяющее отделять одну часть от другой. Мощности этих множеств зависят только от заранее выбранных параметров и существенно меньше длины пути. С каждым таким множеством вершин (или дуг) ассоциируется функция f_i , зависящая только от этого подмножества вершин или дуг программы \mathcal{P} и не зависящая от пути, по которому она строилась. При этом

$$f = \vee f_i, \quad (1)$$

т. е. функции f_i задают покрытие множества единиц функции f . Если число единиц каждой функции f_i не очень большое, а число единиц функции f велико, то и число различных подмножеств, которые ставятся в соответствие единицам булевой функции, велико. Это позволяет оценить снизу число вершин (или дуг) ветвящейся программы.

В [3] для получения нижних оценок сложности ветвящихся программ используется сопоставление с каждой единицей булевой функции последовательности вершин ветвящейся программы. Это требует преобразования ветвящейся программы к однородному виду (точное определение этого понятия дано в § 2), что приводит к некоторому усложнению программы, но позволяет рассматривать обобщенные отрезки пути. Это позволяет ставить в соответствие каждому пути не все вершины, первоначально служившие разделителями частей, на которые делился путь ветвящейся программы, а только часть из них. При таком подходе в некоторых случаях удается получить лучшие оценки, чем при применении метода из [7], особенно в тех случаях, когда ветвящиеся k -программы используются при получении нижних оценок сложности для ветвящихся программ без ограничений.

При применении метода Бородина, Разборова, Смоленски [7] каждой единице булевой функции ставится в соответствие последовательность

дуг ветвящейся программы. Это, с одной стороны, не требует приведения программы к однородному виду, но, с другой стороны, не позволяет объединять отрезки пути, т. е. каждому пути необходимо ставить в соответствие все дуги, которые служили разделителями пути программы на части. При получении нижней оценки сложности ветвящейся программы этим методом требуется извлекать корень большой степени из мощности полученного покрытия множества единиц функции из (1).

§ 2. Определения, предварительные сведения

Недетерминированной ветвящейся программой от переменных x_1, \dots, x_n называется ориентированный граф без циклов с одной входной и двумя выходными вершинами, одна из которых помечена нулем, другая — единицей. Из каждой вершины, за исключением выходных, выходит две дуги. При этом все невыходные вершины делятся на два типа:

— вершины, помеченные переменными из множества $\{x_1, \dots, x_n\}$; из каждой такой вершины выходит одна дуга, помеченная единицей, и одна дуга, помеченной нулем;

— недетерминированные вершины («guessing nodes», «V-nodes», «existential nodes»); эти вершины не помечены и из каждой такой вершины выходит ровно две непомеченных дуги (свободные дуги).

Булева функция $f(x_1, \dots, x_n)$, реализуемая недетерминированной ветвящейся программой, описывает проводимость между входной и выходной вершиной, помеченной единицей, в зависимости от значений переменных x_1, \dots, x_n . Число вершин, помеченных переменными, называется *сложностью* недетерминированной ветвящейся программы \mathcal{P} и обозначается через $NBP(\mathcal{P})$. Сложность минимальной недетерминированной программы, реализующей функцию f , называется *сложностью реализации* булевой функции f и обозначается через $NBP(f)$.

Недетерминированная ветвящаяся программа называется *детерминированной ветвящейся программой*, если в ней нет недетерминированных вершин. Под *сложностью* детерминированной ветвящейся программы \mathcal{P} понимается число невыходных вершин, которое будем обозначать через $BP(\mathcal{P})$. Сложность минимальной детерминированной программы, реализующей функцию f , называется *сложностью реализации* булевой функции f и обозначается через $BP(f)$.

Ветвящаяся (недетерминированная или детерминированная) программа называется k -программой (k — натуральное число) тогда и только тогда, когда для каждого i , $1 \leq i \leq n$, вдоль любого пути

от входной вершины к выходной вершине встречается не более k вхождений переменной x_i . Сложность реализации булевой функции f недетерминированными и детерминированными ветвящимися k -программами будем обозначать через $\text{NBPk}(f)$ и $\text{BPk}(f)$ соответственно.

Ветвящуюся (недетерминированную или детерминированную) программу будем называть *однородной*, если для любой вершины a и для любого i , $1 \leq i \leq n$, на каждом пути, идущем от входной вершины к вершине a , число вершин, помеченных переменной x_i , не зависит от пути (для разных значений i это число может быть различным). Кроме того, при любом i , $1 \leq i \leq n$, на каждом пути от входной вершины к любой выходной число вершин, помеченных переменной x_i , равно k . Сложность реализации булевой функции f недетерминированными и детерминированными однородными ветвящимися k -программами будем обозначать через $\text{UNBPk}(f)$ и $\text{UBPk}(f)$ соответственно.

Пусть \mathcal{P} — однородная недетерминированная (детерминированная) k -программа. Будем считать, что вершина a программы \mathcal{P} находится на расстоянии l от входной вершины, если число помеченных дуг на любом пути от входной вершины до вершины a равно l . Через $\text{UNBP}^d(\mathcal{P})$ ($\text{UBP}^d(\mathcal{P})$) обозначим число вершин, помеченных переменными, однородной недетерминированной (детерминированной) ветвящейся программы \mathcal{P} , лежащих на расстоянии кратном d от входной вершины.

Рассмотрим ветвящуюся программу \mathcal{P} , реализующую булеву функцию f . Каждому пути π в программе \mathcal{P} , идущему от входной вершины к выходной, естественным образом можно поставить в соответствие конъюнкцию K : если на пути π есть дуга с меткой единица, выходящая из вершины, помеченной переменной x_i , то x_i включается в конъюнкцию K ; если в π есть дуга с меткой ноль, выходящая из вершины, помеченной x_i , то в K включается \bar{x}_i . При этом конъюнкции, соответствующие некоторым путям ветвящейся программы \mathcal{P} , могут содержать одновременно переменную и ее отрицание, т. е. могут быть тождественно равны нулю. Будем говорить, что путь π реализует конъюнкцию K . Ясно, что если конъюнкция K соответствует некоторому пути ветвящейся программы \mathcal{P}_f , то $K^{-1}(1) \subseteq f^{-1}(1)$.

Будем говорить, что вершина a_i *предшествует* вершине a_j в ветвящейся программе, если в ней существует путь от a_i к a_j .

Множество вершин a_1, \dots, a_i (не обязательно различных) ветвящейся программы \mathcal{P} назовем *последовательностью вершин*, если в \mathcal{P} существует такой путь от входной вершины к выходной, проходящий через вершины a_1, \dots, a_i , что на этом пути вершина a_i предшествует вершине a_j при $i < j$ или a_i совпадает с a_j .

§ 3. Сведение нижних оценок сложности для программ без ограничений к оценкам сложности для k -программ

Пусть $f(x_1, x_2, \dots, x_n)$ — булева функция, $X' = \{x_{i_1}, \dots, x_{i_m}\}$ — подмножество множества переменных функции f , а $\alpha = \{\alpha_{i_1}, \dots, \alpha_{i_m}\}$ — множество констант. Через $f|_{X'=\alpha}$ обозначим функцию, которая получается из f подстановкой констант из α вместо переменных из X' , а именно заменой переменной x_{i_j} на константу α_{i_j} , $1 \leq j \leq m$.

Следующая теорема показывает, что можно получать нижние оценки сложности реализации булевых функций ветвящимися программами без ограничений, используя ветвящиеся k -программы.

Теорема 1. Пусть $g(X)$ — булева функция и C — константа, $0 < C < 1$. Пусть для любого подмножества переменных X_0 , $X_0 \subseteq X$ и $|X_0| = \lfloor Cn \rfloor$, существует такая подстановка констант из α в X_0 , что сложность реализации функции $g|_{X_0=\alpha}(X \setminus X_0)$ недетерминированными (детерминированными) ветвящимися $k(n)$ -программами не менее чем $n\psi(n)$, где $\psi(n)$ — растущая функция. Тогда сложность реализации функции g недетерминированными (детерминированными) ветвящимися программами без ограничений не меньше $\min\{Cnk(n), n\psi(n)\}$.

Доказательство. Пусть \mathcal{P} — произвольная ветвящаяся программа, реализующая функцию g . Покажем, что ее сложность не меньше $\min\{Cnk(n), n\psi(n)\}$. Через X' обозначим множество переменных функции g , которыми в программе \mathcal{P} помечено не менее $k(n)$ вершин. Возможны 2 случая.

I. $|X'| > \lfloor Cn \rfloor$. В этом случае в программе \mathcal{P} содержится по крайней мере $\lfloor Cn \rfloor$ переменных, каждой из которых помечено не менее $k(n)$ вершин. Поэтому общее число вершин в программе \mathcal{P} не меньше $Cnk(n)$. Следовательно, сложность программы \mathcal{P} не меньше $\min\{Cnk(n), n\psi(n)\}$.

II. $|X'| \leq \lfloor Cn \rfloor$. Если $|X'| < \lfloor Cn \rfloor$, то множество X' произвольным образом дополним до множества X_0 мощности $\lfloor Cn \rfloor$. По условию теоремы существует такая подстановка констант из α в подмножество переменных из X_0 , что сложность реализации функции $g|_{X_0=\alpha}$ ветвящимися k -программами не меньше $n\psi(n)$, где $\psi(n)$ — растущая функция. В программе \mathcal{P} переменные из X_0 «забьем» константами из α . Произведя несложную перестройку программы \mathcal{P} , получим новую программу \mathcal{P}' , сложность которой не больше сложности программы \mathcal{P} . При этом программа \mathcal{P}' реализует функцию $g|_{X_0=\alpha}(X \setminus X_0)$. В программе \mathcal{P}' нет переменной, которой помечено более $k(n)$ вершин. А это значит, что в \mathcal{P}' нет пути, на котором встречается более $k(n)$ вершин, помеченных одной и той же переменной, т. е. \mathcal{P}' является ветвящейся $k(n)$ -программой. Следовательно, по условию теоремы ее сложность не

меньше $n\psi(n)$. Таким образом, и в этом случае сложность программы \mathcal{P} не меньше $\min\{Cnk(n), n\psi(n)\}$. Теорема доказана.

Таким образом, для получения нижних оценок сложности реализации функции g программами без ограничений надо научиться получать нижние оценки сложности реализаций подфункций функции g ветвящимися k -программами.

§ 4. Нижние оценки сложности ветвящихся k -программ

Для того чтобы оценить увеличение сложности функции g при переходе от ее реализации произвольной недетерминированной k -программой к реализации g однородной недетерминированной k -программой, надо оценить сверху общее число дуг (включая свободные дуги) в недетерминированной программе. Это будет осуществляться так же, как при доказательстве теоремы 1 из [7]; но там это утверждение было сформулировано для ациклических контактно-вентильных схем. Известно, что сложности реализации булевых функций ациклическими контактно-вентильными схемами и недетерминированными ветвящимися программами с точностью до порядка совпадают, тем не менее для удобства изложения это утверждение целесообразно сформулировать в терминах недетерминированных ветвящихся программ.

Лемма 1. Любую недетерминированную программу \mathcal{P} можно преобразовать в такую недетерминированную программу \mathcal{P}' , сложность которой не превосходит сложности программы \mathcal{P} и общее число дуг (включая свободные дуги) в \mathcal{P}' не превышает $16(\text{NBP}(\mathcal{P}))^2 - 2$.

Доказательство. Обозначим через a_0, a_1, \dots, a_L входную вершину и все вершины, из которых исходят дуги, помеченные 0 или 1. Ясно, что $L \leq 2\text{NBP}(\mathcal{P})$. Пусть a_j , $0 \leq j \leq L$, — недетерминированная вершина, из которой исходят пути по свободным дугам, ведущие в l вершин, помеченных переменными, или в выходные вершины ($l \leq \text{NBP}(\mathcal{P}) + 2$). Множество всех таких путей заменим ориентированным деревом с корнем a_j , содержащим не более $2(l - 1)$ свободных дуг; при этом выходные вершины этого дерева ведут в те же l вершин, что и пути, выходящие из вершины a_j в программе \mathcal{P} (рис. 1).

Такую замену произведем для всех недетерминированных вершин из множества $\{a_0, a_1, \dots, a_L\}$. Получим новую программу \mathcal{P}' , в которой число помеченных вершин не изменилось, а число свободных дуг не превышает $(2(\text{NBP}(\mathcal{P}) + 1))(2\text{NBP}(\mathcal{P}) + 1)$. Общее же число дуг в новой программе не превышает $2(\text{NBP}(\mathcal{P}) + 1)(2\text{NBP}(\mathcal{P}) + 1) + 2\text{NBP}(\mathcal{P}) \leq 16(\text{NBP}(\mathcal{P}))^2 - 2$. Лемма доказана.

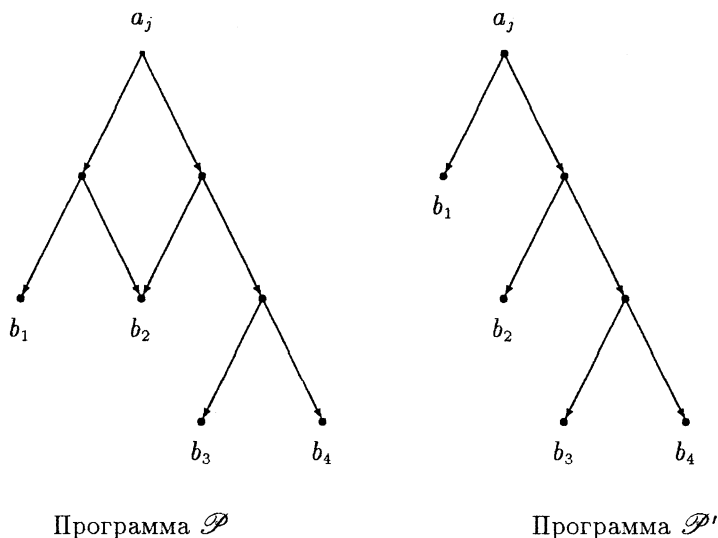


Рис. 1

Перейдем к преобразованию ветвящейся программы к однородной программе, что уже было сделано в [3, 9]. Но в отличие от [9], где нас не интересовали точные оценки, здесь мы будем оценивать соотношение не просто между сложностью ветвящейся программы и однородной ветвящейся программы, а между сложностью ветвящейся программы и числом вершин ветвящейся программы, которые находятся на таком расстоянии от входной вершины, которое кратно некоторой величине.

Лемма 2. а) Любую недетерминированную ветвящуюся k -программу \mathcal{P} , реализующую булеву функцию $f(x_1, \dots, x_n)$, можно преобразовать в такую однородную k -программу \mathcal{P}_0 , которая реализует функцию f и число вершин $\text{UNBP}^d(\mathcal{P}_0)$, лежащих на расстоянии кратно d от входной вершины, удовлетворяет неравенству

$$\text{UNBP}^d(\mathcal{P}_0) \leq \lceil kn/d \rceil (4\text{NBPk}(\mathcal{P}))^2.$$

б) Любую детерминированную ветвящуюся k -программу \mathcal{P} , реализующую булеву функцию $f(x_1, \dots, x_N)$, можно преобразовать в такую однородную k -программу \mathcal{P}_0 , реализующую функцию f , что

$$\text{UBP}^d(\mathcal{P}_0) \leq \lceil kn/d \rceil \cdot \text{BPk}(\mathcal{P}).$$

Доказательство проводится по аналогии с доказательством леммы 1 из [3, 4].

а) Пусть \mathcal{P} — недетерминированная ветвящаяся k -программа, реализующая булеву функцию $f(x_1, x_2, \dots, x_n)$. Лемма 1 утверждает, что

любую недетерминированную ветвящуюся k -программу \mathcal{P} можно преобразовать в недетерминированную ветвящуюся k -программу \mathcal{P}' с тем же числом помеченных вершин, в которой общее число дуг (включая свободные дуги) не превосходит $16\text{NBP}(\mathcal{P})^2 - 2$.

Максимальное число вершин с меткой x_q на произвольном пути от входной вершины к вершине a в программе \mathcal{P}' обозначим через $l_q(a)$. Ясно, что если вершина a_i предшествует вершине a_j в \mathcal{P}' , то при любом $q = 1, 2, \dots, n$ выполняется неравенство

$$l_q(a_i) \leq l_q(a_j).$$

Рассмотрим случай, когда дуга (a_i, a_j) выходит из вершины, помеченной переменной, и случай, когда дуга (a_i, a_j) выходит из недетерминированной вершины.

СЛУЧАЙ 1. Пусть дуга (a_i, a_j) в \mathcal{P}' выходит из помеченной вершины. Без ограничения общности можно считать, что эта дуга имеет метку 1 и выходит из вершины x_1 . Тогда $l_1(a_i) < l_1(a_j)$. Дугу (a_i, a_j) заменим на дугу (a_i, a') и на «цепочку» дуг, которые соединяют вершины a' и a_j и реализуют фиктивные проверки переменных x_1, x_2, \dots, x_n : $(l_1(a_j) - l_1(a_i) - 1)$ проверок переменной x_1 и $(l_q(a_j) - l_q(a_i))$, $2 \leq q \leq n$, проверок переменной x_q . Среди всех вершин, лежащих на пути от вершины a_i к вершине a_j после введения фиктивных проверок переменных, не более чем $\lceil kn/d \rceil$ вершин лежат на расстоянии кратном d от входной вершины (вершина a_j в рассмотрение не входит).

СЛУЧАЙ 2. Пусть (a_i, a_j) — свободная дуга в \mathcal{P}' . Если $l_q(a_j) = l_q(a_i)$ при каждом q , $1 \leq q \leq n$, то вершины a_i и a_j соединим свободной дугой (a_i, a_j) . Если имеется q , $1 \leq q \leq n$, такое, что $l_q(a_j) \neq l_q(a_i)$, то дугу (a_i, a_j) заменим на путь, соединяющий вершины a_i и a_j , дуги которого реализуют фиктивные проверки переменных x_1, x_2, \dots, x_n ; при этом используется $(l_q(a_j) - l_q(a_i))$, $1 \leq q \leq n$, проверок переменной x_q . Среди всех вершин, лежащих на пути от вершины a_i к вершине a_j после введения фиктивных проверок переменных, не более чем $\lceil kn/d \rceil$ вершин лежат на расстоянии кратном d от входной вершины (вершина a_j в рассмотрение не входит).

Проведем эту процедуру со всеми дугами в \mathcal{P}' . Для того чтобы на любом пути от входной вершины к выходной вершине было k дуг, помеченных произвольной переменной, введем новую выходную вершину и соединим прежнюю и новую выходную вершины путем, который реализует необходимое число фиктивных проверок переменных. В результате получим такую однородную ветвящуюся k -программу, что

$$\text{UNBP}^q(\mathcal{P}_0) \leq \lceil kn/q \rceil (4\text{NBP}(\mathcal{P}))^2.$$

б) В детерминированной программе нет свободных дуг, и поэтому не требуется производить преобразование программы, указанное в лемме 1. Следовательно, для нее справедлива оценка из пункта б) леммы. Лемма доказана.

Пусть \mathcal{P}_0 — однородная k -программа, реализующая булеву функцию $f(X)$. Тогда любой путь в \mathcal{P}_0 реализует либо некоторую элементарную конъюнкцию от переменных из X , либо тождественно равную нулю конъюнкцию. Пусть π — путь в \mathcal{P}_0 , реализующий ненулевую конъюнкцию K . Будем говорить, что *переменная x встречается на отрезке (b, c) пути π* , если на отрезке (b, c) пути π между вершинами b и c есть дуга, которая исходит из вершины ветвящейся программы, помеченной переменной x .

Пусть a_1, a_2, \dots, a_{2m} — последовательность вершин однородной k -программы \mathcal{P}_0 , лежащих на пути π . Введем следующие обозначения.

- $Q_\pi^1(a_1, a_2, \dots, a_{2m})$ — множество переменных, каждая из которых встречается хотя бы на одном из отрезков $(a_1, a_2), \dots, (a_{2m-1}, a_{2m})$ пути π и не встречается вне этих отрезков на этом пути.
- $Q_\pi^2(a_1, a_2, \dots, a_{2m})$ — множество переменных, которые встречаются только вне указанных выше отрезков пути π .
- $Q_\pi^0(a_1, a_2, \dots, a_{2m})$ — множество переменных, которые встречаются как на указанных выше отрезках пути π , так и вне их.

Если \mathcal{P}_0 — однородная k -программа, то в ней на любом пути, проходящем через вершины b и c , множество переменных, которые встречаются на отрезке (b, c) этого пути, не зависит от пути. Поэтому множества $Q_\pi^j(a_1, a_2, \dots, a_{2m})$ ($j = 0, 1, 2$) зависят только от последовательности вершин a_1, a_2, \dots, a_{2m} и не зависят от пути. Следовательно, индекс π при Q_π^j можно опустить. Ясно, что множества $Q^j(a_1, a_2, \dots, a_{2m})$ ($j = 0, 1, 2$) попарно не пересекаются и их объединение совпадает с множеством всех переменных реализуемой функции.

Пусть k, p и t — натуральные числа такие, что $k \leq p \leq t$. Введем следующие обозначения:

$$n_1(n; k, p, t) = \left\lceil n \binom{t-k}{p-k} / \binom{t}{p} \right\rceil; \quad (2)$$

$$n_2(n; k, p, t) = n - p \lceil kn/t \rceil + (k-1) \left\lceil n \binom{t-k}{p-k} / \binom{t}{p} \right\rceil; \quad (3)$$

$$n_0(n; k, p, t) = n - n_1 - n_2. \quad (4)$$

В следующей лемме приведены некоторые оценки величин $n_1(n; k, p, t)$ и $n_2(n; k, p, t)$, зависящие от параметров p и t .

Лемма 3.

1. Если $p = k$ и $t = k^2 + k$, то $n_1(n; k, p, t) \geq \frac{n}{2(ke)^k}$ и $n_2(n; k, p, t) \geq \frac{n}{k+1}$.
2. Если $p = k$ и $t = 2k^2$, то $n_1(n; k, p, t) \geq \frac{2n}{(2ke)^k}$ и $n_2(n; k, p, t) \geq \frac{n}{2}$.

Доказательство. Из формулы Стирлинга следует, что при любых b и a , $1 \leq a \leq b/2$, выполняется неравенство

$$\binom{b}{a} \leq \frac{1}{2} \left(\frac{be}{a} \right)^a. \quad (5)$$

1. Пусть $p = k$ и $t = k^2 + k$. Тогда $n_1 = \left\lceil n / \binom{k^2+k}{k} \right\rceil$ и $n_2 \geq n - k \left\lceil \frac{nk}{k^2+k} \right\rceil$.

Из (5) следует, что $n_1 \geq \frac{2n}{((k+1)e)^k} \geq \frac{2n}{k^k e^{k+1}} \geq \frac{n}{2(ke)^k}$ и $n_2 \geq \frac{n}{k+1}$.

2. Пусть $p = k$ и $t = 2k^2$. Тогда $n_1 = n / \binom{2k^2}{k}$ и $n_2 \geq n - k \lceil nk / (2k^2) \rceil$.

Из (5) следует, что $n_1 \geq \frac{2n}{(2ke)^k}$ и $n_2 \geq \frac{n}{2}$.

Лемма доказана.

Теорема 2. Пусть \mathcal{P}_0 — однородная недетерминированная k -программа, реализующая функцию f , натуральные числа k , p и t таковы, что $k \leq p \leq t$, и числа $n_1(n; k, p, t)$, $n_2(n; k, p, t)$, $n_0(n; k, p, t)$ положительны. Тогда любому набору $\gamma = (\gamma_1, \dots, \gamma_n)$ такому, что $f(\gamma) = 1$, можно поставить в соответствие такую последовательность $\Psi(\gamma)$ из $2p'$, $p' \leq p$, различных вершин, помеченных переменными, что

(а) все вершины последовательности $\Psi(\gamma)$ принадлежат некоторому пути $\pi(\gamma)$, реализующему γ ;

(б) все вершины последовательности $\Psi(\gamma)$ лежат на расстоянии кратном $\lceil kn/t \rceil$ от входной вершины;

(с) $|Q^1(\Psi(\gamma))| \geq n_1(n; k, p, t)$;

$|Q^2(\Psi(\gamma))| \geq n_2(n; k, p, t)$;

$|Q^0(\Psi(\gamma))| \leq n_0(n; k, p, t)$.

Доказательство практически совпадает с доказательством леммы 2 из [3]. Наличие свободных дуг лишь незначительно изменяет доказательство.

В однородной программе \mathcal{P}_0 имеется путь $\pi(\gamma)$ длины kn , который реализует единицу γ булевой функции f . На пути $\pi(\gamma)$ выберем вершины a_0, a_1, \dots, a_t , где a_0 — первая вершина, помеченная переменной на пути π (т.е. вершина, лежащая на расстоянии 0 от входной вершины); a_1 — вершина, помеченная переменной и лежащая на расстоянии $\lceil kn/t \rceil$ от входной вершины; a_2 — вершина, помеченная переменной и лежащая на расстоянии $2 \cdot \lceil kn/t \rceil$ от входной вершины, и так далее до тех пор, пока не появится выходная вершина, помеченная единицей. Выходную вершину выберем в качестве очередной s -й вершины пути. При этом расстояние между вершиной, предшествующей выходной вершине, и выходной вершиной может быть меньше $\lceil kn/t \rceil$. Если $s < t + 1$, то в качестве вершин

a_{s+1}, \dots, a_{t+1} возьмем выходную вершину, помеченную единицей. Ясно, что при этом вершины выбранной последовательности (за исключением вершин, совпадающих с выходной вершиной) помечены переменными и лежат на расстоянии кратном $\lceil kn/t \rceil$ от входной вершины.

Любые p вершин a_{i_1}, \dots, a_{i_p} , $0 \leq i_1 < i_2 < \dots < i_p \leq t-1$, из множества $\{a_0, a_1, \dots, a_{t-1}\}$ задают p отрезков пути $\pi(\gamma)$: $(a_{i_1}, a_{i_1+1}), (a_{i_2}, a_{i_2+1}), \dots, (a_{i_p}, a_{i_p+1})$. Множество концов этих отрезков обозначим через A_{i_1, i_2, \dots, i_p} , т. е. $A_{i_1, i_2, \dots, i_p} = \{a_{i_1}, a_{i_1+1}, a_{i_2}, a_{i_2+1}, \dots, a_{i_p}, a_{i_p+1}\}$ является последовательностью вершин ветвящейся программы \mathcal{P}_0 .

В конце доказательства теоремы будет показано, что среди всевозможных последовательностей A_{i_1, i_2, \dots, i_p} можно выбрать такую, что ее незначительная модификация (последовательность B) удовлетворяет условиям теоремы.

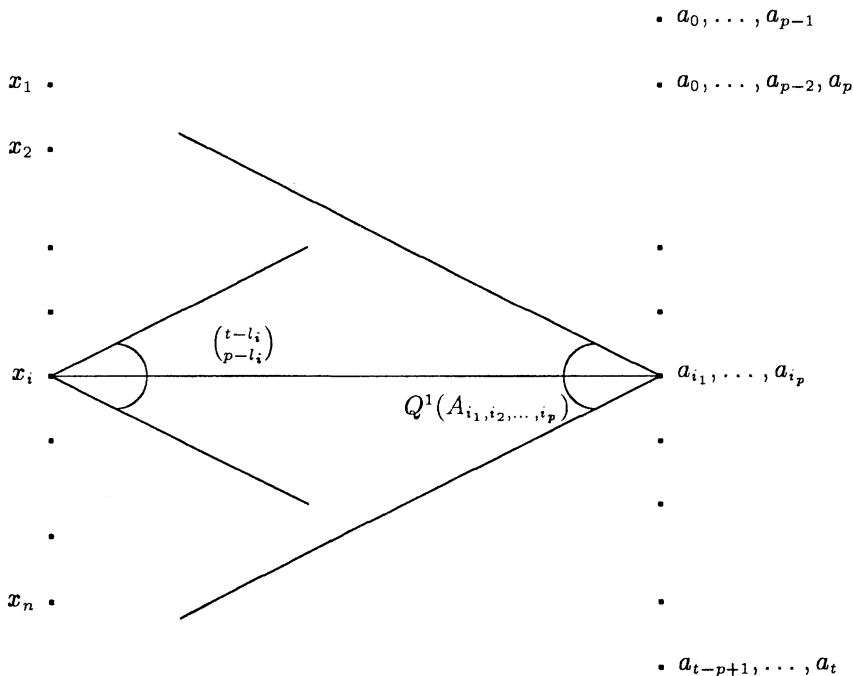


Рис. 2

Рассмотрим неориентированный граф G (рис. 2), содержащий два множества вершин: n вершин, соответствующих переменным x_1, \dots, x_n , и $\binom{t}{p}$ вершин, соответствующих всевозможным p -элементным выборкам $\{a_{i_1}, \dots, a_{i_p}\}$ из множества $\{a_0, a_1, \dots, a_{t-1}\}$, а значит, и всевозможным последовательностям A_{i_1, i_2, \dots, i_p} . Вершину, соответствующую

переменной x_i , соединим с вершиной, соответствующей подмножеству $\{a_{i_1}, a_{i_2}, \dots, a_{i_p}\}$, $0 \leq i_1 < i_2 < \dots < i_p \leq (t-1)$, в том и только том случае, когда $x_{(i-1)s+1, \dots, is} \in Q^1(A_{i_1, i_2, \dots, i_p})$, т. е. когда эта переменная входит хотя бы в один из отрезков пути $(a_{i_1}, a_{i_1+1}), (a_{i_2}, a_{i_2+1}), \dots, (a_{i_p}, a_{i_p+1})$, но не входит в остальные отрезки пути. Пусть l_i — число отрезков (a_{i_j}, a_{i_j+1}) , $0 \leq j \leq (t-1)$, в которые входит переменная x_i . Тогда вершина, соответствующая переменной x_i , соединена в графе G со всеми подмножествами, содержащими эти отрезки. Число таких подмножеств равно $\binom{t-l_i}{p-l_i}$. С другой стороны, вершина, соответствующая подмножеству $\{a_{i_1}, \dots, a_{i_p}\}$, соединена в графе G с $|Q^1(A_{i_1, i_2, \dots, i_p})|$ вершинами, которые соответствуют переменным. Подсчитав число ребер в графе, получаем, что

$$\sum_{\substack{i_1, \dots, i_p \\ 0 \leq i_1 < \dots < i_p \leq (t-1)}} |Q^1(A_{i_1, i_2, \dots, i_p})| = \sum_{i=1}^n \binom{t-l_i}{p-l_i}. \quad (6)$$

Так как на каждом пути ветвящейся программы \mathcal{P}_0 любая переменная встречается k раз, то $l_i \leq k$. Поэтому выполняется неравенство

$$\binom{t-l_i}{p-l_i} \geq \binom{t-k}{p-k}.$$

Из этого неравенства и (6) следует, что

$$\sum_{\substack{i_1, \dots, i_p \\ 0 \leq i_1 < \dots < i_p \leq (t-1)}} |Q^1(A_{i_1, i_2, \dots, i_p})| \geq n \binom{t-k}{m-k}. \quad (7)$$

Выберем подмножество вершин A_{i_1, i_2, \dots, i_p} с максимальным значением $|Q^1(A_{i_1, i_2, \dots, i_p})|$. Можно считать, что в это подмножество не входит выходная вершина, так как вклад отрезков, начинающихся с выходной вершины, в левую часть из (7) равен 0. Поэтому эти вершины можно заменить любыми другими, отличными от выходной вершины; при этом значение $|Q^1(A_{i_1, i_2, \dots, i_p})|$ не уменьшится. Значит, имеется такое множество вершин a_{i_1}, \dots, a_{i_p} , не содержащее выходной вершины, что справедливо неравенство

$$|Q^1(A_{i_1, i_2, \dots, i_p})| \geq n \binom{t-k}{p-k} / \binom{t}{p}.$$

Так как $|Q^1(A_{i_1, i_2, \dots, i_p})|$ целое число, то

$$|Q^1(A_{i_1, i_2, \dots, i_p})| \geq \left\lceil n \binom{t-k}{p-k} / \binom{t}{p} \right\rceil. \quad (8)$$

Общее число переменных, входящих в отрезки $(a_1, a_2), (a_3, a_4), \dots, (a_{2p-1}, a_{2p})$, удовлетворяет неравенству

$$|Q^1(A_{i_1, i_2, \dots, i_m}) \cup Q^0(A_{i_1, i_2, \dots, i_m})| \leq [kn/t]p - (k-1)|Q^1(A_{i_1, i_2, \dots, i_m})|. \quad (9)$$

Поскольку

$$|Q^2(A)| = n - |Q^1(A) \cup Q^0(A)|,$$

из (8) и (9) получаем

$$\begin{aligned} |Q^2(A_{i_1, i_2, \dots, i_m})| &\geq n - [kn/t]p + (k-1)|Q^1(A_{i_1, i_2, \dots, i_m})| \\ &\geq n - [kn/t]p + (k-1) \left[n \binom{t-k}{p-k} / \binom{t}{p} \right]. \end{aligned} \quad (10)$$

Так как

$$|Q^0(A_{i_1, i_2, \dots, i_m})| + |Q^1(A_{i_1, i_2, \dots, i_m})| + |Q^2(A_{i_1, i_2, \dots, i_m})| = n, \quad (11)$$

то требуемая оценка справедлива и для $|Q^0(A_{i_1, i_2, \dots, i_m})|$.

Ясно, что все вершины последовательности A_{i_1, i_2, \dots, i_p} лежат на расстоянии, кратном $[kn/t]$. Если в последовательность A_{i_1, i_2, \dots, i_p} какие-нибудь вершины входят более одного раза, то можно объединить отрезки, содержащие общие вершины, выбросив эти вершины. Например, если $i_3 = i_2 + 1$, то в последовательности A_{i_1, i_2, \dots, i_p} вершина a_{i_3} встречается два раза. Поэтому можно рассмотреть последовательность, содержащую концы отрезков $(a_{i_1}, a_{i_1+1}), (a_{i_2}, a_{i_3+1}), \dots, (a_{i_p}, a_{i_p+1})$. Прделав эту процедуру со всеми совпадающими концами отрезков, от последовательности A_{i_1, i_2, \dots, i_p} перейдем к последовательности B , состоящей из $2p'$ вершин, $p' \leq p$. Легко видеть, что последовательность B удовлетворяет условиям (а) и (б) теоремы. Также легко видеть, что при $j = 0, 1, 2$

$$Q^j(A_{i_1, i_2, \dots, i_p}) = Q^j(B).$$

Тогда из (2)–(4), (8), (10) и (11) следует, что последовательность B удовлетворяет условию (с) теоремы. Теорема доказана.

Пусть \mathcal{P} — ветвящаяся программа, реализующая булеву функцию f , a и b — вершины программы \mathcal{P} . Через $f(\mathcal{P}; a, b)$ обозначим булеву функцию, реализуемую подпрограммой программы \mathcal{P} , в которой вершина a рассматривается как входная вершина, а вершина b — как выходная вершина, помеченная 1. (Для того чтобы полученная подпрограмма была ветвящейся программой, вершину b надо пометить единицей и удалить из нее дуги программы, выходящие из вершины b .) Пусть $\Psi = (a_1, a_1, \dots, a_{2p'})$ — последовательность вершин ветвящейся программы \mathcal{P} , реализующей булеву функцию $f(x_1, \dots, x_n)$. Через a_0

обозначим входную вершину программы \mathcal{P} , через $a_{2p'+1}$ — выходную вершину, помеченную 1. Положим

$$f^1(\mathcal{P}; \Psi) = \bigwedge_{j=1}^{p'} f(\mathcal{P}; a_{2j-1}, a_{2j}), \quad f^2(\mathcal{P}; \Psi) = \bigwedge_{j=0}^{p'} f(\mathcal{P}; a_{2j}, a_{2j+1}).$$

Из определения множеств $Q^j(\Psi)$, $j = 0, 1, 2$, следует, что функция $f^1(\mathcal{P}; \Psi)$ зависит только от переменных из множеств $Q^1(\Psi)$ и $Q^0(\Psi)$, а функция $f^2(\mathcal{P}; \Psi)$ — от переменных из множеств $Q^2(\Psi)$ и $Q^0(\Psi)$.

Ясно, что если $f(\gamma) = 1$, то

$$f^1(\mathcal{P}; \Psi(\gamma))(\gamma) \wedge f^2(\mathcal{P}; \Psi(\gamma))(\gamma) = 1.$$

Пусть \mathcal{P}_0 — однородная недетерминированная k -программа, реализующая функцию f ; k , p и t — натуральные числа такие, что $k \leq p \leq t$, и числа $n_1(n; k, p, t)$, $n_2(n; k, p, t)$, $n_0(n; k, p, t)$ положительны. В теореме 2 каждой единице γ булевой функции f была поставлена в соответствие такая последовательность $\Psi(\gamma)$ из $2p'$ вершин (p' — натуральное число и $p' \leq p$), лежащих на расстоянии кратном $\lceil kn/t \rceil$ от входной вершины, что $|Q^1(\Psi(\gamma))| \geq n_1(n; k, p, t)$; $|Q^2(\Psi(\gamma))| \geq n_2(n; k, p, t)$; $|Q^0(\Psi(\gamma))| \leq n_0(n; k, p, t)$.

Через $V(\mathcal{P})$ обозначим множество $2p'$ -вершинных последовательностей однородной ветвящейся программы \mathcal{P} , которые поставлены в соответствие единицам булевой функции f , реализуемой программой \mathcal{P} .

Очевидна следующая

Лемма 4. Булева функция f , реализуемая программой \mathcal{P}_0 , может быть представлена в виде

$$f = \bigvee_{j=1}^{|V(\mathcal{P}_0)|} (f_j^1(Q^0(\Psi^j) \cup Q^1(\Psi^j)) \wedge f_j^2(Q^0(\Psi^j) \cup Q^2(\Psi^j))).$$

Рассмотрим всевозможные представления функции $f(Y)$, $|Y| = n$, в виде

$$f(Y) = \bigvee f^1(Y_1 \cup Y_0) \wedge f^2(Y_2 \cup Y_0), \quad (12)$$

где Y_1 , Y_2 и Y_0 — непересекающиеся множества; $Y = Y_1 \cup Y_2 \cup Y_0$; $|Y| = n$, $|Y_1| \geq n_1(n; k, p, t)$, $|Y_2| \geq n_2(n; k, p, t)$ и $|Y_0| = n - |Y_1| - |Y_2|$.

Минимальное число дизъюнктивных членов в представлении (12) обозначим через $R(f; n, k, p, t)$. Ясно, что

$$R(f; n, k, p, t) \leq |V(\mathcal{P}_0)| \quad (13)$$

для любой однородной k -программы \mathcal{P}_0 , реализующей функцию f .

Теорема 3. Пусть f — булева функция, существенно зависящая от n переменных, $n \geq 16$; k, p и t , $k \leq p \leq t$, — произвольные натуральные числа такие, что величины $n_1(n; p, k, t)$, $n_2(n; p, k, t)$ и $n_0(n; p, k, t)$, вычисленные по формулам (2)–(4), положительны. Тогда

(а) сложность $\text{NBPK}(f)$ реализации булевой функции f недетерминированными k -программами удовлетворяет неравенству

$$\text{NBPK}(f) \geq \max \left\{ n; \frac{1}{4} \sqrt{\frac{2p}{et}} \cdot (R(f; n, k, p, t))^{1/(4p)} \right\};$$

(б) сложность $\text{BPK}(f)$ реализации булевой функции f детерминированными k -программами удовлетворяет неравенству

$$\text{BPK}(f) \geq \max \left\{ n; \frac{2p}{et} \cdot (R(f; n, k, p, t))^{1/(2p)} \right\}.$$

Доказательство. Пусть \mathcal{P} — произвольная недетерминированная k -программа, реализующая булеву функцию f , существенно зависящую от n переменных. По лемме 2 преобразуем k -программу \mathcal{P} в однородную недетерминированную k -программу \mathcal{P}_0 , реализующую функцию f . Через L_0 обозначим множество всех вершин программы \mathcal{P}_0 , лежащих на расстоянии кратном $\lceil kn/t \rceil$ от входной вершины.

Все вершины последовательностей, поставленных по теореме 2 в соответствие единицам булевой функции, лежат на расстоянии кратном $\lceil kn/t \rceil$ от входной вершины и, следовательно, принадлежат множеству L_0 . Поэтому выполняется соотношение

$$|V(\mathcal{P}_0)| \leq \sum_{j=1}^p \binom{|L_0|}{2j}. \quad (14)$$

Так как функция f существенно зависит от n переменных, то $\text{NBPK}(f) \geq n$ и $\text{BPK}(f) \geq n$. Поэтому достаточно рассмотреть только случай, когда $R(f; n, k, p, t)^{1/2p} \geq n$, т. е.

$$R(f; n, k, p, t) \geq n^{2p} = 2^{2p \log_2 n} \geq 2^{8p}, \quad (15)$$

поскольку по условию теоремы $n \geq 16$.

Покажем, что в этом случае $|L_0| \geq 8p$. Предположим, что $|L_0| < 8p$. Тогда в силу (13) и (14) имеем

$$R(f; n, k, p, t) \leq |V(\mathcal{P}_0)| \leq \sum_{j=1}^p \binom{|L_0|}{2j} < 2^{|L_0|} \leq 2^{8p}.$$

Это противоречит предположению (15).

Таким образом, $|L_0| \geq 8p$. Отсюда и из (13)–(15) следует, что

$$R(f; n, k, p, t) \leq |V(\mathcal{P}_0)| \leq \sum_{j=1}^p \binom{|L_0|}{2j} \leq 2 \binom{|L_0|}{2p} \leq \left(\frac{e|L_0|}{2p} \right)^{2p}.$$

Поэтому

$$|L_0| \geq \frac{2p}{e} (R(f; n, k, p, t))^{1/(2p)}. \quad (16)$$

Но по определению множества L_0 и величины $\text{UNBP}_k^{\lceil kn/t \rceil}(\mathcal{P}_0)$ имеем

$$|L_0| = \text{UNBP}_k^{\lceil kn/t \rceil}(\mathcal{P}_0).$$

Тогда по лемме 2

$$|L_0| \leq \left\lceil \frac{kn}{\lceil kn/t \rceil} \right\rceil (4\text{NBP}_k(\mathcal{P}))^2 \leq t(4\text{NBP}_k(\mathcal{P}))^2.$$

Из этого факта и (16) следует, что

$$\text{NBP}_k(\mathcal{P}) \geq \frac{1}{4} \sqrt{\frac{2p}{et}} (R(f; n, k, p, t))^{1/(4p)}.$$

Так как \mathcal{P} — произвольная программа, реализующая булеву функцию f , то из полученного неравенства следует утверждение (а) теоремы. Утверждение (б) теоремы доказывается аналогично.

Из теорем 1 и 3 следует

Теорема 4. Пусть заданы последовательность булевых функций $g_n(X_n)$, $|X_n| = n$, растущая функция $k(n)$ и константа C , $0 < C < 1$. Пусть для любого множества переменных X , $X \subseteq X_n$ и $|X| = \lfloor Cn \rfloor$ существует подстановка констант из α вместо переменных из X , целочисленные $p(X)$ и $t(X)$ такие, что $k(n) \leq p(X) \leq t(X)$, и величины n_1 , n_2 и n_0 , вычисленные по формулам (2)–(4) как функции от $|X_n \setminus X|$, $k(n)$, $p(X)$ и $t(X)$, положительны. Тогда

(а) сложность $\text{NBP}(g_n)$ реализации функции $g_n(X_n)$ недетерминированными ветвящимися программами (без ограничений) удовлетворяет неравенству

$$\text{NBP}(g_n) \geq \min \left\{ Cnk(n), \frac{1}{4} \cdot \sqrt{2p/(et)} \cdot (R(g_n|_{X=\alpha}; |X_n \setminus X|, k, p, t))^{1/(4p)} \right\};$$

(б) ([8], теорема 3) сложность $\text{BP}(g_n)$ реализации функции $g_n(X_n)$ детерминированными ветвящимися программами (без ограничений) удовлетворяет неравенству

$$\text{BP}(g_n) \geq \min \left\{ Cnk(n), \frac{2p}{et} \cdot (R(g_n|_{X=\alpha}; |X_n \setminus X_0|, k, p, t))^{1/(2p)} \right\}.$$

Можно предложить несколько способов получения нижней оценки для $R(f; n, k, p, t)$ (см. [3]). В данной работе воспользуемся следующей оценкой.

Среди всех i -мерных граней куба размерности n выделим грань, в которой содержится максимальное число единиц функции f . Число единиц в такой грани обозначим через $H_i(f)$.

Лемма 5. Величина $R(f; n, k, p, t)$ удовлетворяет неравенству

$$R(f; n, k, p, t) \geq \frac{|f^{-1}(1)|}{2^{n_0} H_{n_1}(f) H_{n_2}(f)},$$

где $n_1 = n_1(n; k, p, t)$, $n_2 = n_2(n; k, p, t)$ и $n_0 = n_0(n; k, p, t)$.

Доказательство. Утверждение леммы следует из того, что каждый дизъюнктивный член в представлении (12) реализует не более $2^{n_0} h_{n_1}(f) h_{n_2}(f)$ единиц функции f .

Из леммы 5 и теоремы 4 следует

Теорема 5. Пусть заданы последовательность булевых функций $g_n(X_n)$, $|X_n| = n$, константа C , $0 < C < 1$, растущая функция $k(n)$ и целочисленные функции $p(n)$, $t(n)$ такие, что $k(n) \leq p(n) \leq t(n)$, и величины n_1 , n_2 и n_0 , вычисленные по формулам (2)–(4) как функции от $\lceil (1 - C)n \rceil$, $k(n)$, $p(n)$ и $t(n)$, положительны. Тогда

(а) сложность $\text{NBP}(g_n)$ реализации функции g_n недетерминированными ветвящимися программами без ограничений удовлетворяет неравенству

$$\text{NBP}(g_n) \geq \min \left\{ Cnk(n), \frac{1}{4} \sqrt{\frac{2p}{et}} \cdot \left(\frac{|g^{-1}(1)|}{2^{n-n_1-n_2} H_{n_1}(g) H_{n_2}(g)} \right)^{1/(4p)} \right\};$$

(б) сложность $\text{BP}(g_n)$ реализации функции g_n детерминированными ветвящимися программами без ограничений удовлетворяет неравенству

$$\text{BP}(g) \geq \min \left\{ Cnk(n), \frac{2p}{et} \cdot \left(\frac{|g^{-1}(1)|}{2^{n-n_1-n_2} H_{n_1}(g) H_{n_2}(g)} \right)^{1/(2p)} \right\}.$$

Доказательство. Пусть X_0 — произвольное n -элементное подмножество множества X_n , $|X_0| = \lfloor Cn \rfloor$. Зафиксируем переменные из X_0 таким образом, чтобы для функции $g|_{X_0=\alpha}$ выполнялось неравенство

$$\left| (g|_{X_0=\alpha})^{-1}(1) \right| \geq \frac{|(g)^{-1}(1)|}{2^{|X_0|}}.$$

Отсюда и из леммы 5 следует, что

$$\begin{aligned}
 R(g|_{X_0=\alpha}; [(1-C)n], k, p, t) &\geq \frac{|(g|_{X_0=\alpha})^{-1}(1)|}{2^{n_0} H_{n_1}(g|_{X_0=\alpha}) \cdot H_{n_2}(g|_{X_0=\alpha})} \\
 &\geq \frac{|g^{-1}(1)|}{2^{|X_0|+n_0} H_{n_1}(g|_{X_0=\alpha}) \cdot H_{n_2}(g|_{X_0=\alpha})} \\
 &\geq \frac{|g^{-1}(1)|}{2^{[Cn]+[(1-C)n]-n_1-n_2} H_{n_1}(g) \cdot H_{n_2}(g)} \\
 &\geq \frac{|g^{-1}(1)|}{2^{n-n_1-n_2} H_{n_1}(g) \cdot H_{n_2}(g)}.
 \end{aligned}$$

Из этого неравенства и теоремы 4 следует утверждение теоремы.

§ 5. Подсчет числа единиц в гранях куба для кодов Рида—Маллера

В работе [13] введено понятие обобщенного веса Хемминга и весовой иерархии для линейного кода. Пусть C — линейный $[n, k]$ код (т. е. код длины n , содержащий 2^k кодовых слов) и D — его подкод. Носителем D , обозначаемым через $\chi(D)$, является множество тех позиций в кодовых словах, в каждой из которых хотя бы одно кодовое слово подкода D не равно 0, т. е.

$$\chi(C) = \{i \mid \exists (x_1, x_2, \dots, x_n) \in C, x_i \neq 0\}.$$

В этих терминах линейный $[n, k]$ -код есть бинарный линейный код ранга k и размером носителя не больше n .

Одномерный подкод D кода C состоит из двух кодовых слов: нулевого слова и ненулевого кодового слова. Носитель D равен весу Хемминга ненулевого слова. Под r -м обобщенным весом Хемминга кода C , обозначаемым через $d_r(C)$, понимается размер минимального носителя подкода ранга r кода C , т. е.

$$d_r(C) = \min\{|\chi(D)| \mid D \text{ — подкод ранга } r \text{ кода } C\}.$$

Легко видеть, что $d_1(C)$ равен обычному минимальному весу Хемминга кода C . Под весовой иерархией линейного кода C понимается множество $\{d_1(C), \dots, d_k(C)\}$.

Интерес к обобщенным весам Хемминга в [13] вызван возможностью применения этого понятия в криптографии. Другим приложением обобщенных весов Хемминга являются так называемые t -резистантные функции.

В данной работе интерес к обобщенным весам Хемминга вызван тем, что они позволяют оценить максимальное число кодовых вершин, содержащихся в гранях куба определенной размерности, включающих нулевую вершину.

Лемма 6. В любой $d_r(C)$ -мерной грани куба, содержащей нулевую вершину, имеется не более 2^r кодовых вершин линейного кода.

Доказательство. Предположим, что в $d_r(C)$ -мерной грани куба, содержащей нулевую вершину, содержится более 2^r кодовых вершин, т. е. по крайней мере 2^{r+1} кодовых вершин. Это значит, что в $d_r(C)$ -мерную грань куба, содержащую нулевую вершину, можно вложить подкод с 2^{r+1} кодовыми вершинами, т. е.

$$d_{r+1}(C) \leq d_r(C). \quad (17)$$

Но, как показано в [13, теорема 1], имеет место монотонность, а именно

$$1 \leq d_1(C) < d_2(C) < \dots < d_k(C) \leq n.$$

Следовательно, неравенство (17) неверно. Таким образом, в любом подкоде размерности $d_r(C)$ содержится не более 2^r кодовых вершин. Лемма доказана.

Эта лемма показывает, что для оценки сверху числа кодовых вершин в гранях куба, содержащих нулевую вершину, достаточно знать обобщенные кодовые веса.

Кроме того, в [13] исследовалась иерархия обобщенных весов Хемминга для кодов Рида—Маллера. Для этих кодов будем использовать обозначения из [1, 13]. Код Рида—Маллера $\mathcal{R}(u, m)$ рассматривается как линейное пространство, задаваемое булевыми полиномами степени не выше u от m переменных v_1, v_2, \dots, v_m . Известно, что число кодовых вершин в коде $\mathcal{R}(u, m)$ равно

$$2^{1+\binom{m}{1}+\binom{m}{2}+\dots+\binom{m}{u}}, \quad (18)$$

длина кодовых слов

$$n = 2^m; \quad (19)$$

минимальное расстояние

$$d = 2^{m-u}.$$

Можно перечислить все мономы от переменных v_1, \dots, v_m в антилексикографическом порядке: $v_m \succ v_{m-1} \succ \dots \succ v_1 \succ \Lambda$ (пустая строка). Например, если $c \succ b \succ a \succ \Lambda$, то $\{cba, cb, ca, c, ba, b, a, \Lambda\}$ — перечисление мономов в антилексикографическом порядке. Как указано в [13], такое перечисление не эквивалентно обратному к лексикографическому порядку. В самом деле, в данном примере $\{\Lambda, a, ab, abc, ac, b, bc, c\}$ — перечисление в лексикографическом порядке. Обратное к нему не является антилексикографическим порядком.

Полная весовая иерархия кодов Рида—Маллера описывается в [13] в терминах антилексикографического порядка.

Теорема 6 ([13, теорема 7]). Подкод кода $R(u, m)$, натянутый на первые r мономов степени не более u , упорядоченных в антилексикографическом порядке, имеет носитель размера $d_r(R(u, m))$.

В качестве примера, как и в [13], рассмотрим код $R(2, 5)$. Этот код имеет базис $\{v_5 v_4, v_5 v_3, v_5 v_2, v_5 v_1, v_5, v_4 v_3, v_4 v_2, v_4 v_1, v_4, v_3 v_2, v_3 v_1, v_3, v_2 v_1, v_2, v_1, 1\}$, упорядоченный в антилексикографическом порядке. Весовая иерархия этого кода есть $\{8, 12, 14, 15, 16, 20, 22, 23, 24, 26, 27, 28, 29, 30, 31, 32\}$.

Для получения нижних оценок сложности не обязательно знать полную иерархию весов кода Рида—Маллера, можно ограничиться получением точных значений лишь некоторых величин $d_r(C)$.

Теорема 7. Пусть натуральное число φ не превосходит m . Тогда в любой $2^m/2^\varphi$ -мерной грани куба содержится не более $2^{\binom{m-\varphi}{0} + \binom{m-\varphi}{1} + \dots + \binom{m-\varphi}{u-\varphi}}$ кодовых вершин кода $\mathcal{R}(u, m)$.

Доказательство. Рассмотрим первые $2^{\binom{m-\varphi}{0} + \binom{m-\varphi}{1} + \dots + \binom{m-\varphi}{u-\varphi}}$ мономов в антилексикографическом порядке. Все такие мономы и только они в качестве множителя содержат моном $v_m \dots v_{m-\varphi+1}$. Поэтому носитель всех этих мономов содержится в носителе вектора $v_m \dots v_{m-\varphi+1}$, т. е. равен $2^m/2^\varphi$. Таким образом, в $2^m/2^\varphi$ -мерной грани куба, содержащей нулевую вершину, имеется не более $2^{\binom{m-\varphi}{0} + \binom{m-\varphi}{1} + \dots + \binom{m-\varphi}{u-\varphi}}$ кодовых вершин.

Так как код Рида—Маллера линейный, то из этого утверждения следует, что любая грань куба содержит не более чем $2^{\binom{m-\varphi}{0} + \binom{m-\varphi}{1} + \dots + \binom{m-\varphi}{u-\varphi}}$ кодовых вершин. Теорема доказана.

§ 6. Нижние оценки сложности реализации характеристических функций кодов Рида—Маллера ветвящимися программами

Для получения нижней оценки сложности реализации характеристических функций кодов Рида—Маллера воспользуемся теоремами 5 и 7.

Теорема 8. Пусть $\frac{m}{m-u_m} \rightarrow \infty$ при $m \rightarrow \infty$ и $m - u \geq 3$. Тогда

$$\text{NBP}(\mathcal{R}(u_m, m)) = \Omega \left(2^m \frac{m}{m - u_m} / \ln \frac{m}{m - u_m} \right).$$

Доказательство. Так как $\frac{m}{m-u_m} \rightarrow \infty$ при $m \rightarrow \infty$, то можно считать, что

$$\frac{m}{m - u_m} \geq 2^{16}. \quad (20)$$

В качестве $k(m)$ рассмотрим функцию

$$k = \frac{1}{4} \frac{m}{m - u} / \log_2 \frac{m}{m - u}. \quad (21)$$

Положим

$$C = 1/2, \quad p = k, \quad t = k^2 + k. \quad (22)$$

Тогда по утверждению 1 леммы 3 имеем

$$n_1(n/2, k, p, t) \geq \frac{n}{2(ke)^k} = \frac{2^m}{2^{1+k \log_2(ke)}} \geq \frac{2^m}{2^{\varphi_1}},$$

где

$$\varphi_1 = \left\lfloor \frac{m}{4(m-u)} \right\rfloor. \quad (23)$$

В самом деле, если $\frac{m}{m-u} \geq 2^{16}$, то

$$\begin{aligned} 1 + k \log_2(ke) &\leq 1 + \frac{\frac{m}{(m-u)}}{4 \log_2 \frac{m}{m-u}} \left(\log_2 \frac{m}{m-u} - \log_2 \log_2 \frac{m}{m-u} + \log_2 \frac{e}{4} \right) \\ &\leq 1 + \frac{m}{4(m-u)} - \frac{\frac{m}{m-u} \log_2 \log_2 \frac{m}{m-u}}{4 \log_2 \frac{m}{m-u}} \leq \left\lfloor \frac{m}{4(m-u)} \right\rfloor. \end{aligned}$$

Кроме того,

$$n_2(n/2; k, p, t) \geq \frac{n}{k+1} = \frac{2^m}{2^{\log_2(k+1)}} \geq \frac{2^m}{2^{\varphi_2}},$$

где

$$\varphi_2 = \left\lfloor \log_2 \frac{m}{m-u} \right\rfloor. \quad (24)$$

При $\frac{m}{m-u} \geq 2^{16}$ это утверждение справедливо.

Так как при $n' \leq n''$ справедливо неравенство

$$H_{n''}(f) \leq 2^{n''-n'} H_{n'}(f),$$

то при уменьшении величин n_1 и n_2 оценка из теоремы 5 остается справедливой. Поэтому будет считать, что

$$n_1 = \frac{2^m}{2^{\varphi_1}} \text{ и } n_2 = \frac{2^m}{2^{\varphi_2}}.$$

Отсюда и из теоремы 7 следует, что

$$H_{n_1}(\mathcal{R}(u_m, m)) \leq 2^{\binom{m-\varphi_1}{0} + \binom{m-\varphi_1}{1} + \dots + \binom{m-\varphi_1}{m-\varphi_1}} \quad (25)$$

и

$$H_{n_2}(\mathcal{R}(u_m, m)) \leq 2^{\binom{m-\varphi_2}{0} + \binom{m-\varphi_2}{1} + \dots + \binom{m-\varphi_2}{m-\varphi_2}}. \quad (26)$$

При получении нижних оценок для $\text{NBP}(\mathcal{R}(u, m))$ воспользуемся теоремой 5. Поэтому нужно оценить снизу величину

$$R = \frac{|(\mathcal{R}(u, m))^{-1}(1)|}{2^{n-n_1-n_2} H_{n_1}(\mathcal{R}(u, m)) H_{n_2}(\mathcal{R}(u, m))}. \quad (27)$$

По (18), (25) и (26) имеем

$$\begin{aligned}
 R &\geq \frac{2^{1+\binom{m}{1}+\binom{m}{2}+\dots+\binom{m}{u}}}{2^{2^m-2^{m-\varphi_1}-2^{m-\varphi_2}} \cdot 2^{\binom{m-\varphi_1}{0}+\binom{m-\varphi_1}{1}+\dots+\binom{m-\varphi_1}{u-\varphi_1}} \cdot 2^{\binom{m-\varphi_2}{0}+\binom{m-\varphi_2}{1}+\dots+\binom{m-\varphi_2}{u-\varphi_2}}} \\
 &= \frac{2^{\sum_{j=u-\varphi_1+1}^{m-\varphi_1} \binom{m-\varphi_1}{j} + \sum_{j=u-\varphi_2+1}^{m-\varphi_2} \binom{m-\varphi_2}{j}}}{2^{\sum_{j=u+1}^m \binom{m}{j}}} \\
 &= \frac{2^{\sum_{j=0}^{m-u-1} \binom{m-\varphi_1}{j} + \sum_{j=0}^{m-u-1} \binom{m-\varphi_2}{j}}}{2^{\sum_{j=0}^{m-u-1} \binom{m}{j}}} \\
 &= 2^{\sum_{j=0}^{m-u-1} ((\binom{m-\varphi_1}{j} + \binom{m-\varphi_2}{j}) - \binom{m}{j})}.
 \end{aligned} \tag{28}$$

Поэтому при получения нижней оценки для $R(\mathcal{R}(u, m); n/2, p, t)$ надо оценить снизу значение величины $\binom{m-\varphi}{j} / \binom{m}{j}$ при $j \leq m-u-1$. Для этого будем использовать соотношения (23), (24), условия теоремы, а также предположение (20). Имеем $m \geq 3 \cdot 2^{16}$; $3 \leq m-u \leq m/2^{16}$. Отсюда с использованием формулы Стирлинга при $j \leq m-u-1$ и $\varphi \leq \varphi_1 \leq \frac{m}{4(m-u)}$ получаем

$$\begin{aligned}
 \binom{m-\varphi}{j} / \binom{m}{j} &= \frac{(m-\varphi)! j! (m-j)!}{j! (m-\varphi-j)! m!} \\
 &\geq \sqrt{\frac{(m-\varphi)(m-j)}{(m-\varphi-j)m}} \cdot \frac{(m-\varphi)^{m-\varphi} (m-j)^{m-j}}{(m-\varphi-j)^{m-\varphi-j} m^m e^{\frac{1}{12(m-\varphi-j)} + \frac{1}{12m}}} \\
 &\geq \frac{(1 - \frac{\varphi}{m})^{m-\varphi} (1 - \frac{j}{m})^{m-j}}{(1 - \frac{\varphi+j}{m})^{m-\varphi-j} e^{\frac{1}{6(m-\varphi-j)}}} \\
 &\geq \exp \left\{ (m-\varphi) \left(-\frac{\varphi}{m} - \frac{\varphi^2}{2m^2} - \dots \right) + (m-j) \left(-\frac{j}{m} - \frac{j^2}{2m^2} - \dots \right) \right. \\
 &\quad \left. - (m-\varphi-j) \left(-\frac{\varphi+j}{m} - \frac{(\varphi+j)^2}{2m^2} - \dots \right) - \frac{1}{6(m - \frac{m}{4(m-u)} - (m-u-1))} \right\} \\
 &\geq \exp \left\{ -\varphi + \frac{\varphi^2}{2m} + \sum_{l=2}^{\infty} \frac{\varphi^{l+1}}{l(l+1)m^l} - j + \frac{j^2}{2m} + \sum_{l=2}^{\infty} \frac{j^{l+1}}{l(l+1)m^l} \right. \\
 &\quad \left. + (\varphi+j) - \frac{(\varphi+j)^2}{2m} - \sum_{l=2}^{\infty} \frac{(\varphi+j)^{l+1}}{l(l+1)m^l} - \frac{1}{5,49m} \right\} \\
 &\geq \exp \left\{ -\frac{2\varphi j}{m} + \sum_{l=2}^{\infty} \frac{\varphi^{l+1} + j^{l+1} - (\varphi+j)^{l+1}}{l(l+1)m^l} - 2,8 \cdot 10^{-6} \right\}.
 \end{aligned} \tag{29}$$

Оценим снизу сумму $\sum_{l=2}^{\infty} \frac{\varphi^{l+1} + j^{l+1} - (\varphi+j)^{l+1}}{l(l+1)m^l}$ при $j \leq m - u - 1$ и $\varphi \leq \varphi_1 \leq \frac{m}{4(m-u)}$. Рассмотрим случай, когда $j < \varphi$, и случай, когда $j \geq \varphi$.

Случай 1. Пусть $j < \varphi$. Тогда

$$\begin{aligned} \sum_{l=2}^{\infty} \frac{\varphi^{l+1} + j^{l+1} - (\varphi+j)^{l+1}}{l(l+1)m^l} &\geq \sum_{l=2}^{\infty} \frac{-j((\varphi+j)^l + (\varphi+j)^{l-1}\varphi + \dots + \varphi^l)}{l(l+1)m^l} \\ &\geq -\sum_{l=2}^{\infty} \frac{j(l+1)(2\varphi)^l}{l(l+1)m^l} \geq -\sum_{l=2}^{\infty} \frac{(m-u) \cdot 2^l m^l}{l \cdot 4^l (m-u)^l m^l} \geq -\sum_{l=2}^{\infty} \frac{1}{l \cdot 2^l (m-u)^{l-1}} \\ &\geq -\sum_{l=2}^{\infty} \frac{1}{l \cdot 2^l (3)^{l-1}} \geq -0,047. \end{aligned}$$

Случай 2. Пусть $\varphi \leq j$. Тогда

$$\begin{aligned} \sum_{l=2}^{\infty} \frac{\varphi^{l+1} + j^{l+1} - (\varphi+j)^{l+1}}{l(l+1)m^l} &\geq -\sum_{l=2}^{\infty} \frac{\varphi((\varphi+j)^l + (\varphi+j)^{l-1}j + \dots + j^l)}{l(l+1)m^l} \\ &\geq -\sum_{l=2}^{\infty} \frac{\varphi(l+1)(2j)^l}{l(l+1)m^l} \geq -\sum_{l=2}^{\infty} \frac{m \cdot 2^l (m-u-1)^l}{4l(m-u)m^l} \\ &\geq -\sum_{l=2}^{\infty} \frac{2^l (m-u)^{l-1}}{4lm^{l-1}} \geq -8 \cdot 10^{-6}. \end{aligned}$$

Из этих оценок и (29) следует, что

$$\binom{m-\varphi_1}{j} / \binom{m}{j} \geq -\frac{2\varphi j}{m} - 0,048.$$

Пользуясь этим неравенством, а также (20), (23) и (24), получаем

$$\begin{aligned} \binom{m-\varphi_1}{j} / \binom{m}{j} &\geq \exp \left\{ -\frac{2\varphi_1 j}{m} - 0,048 \right\} \\ &\geq \exp \left\{ -\frac{\frac{2m}{4(m-u)}(m-u-1)}{m} - 0,048 \right\} \geq \exp \{ -0,5 - 0,048 \} \geq 0,57 \end{aligned} \quad (30)$$

и

$$\begin{aligned} \binom{m-\varphi_2}{j} / \binom{m}{j} &\geq \exp \left\{ -\frac{2\varphi_1 j}{m} - 0,048 \right\} \\ &\geq \exp \left\{ -\frac{2(m-u-1) \log_2 \frac{m}{(m-u)}}{m} - 0,048 \right\} \geq 0,95. \end{aligned} \quad (31)$$

Из последних двух неравенств и (28) следует, что

$$R \geq 2 \sum_{j=0}^{m-u-1} ((\binom{m-\varphi_1}{j}) + (\binom{m-\varphi_2}{j}) - \binom{m}{j}) \geq 2 \sum_{j=0}^{m-u-1} (0,57+0,95-1) \binom{m}{j} \geq 2^{0,52} \binom{m}{2} \geq 2^{0,25m^2}. \quad (32)$$

Из теоремы 5, (19)–(22), (27) и (32) следует, что

$$\begin{aligned} \text{NBP}(\mathcal{R}(u, m)) &\geq \min \left\{ \frac{n}{2} \cdot k; \frac{1}{4} \sqrt{\frac{2}{e(k+1)}} \cdot R^{1/(4k)} \right\} \\ &= \min \left\{ \frac{1}{8} \cdot \frac{nm/(m-u)}{\log_2 m/(m-u)}; \frac{1}{4} \sqrt{\frac{2}{e \left(\frac{m/(m-u)}{4 \log_2 m/m-u} + 1 \right)}} \cdot R^{\frac{m-u}{m} \log_2 \frac{m}{m-u}} \right\} \\ &\geq \min \left\{ \frac{1}{8} \cdot \frac{2^m m/(m-u)}{\log_2 m/(m-u)}; \frac{1}{4} \sqrt{\frac{1}{\frac{m/(m-u)}{\log_2 m/m-u}}} \cdot 2^{\frac{0,25m^2(m-u)}{m} \log_2 \frac{m}{m-u}} \right\} \\ &\geq \min \left\{ \frac{1}{8} \cdot \frac{2^m m/(m-u)}{\log_2 m/(m-u)}; \frac{1}{4} \sqrt{\frac{1}{\frac{m/(m-u)}{\log_2 m/m-u}}} \cdot 2^{3m} \right\}. \end{aligned}$$

Из этого неравенства и предположения, что $m/(m-u) \geq 2^{16}$, получаем

$$\text{NBP}(\mathcal{R}(u, m)) = \Omega \left(2^m \frac{m}{m-u} / \ln \frac{m}{m-u} \right).$$

Теорема доказана.

Из теоремы 8 и (19) имеем

Следствие. Пусть $u_m = m - C^0$, где C^0 , $C^0 \geq 3$, — константа. Тогда

$$\text{NBP}(\mathcal{R}(u_m, m)) = \Omega(n \log n / \log \log n),$$

где n — число переменных характеристической функции кода $\mathcal{R}(u_m, m)$.

ЛИТЕРАТУРА

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. Нечипорук Э. И. Об одной булевой функции // Докл. АН СССР. 1966. Т. 169, № 4. С. 765–766.

3. **Окольниковишников Е. А.** Нижние оценки сложности реализации характеристических функций двоичных кодов бинарными программами // Методы дискретного анализа в синтезе реализаций булевых функций: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1991. Вып. 51. С. 61–83.
4. **Окольниковишников Е. А.** О сравнении сложностей недетерминированных ветвящихся k -программ // Дискрет. анализ и исслед. операций. Сер. 1. 1999. Т. 6, № 1. С. 65–85.
5. **Разборов А. А.** Нижние оценки сложности реализации симметрических булевых функций контактно-вентильными схемами // Мат. заметки. 1990. Т. 48, вып. 6. С. 79–90.
6. **Babai L., Pudlák P., Rödl V., Szemerédi M.** Lower bounds to the complexity of symmetric Boolean functions // Theoretical Comput. Sci. 1990. V. 74, N 3. P. 313–324.
7. **Borodin A., Razborov A., Smolensky R.** On lower bounds for read- k -times branching programs // Computational Complexity. 1993. V. 3, N 1. P. 1–18.
8. **Okol'nishnikova E. A.** Lower bounds on branching programs // Siberian Adv. Math. 1993. V. 3, N 1. P. 152–166.
9. **Okol'nishnikova E. A.** On the hierarchy of nondeterministic branching k -programs // Fundamentals of computation theory. 11th Intern. symp., FCT 97. Berlin: Springer, 1997. P. 376–387. (Lecture Notes in Comput. Sci.; V. 1279).
10. **Pudlák P.** A lower bound on complexity of branching programs // Mathematical foundations of computer science. Berlin: Springer-Verl., 1984. P. 480–489. (Lecture Notes in Comput. Sci.; V. 176).
11. **Pudlák P.** The hierarchy of Boolean circuits // Comput. Artificial Intelligence. 1987. V. 6, N 5. P. 449–468.
12. **Thathachar J. S.** On separating the read- k -times program hierarchy // Proc. of the 30th annual ACM symp. on theory of computing (Dallas, 1998). New York: ACM Press, 1998. P. 652–662.
13. **Wei V. K.** Generalized Hamming weights for linear codes // IEEE Trans. on Inform. Theory. 1991. V. 37, N 5. P. 1412–1418.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила
28 августа 2001 г.