К. Д. Кириченко, Верхняя оценка сложности полиномиальных нормальных форм булевых функций, *Дискрет. матем.*, 2005, том 17, выпуск 3, 80–88

DOI: http://dx.doi.org/10.4213/dm117

Дискретная математика

том 17 выпуск 3 * 2005

УДК 519.71

Верхняя оценка сложности полиномиальных нормальных форм булевых функций

© 2005 г. К. Д. Кириченко

Рассматривается задача минимизации булевых функций в классе полиномиальных нормальных форм. Предлагается алгоритм построения полиномиально нормальных форм для произвольных булевых функций, причем длина полученной формулы зависит только от числа переменных функции. В качестве исходной информации для алгоритма, помимо функции, используется решение одной задачи о покрытии. При этом число элементарных конъюнкций в полученной формуле равно мощности покрытия. Для введенной задачи о покрытии найдено приближенное решение. В итоге удалось доказать, что сложность булевых функций в классе полиномиальных нормальных форм меньше чем $2^{n+1}(\log_2 n + 1)/n$. Это позволяет сделать вывод о том, что для почти всех булевых функций их сложность при представлении в виде полиномиальных нормальных форм меньше чем при представлении в виде дизъюнктивных нормальных форм.

1. Введение

Как известно, из всех типов формул булевых функций наибольшее применение в приложениях находят дизъюнктивные нормальные формы (д.н.ф.). Одной из причин этого является то, что этот тип представлений булевых функций достаточно хорошо изучен, для него разработан ряд алгоритмов, известны оценки сложности. Другой причиной является то, что д.н.ф. обладают структурой, удобной для применения в разных областях, например, для создания программируемых логических матриц. Однако, этот тип формул не является единственным, обладающим подобной структурой. Очень похожий вид имеют полиномиальные нормальные формы (п.н.ф.), определяемые как представления вида суммы по модулю два произвольного набора элементарных конъюнкций и единицы.

Известно, что при небольшом числе переменных для большей части булевых функций удается получить более короткую п.н.ф. по сравнению с д.н.ф., и потому ряд разработчиков электронных схем проявляют интерес к этой области. Однако этот класс формул на сегодня очень слабо изучен. Существующие алгоритмы точной минимизации работают лишь для функций, зависящих не более чем от шести переменных. Почти ничего не известно о поведении функции Шеннона сложности п.н.ф. булевых функций.

Сложностью булевой функции в классе п.н.ф. называют число слагаемых в наикратчайшей п.н.ф., представляющей эту функцию. Максимум по сложностям всех булевых функций от n аргументов обычно называют функцией Шеннона сложности п.н.ф. булевых функций и обозначают L^n_{pnf}.

Были известны следующие оценки сложности булевых функций в классе п.н.ф. Нижняя оценка

$$L^n_{\text{pnf}} \geqslant \frac{2^n}{n \log_2 3}$$

может быть легко получена из мощностных соображений [5]. До сих пор была известна лишь очень грубая по порядку верхняя оценка $L^n_{\text{pnf}} \leqslant 2^n$, которая легко следует из очевидного неравенства $L^{n+1}_{\text{pnf}} \leqslant 2L^n_{\text{pnf}}$.

Наилучшая из известных до сих пор верхних оценок такого типа

$$L^n_{\text{pnf}} \leqslant \frac{15}{64} 2^n, \qquad n \geqslant 6,$$

была получена в результате нахождения самой сложной функции от шести переменных при помощи компьютерных вычислений [6]. Экспоненциально нарастающая сложность вычислений не позволяет получить точное значения функции Шеннона в классе п.н.ф. при больших n.

В этой работе вводится новый класс полиномиальных представлений булевых функций, являющийся подмножеством п.н.ф., где каждая п.н.ф. определяется через решение одного из вариантов задачи о покрытии. Доказано, что всякая функция имеет представление такого вида и его сложность не превосходит $2^{n+1}(\log_2 n + 1)/n$, что дает верхнюю оценку функции Шеннона для класса п.н.ф. Различные виды полиномиальных разложений булевых функций рассматриваются в обзоре [1].

2. Метод получения верхней оценки функции Шеннона

После необходимых определений мы сформулируем задачу о минимальном затеняющем покрытии. Все недостающие определения можно найти в книге [4].

Пусть $\sigma_i \in \{0, 1\}, i \in \{1, \ldots, n\}$, тогда $(\sigma_1, \ldots, \sigma_n)$ будем называть двоичным набором, а σ_i — i-й компонентой двоичного набора. Набор $(\sigma_1, \ldots, \sigma_n)$ будем обозначать через $\tilde{\sigma}$. В словосочетании двоичный набор слово двоичный часто будем опускать.

Число n называют длиной набора $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$ и обозначают через $|\tilde{\sigma}|$. Весом $\|\tilde{\sigma}\|$ двоичного набора $\tilde{\sigma}$ будем называть число его компонент равных единице, то есть $\|\tilde{\sigma}\| = \sum_{i=1}^n \sigma_i$.

Обозначим через E^n множество двоичных наборов длины n. Множество всех наборов длины n и веса k будем обозначать E^n_k. На множестве E^n естественным образом устанавливается частичный порядок, а именно, $(\sigma_1, \ldots, \sigma_n) \leqslant (\tau_1, \ldots, \tau_n)$ тогда и только тогда, когда $\sigma_i \leqslant \tau_i$ для всех $i \in \{1, \ldots, n\}$.

Множество наборов $S(\tilde{\sigma})$ называется тенью набора $\tilde{\sigma}$, если

$$S(\tilde{\sigma}) = \{\tilde{\tau} \mid \tilde{\tau} \in E^n_k, \tilde{\tau} \leqslant \tilde{\sigma}\},$$

где $n = |\tilde{\sigma}|$, а $k = \|\tilde{\sigma}\| - 1$. Если Q — некоторое множество наборов, то полагаем

$$S(Q) = \bigcup_{\tilde{\sigma} \in Q} S(\tilde{\sigma}).$$

Множество наборов T^n будем называть затеняющим множеством длины n, если

$$\bigcup_{\tilde{\sigma} \in T^n} S(\tilde{\sigma}) = E^n \setminus (1 \ldots 1).$$

Мощность минимального из затеняющих множеств будем обозначать R^n.

Определим возведение в степень для булевых переменных по следующему правилу: $x^y = x \oplus y \oplus 1$. Тогда $x^0 = \bar{x}$, $x^1 = x$, $x^x = 1$.

Булевы функции будут обозначаться символом f с различными индексами. В функции, зависящей от n аргументов, будем использовать аргументы $x_1, \ldots, x_n$. Будем использовать обозначение

$$\prod_{P(i)} x_i = x_{i_1} \ldots x_{i_k},$$

где $P(i)$ — множество индексов $\{i_1, \ldots, i_k\}$.

Если $\tilde{\sigma}$ — набор той же размерности, что и множество аргументов функция f, то обозначим $\alpha_{\tilde{\sigma}}(f)$ коэффициент полинома Жегалкина для функции f при слагаемом $\prod_{\sigma_i=1} x_i$. Тогда полином Жегалкина для n-местной функции f может быть записан в виде

$$f = \bigoplus_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}}(f) \prod_{\sigma_i = 1} x_i.$$

При этом будем говорить, что элементарная конъюнкция $\prod_{\sigma_i=1} x_i$ соответствует набору $\tilde{\sigma}$.

Теорема 1. *Справедливо неравенство*

$$L^n_{\text{pnf}} \leqslant R^n + 1.$$

Доказательство. Пусть $T^n = \{\tilde{\sigma}^1, \ldots, \tilde{\sigma}^{R^n}\}$ — минимальное затеняющее покрытие длины n, в котором наборы упорядочены по убыванию весов. Наборы одинакового веса могут располагаться в произвольном порядке, например, в лексикографическом.

Обозначим Φ^n п.н.ф., определяемую формулой

$$\Phi^n = \bigoplus_{\tilde{\sigma} \in T^n} \prod_{\sigma_j = 1} x_j.$$

Определим набор множеств

$$\hat{T}^n_i = \{\tilde{\sigma}^{i+1}, \tilde{\sigma}^{i+2}, \quad \ldots, \tilde{\sigma}^{R^n}\}, \quad \hat{T}^n_0 = T^n, \quad \hat{T}^n_{R^n} = \varnothing.$$

Обозначим $\tilde{\sigma}^{ij}$ двоичный набор $(\sigma^i_0, \ldots, \sigma^i_{j-1}, 0, \sigma^i_{j+1}, \ldots, \sigma^i_n)$. Определим последовательность функций $f_0, f_1, \ldots, f_{R^n}$ следующим образом:

$$f_0 = \begin{cases} \alpha_{\tilde{1}}(f) = 1, & \text{если } f \oplus \Phi^n, \\ \alpha_{\tilde{1}}(f) = 0, & \text{если } f \oplus \Phi^n \oplus \prod_{0<j\leqslant n} x_j, \end{cases}$$

$$f_i = f_{i-1} \oplus \prod_{\sigma^i_j = 1} x_j^{\overline{\alpha_{\tilde{\sigma}^{ij}}(f_{i-1})}} \oplus \prod_{\sigma^i_j = 1} x_j. \tag{1}$$

Слагаемое $\prod_{\sigma^i_j=1} x_j^{\overline{\alpha_{\tilde{\sigma}^{ij}}(f_{i-1})}}$ обозначает элементарную конъюнкцию, соответствующую набору $\tilde{\sigma}^i$, в которой отрицания стоят над переменными x_j такими, что элементарная конъюнкция без x_j входит в полином Жегалкина для функции f_{i-1}.

Докажем следующее утверждение индукцией по n. Пусть слагаемое $x_{k_1} x_{k_2} \ldots x_{k_p}$ входит в полином Жегалкина для функции f_i. Тогда набор, в котором на местах $k_1, k_2, \ldots, k_p$ стоят единицы, а на остальных местах стоят нули, принадлежит $S(\hat{T}^n_i)$.

Доказательство проведем индукцией по i.

В качестве базы индукции рассмотрим случай $i = 0$. По определению

$$S(\widehat{T}_0^n) = E^n \setminus \{(1 \dots 1)\}.$$

Очевидно, слагаемое $x_1 \dots x_n$ входит в Φ^n, поэтому, по построению f_0 полином Жегалкина для этой функции такого слагаемого не содержит. Таким образом, при $i = 0$ утверждение выполняется.

Проведем шаг индукции. Пусть утверждение выполняется при $i = k - 1$, то есть полином Жегалкина для функции f_{k-1} можно записать в виде

$$f_{k-1} = \bigoplus_{\tilde{\tau} \in S(\widehat{T}_{k-1}^n)} \alpha_{\tilde{\tau}}(f_{k-1}) \prod_{\tau_j = 1} x_j = \bigoplus_{\tilde{\tau} \in S(\tilde{\sigma}^k)} \alpha_{\tilde{\tau}}(f_{k-1}) \prod_{\tau_j = 1} x_j \oplus \bigoplus_{\tilde{\tau} \in S(\widehat{T}_k^n)} \alpha_{\tilde{\tau}}(f_{k-1}) \prod_{\tau_j = 1} x_j. \tag{2}$$

Элементарные конъюнкции, соответствующие наборам из $S(\tilde{\sigma}^k)$, можно представить в виде

$$\bigoplus_{\tilde{\tau} \in S(\tilde{\sigma}^k)} \alpha_{\tilde{\tau}}(f_{k-1}) \prod_{\tau_j = 1} x_j = \prod_{\sigma_j^k = 1} x_j^{\overline{\alpha_{\tilde{\sigma}^k j}(f_{k-1})}} \oplus \prod_{\sigma_j^k = 1} x_j \oplus \Psi_k, \tag{3}$$

где Ψ_k — некоторый полином Жегалкина, содержащий элементарные конъюнкции, состоящие не более чем из $\|\tilde{\sigma}^k - 2\|$ переменных. В этом равенстве легко убедиться, заменив $x_j^{\overline{\alpha_{\tilde{\sigma}^k j}(f_{k-1})}}$ на $(x_j \oplus \alpha_{\tilde{\sigma}^k j}(f_{k-1}))$ и раскрыв скобки.

Найдем полином Жегалкина для функции f_k. Используя определение (1), предположение индукции (2) и равенство (3), получаем, что

$$f_k = \bigoplus_{\tilde{\tau} \in S(\widehat{T}_k^n)} \alpha_{\tilde{\tau}}(f_{k-1}) \prod_{\tau_j = 1} x_j \oplus \Psi_k.$$

Поскольку все элементарные конъюнкции из Ψ_k соответствуют наборам длины $\|\tilde{\sigma}^k - 2\|$ или меньшей, они покрываются наборами длины $\|\tilde{\sigma}^k - 1\|$ или меньшей, которые принадлежат $\widehat{T}_k^n$ по построению. Таким образом, утверждение индукции доказано.

Отсюда, и из того, что $\widehat{T}_{R^n}^n = \varnothing$ следует, что $f_{R^n} = 0$.

Из равенств (1) найдем функцию f:

$$f = \overline{\alpha_{\tilde{1}}(f)} \prod_{0 < j \leqslant n} x_j \oplus \Phi \oplus f_0 = \overline{\alpha_{\tilde{1}}(f)} \prod_{0 < j \leqslant n} x_j \oplus \Phi \oplus \prod_{\sigma_j^1 = 1} x_j^{\overline{\alpha_{\tilde{\tau}^1 j}(f_0)}} \oplus \prod_{\sigma_j^1 = 1} x_j \oplus f_1$$

$$= \overline{\alpha_{\tilde{1}}(f)} \prod_{0 < j \leqslant n} x_j \oplus \Phi \oplus \prod_{\sigma_j^1 = 1} x_j^{\overline{\alpha_{\tilde{\tau}^1 j}(f_0)}} \oplus \prod_{\sigma_j^1 = 1} x_j \oplus \prod_{\sigma_j^2 = 1} x_j^{\overline{\alpha_{\tilde{\tau}^2 j}(f_1)}} \oplus \prod_{\sigma_j^2 = 1} x_j \oplus f_2$$

$$= \dots = \overline{\alpha_{\tilde{1}}(f)} \prod_{0 < j \leqslant n} x_j \oplus \Phi \oplus \bigoplus_{\tilde{\sigma}^i \in T^n} \prod_{\sigma_j^i = 1} x_j^{\overline{\alpha_{\tilde{\tau}^i j}(f_{i-1})}} \oplus \bigoplus_{\tilde{\sigma}^i \in T^n} \prod_{\sigma_j^i = 1} x_j$$

$$= \Phi \oplus \bigoplus_{\tilde{\sigma}^i \in T^n} \prod_{\sigma_j^i = 1} x_j^{\overline{\alpha_{\tilde{\tau}^i j}(f_{i-1})}} \oplus \Phi = \overline{\alpha_{\tilde{1}}(f)} \prod_{0 < j \leqslant n} x_j \oplus \bigoplus_{\tilde{\sigma}^i \in T^n} \prod_{\sigma_j^i = 1} x_j^{\overline{\alpha_{\tilde{\tau}^i j}(f_{i-1})}}.$$

В результате получили п.н.ф., содержащую не более чем $R^n + 1$ слагаемое, что доказывает теорему.

Метод построения п.н.ф., использованный в доказательстве теоремы, является эффективным, в том смысле, что позволяет построить п.н.ф. указанной сложности за полиномиальное время относительно длины вектора, задающего булеву функцию. Далее мы запишем алгоритм, использованный в доказательстве теоремы отдельно и приведем пример его работы. Алгоритм, позволяет строить п.н.ф. сложности не более чем $R^n + 1$ для любой булевой функции, зависящей от n переменных.

Алгоритм. (1) По затеняющему множеству P строим п.н.ф. Φ по формуле

$$\Phi = \bigoplus_{\tilde{\sigma} \in P} \prod_{\sigma_i = 1} x_i.$$

(2) Для заданной булевой функции $f(x_1, \ldots, x_n)$ строим полином Жегалкина F.

(3) Строим п.н.ф. $\Psi = \Phi \oplus F$, сокращая одинаковые слагаемые.

(4) Определяем п.н.ф. Δ: если слагаемое $x_1 \ldots x_n$ присутствует в Ψ, то $\Delta = x_1 \ldots x_n$, в противном случае полагаем $\Delta = 0$.

(5) Удаляем слагаемое $x_1 \ldots x_n$ из Ψ, если оно в ней присутствует.

(6) Упорядочиваем все наборы в P по убыванию весов и для каждого набора $\tilde{\sigma}$ выполняем шаги 7 и 8.

(7) Строим импликанту K, соответствующую набору $\tilde{\sigma}$ и импликанту K', состоящую из тех же переменных, что и K. Для всех i переменная x_i будет входить в K' с отрицаем, если импликанта, соответствующая набору $\{\sigma_1, \ldots, \sigma_{i-1}, 0, \sigma_{i+1}, \ldots, \sigma_n\}$ входит в Ψ.

(8) Добавляем импликанту K' к Δ, а полином Жегалкина для $K + K'$ к Ψ.

Полиномиальная нормальная форма Δ, полученная на последнем шаге, будет эквивалентна исходной функции f.

Пример. (1) По минимальному затеняющему множеству P для E^4 строим п.н.ф. Φ,

$$P = \{(1111), (1110), (1101), (1011), (1100), (0011), (1000)\},$$
$$\Phi = x_1x_2x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_3x_4 \oplus x_1.$$

(2) Полином Жегалкина для f равен

$$F = x_1x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_3 \oplus 1.$$

(3) Построим $\Psi = F \oplus \Phi$:

$$\Psi = x_1x_2x_3 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus 1.$$

(4) Определяем, что $\Delta = 0$.

(5) Полиномиальная нормальная форма Ψ остается без изменений.

(6) Наборы уже упорядочены.

(7.1) Строим K и K' по набору (1111). Получаем, что $K = x_1x_2x_3x_4$, а $K' = x_1x_2x_3\bar{x}_4$, так как слагаемое $x_1x_2x_3$ присутствует в Ψ.

(8.1) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4,$$
$$\Psi = x_1x_2x_3 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus 1 \oplus K \oplus K' = x_3x_4 \oplus x_1 \oplus x_3 \oplus 1.$$

(7.2) Строим K и K' по набору (1110). Получаем, что $K = x_1x_2x_3$ и $K' = x_1x_2x_3$, так как слагаемые x_1x_2, x_1x_3, x_2x_3 отсутствуют в Ψ.

(8.2) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4 \oplus x_1x_2x_3,$$
$$\Psi = x_3x_4 \oplus x_1 \oplus x_3 \oplus 1 \oplus K \oplus K' = x_3x_4 \oplus x_1 \oplus x_3 \oplus 1.$$

(7.3) Строим K и K' по набору (1101). Получаем , что $K = x_1x_2x_4$ и $K' = x_1x_2x_4$, так как слагаемые x_1x_2, x_1x_4, x_2x_4 отсутствуют в Ψ.

(8.3) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4,$$
$$\Psi = x_3x_4 \oplus x_1 \oplus x_3 \oplus 1 \oplus K \oplus K' = x_3x_4 \oplus x_1 \oplus x_3 \oplus 1.$$

(7.4) Строим K и K' по набору (1011). Получаем, что $K = x_1x_3x_4$ и $K' = \bar{x}_1x_3x_4$, так как слагаемое x_3x_4 присутствует в Ψ.

(8.4) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus \bar{x}_1x_3x_4,$$
$$\Psi = x_3x_4 \oplus x_1 \oplus x_3 \oplus 1 \oplus K \oplus K' = x_1 \oplus x_3 \oplus 1.$$

(7.5) Строим K и K' по набору (1100). Получаем, что $K = x_1x_2$ и $K' = x_1\bar{x}_2$, так как слагаемое x_1 присутствует в Ψ.

(8.5) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus \bar{x}_1x_3x_4 \oplus x_1\bar{x}_2,$$
$$\Psi = x_1 \oplus x_3 \oplus 1 \oplus K \oplus K' = x_3 \oplus 1.$$

(7.6) Строим K и K' по набору (0011). Получаем, что $K = x_3x_4$ и $K' = x_3\bar{x}_4$, так как слагаемое x_3 присутствует в Ψ.

(8.6) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus \bar{x}_1x_3x_4 \oplus x_1\bar{x}_2 \oplus x_3\bar{x}_4,$$
$$\Psi = x_3 \oplus 1 \oplus K \oplus K' = 1.$$

(7.7) Строим K и K' по набору (1000). Получаем, что $K = x_1$ и $K' = \bar{x}_1$, так как слагаемое 1 присутствует в Ψ.

(8.7) Изменяем Δ и Ψ:

$$\Delta = x_1x_2x_3\bar{x}_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus \bar{x}_1x_3x_4 \oplus x_1\bar{x}_2 \oplus x_3\bar{x}_4 \oplus \bar{x}_1,$$
$$\Psi = 1 \oplus K \oplus K' = 0.$$

Легко проверить, что полученная п.н.ф. Δ действительно представляет исходную функцию f.

3. Оценка мощности теневого покрытия

Для получения верхней оценки R^n потребуется ввести несколько определений.

Пусть $\tilde{\sigma} = \{\sigma_1, \dots, \sigma_n\}$ — некоторый двоичный набор. Сферой с центром в точке $\tilde{\sigma}$ будем называть множество наборов

$$C(\tilde{\sigma}) = \{(\sigma_1, \dots, \sigma_{k-1}, \sigma_k \oplus 1, \sigma_{k+1}, \dots, \sigma n) \mid 1 \geqslant k \geqslant n\}.$$

Если Q — некоторое множество наборов, то будем писать

$$C(Q) = \bigcup_{\tilde{\sigma} \in Q} C(\tilde{\sigma}).$$

Если P — некоторое множество наборов, то обозначим $\mathrm{EV}(P)$ и $\mathrm{OD}(P)$, соответственно, множества наборов четного и нечетного весов из P. Если P и Q — некоторые множества наборов, то обозначим $P \times Q$ множество наборов $\{\tilde{\sigma} = \tilde{\alpha}\tilde{\beta} \mid \tilde{\alpha} \in P, \tilde{\beta} \in Q\}$. Для улучшения читаемости формул будем считать, что операция $\times$ имеет наибольший приоритет.

Определим множества наборов T_i^n, $n = 2^k$, $0 \leqslant i < n$. Для упрощения записи будет использоваться следующая договоренность: всюду в записи T_i^n под T_{k+m}^n будет подразумеваться $T_{(k+m) \pmod n}^n$. Множества T_i^n определяются соотношениями

$$T_0^1 = \{(0), (1)\}, \quad T_{2p}^{2n} = \bigcup_{i=0}^{n-1} T_i^n \times \mathrm{EV}(T_{i+p}^n), \quad T_{2p+1}^{2n} = \bigcup_{i=0}^{n-1} T_i^n \times \mathrm{OD}(T_{i+p}^n).$$

Используя принцип индукции, легко доказать, что $T_0^n, \dots T_{n-1}^n$ задают разбиение E^n на класс непересекающихся множеств, причем каждое множество содержит $2^n/n$ наборов.

Предложение 1. *Для всех натуральных $n = 2^k$ и i, $0 \leqslant i < n$, справедливо равенство $C(T_i^n) = E^n$.*

Доказательство. Проведем доказательство индукцией по k. При $k = 0$ утверждение очевидно.

Пусть для всех $k \leqslant m$ утверждение верно, тогда положим $k = m + 1$, $n = 2^m$ и рассмотрим множество T_i^{2n} и произвольный набор $\tilde{\sigma} = \tilde{\alpha}\tilde{\beta}$, причем $|\tilde{\alpha}| = |\tilde{\beta}| = n$. Очевидно, что набор $\tilde{\sigma}$ входит в сферу с центром $\tilde{\sigma}'$, если $\tilde{\sigma}' = \tilde{\alpha}'\tilde{\beta}$ или если $\tilde{\sigma}' = \tilde{\alpha}\tilde{\beta}'$, где $\tilde{\alpha}'$ и $\tilde{\beta}'$ есть центры сфер, в которые входят наборы $\tilde{\alpha}$ и $\tilde{\beta}$ соответственно. Тогда, если $i = 2p$ — четное число и $\tilde{\beta}$ имеет четный вес, то для некоторого j справедливо включение $\tilde{\beta} \in \mathrm{EV}(T_{j+p}^n)$, и по предположению индукции $\tilde{\alpha} \in C(T_j^n)$, то есть $\tilde{\sigma} \in T_i^{2n}$. Если же $\tilde{\beta}$ имеет нечетный вес, то для некоторого j справедливо включение $\tilde{\alpha} \in T_j^n$, тогда по индуктивному предположению $\tilde{\beta} \in C(T_{j+p}^n)$, а с учетом того, что вес $\tilde{\beta}$ нечетный, $\tilde{\beta} \in C(\mathrm{EV}(T_{j+p}^n))$. Доказательство для случая нечетного i аналогично.

Из этого предложения следует, что все наборы из E^n входят в $C(T_i^n)$ ровно один раз, так как каждая сфера содержит n наборов, а каждое T_i^n содержит $2^n/n$ наборов.

Лемма 1. *Для любых натуральных чисел n и k таких, что $n = 2^p$, $k \leqslant n$, существует набор множеств $T_{j_1}^n, \ldots T_{j_k}^n$ такой, что для него выполняется неравенство*

$$\left| \bigcup_{i \in \{j_1, \ldots j_k\}} S(T_i^n) \right| \geqslant 2^n - 2^{n-k}.$$

Доказательство. Обозначим b биномиальный коэффициент $\binom{n}{k}$. Множество всех k-элементных подмножеств множества $\{0, 1, \ldots, n-1\}$ обозначим $\{I_1, \ldots, I_b\}$.

Рассмотрим некоторый набор $\tilde{\alpha}$ длины n и веса r. Очевидно, он входит в n различных сфер, причем в $n - r$ случаях он получается заменой единицы на ноль. Учитывая, что все наборы входят в $C(T_i^n)$ ровно один раз, получаем, что $\tilde{\alpha}$ принадлежит ровно $n - r$ множествам $S(T_i^n)$. Тогда, легко понять, что $\tilde{\alpha}$ входит ровно в $\binom{n}{k} - \binom{r}{k}$ различных k-элементных объединений множеств $S(T_i^n)$. Тогда все слова веса r встречаются во всех k-элементных объединениях множеств $S(T_i^n)$ ровно $\left(\binom{n}{k} - \binom{r}{k}\right)\binom{n}{r}$ раз. В силу этого можно найти значение суммы

$$\sum_{j=1}^{b} \left| \bigcup_{i \in I_j} S(T_i^n) \right| = \sum_{r=0}^{n} \left(\binom{n}{k} - \binom{r}{k} \right) \binom{n}{r}$$

$$= \sum_{r=0}^{n} \binom{n}{k}\binom{n}{r} - \sum_{r=0}^{n} \binom{r}{k}\binom{n}{r} = \binom{n}{k} 2^n - \binom{n}{k} 2^{n-k}.$$

Поскольку начальная сумма содержит $\binom{n}{k}$ слагаемых, по крайней мере для одного из них будет выполняться требуемое неравенство.

Теорема 2. *Справедлива оценка*

$$R^n \leqslant \frac{2^n(\log_2 n + 1)}{n} - 1, \qquad n = 2^r.$$

Доказательство. Построим искомое покрытие следующим образом. Выберем k множеств T_i^n таких, что объединение их теней максимально. По лемме оно содержит не менее $2^n - 2^{n-k}$ элементов. При этом незатененными остались $2^{n-k} - 1$ наборов (набор $\tilde{1}$ не может быть затенен). Для каждого незатененного набора найдем набор, его затеняющий, и добавим его в покрытие. Таким образом, верна оценка

$$R^n \leqslant k\frac{2^n}{n} + 2^{n-k} - 1.$$

Теперь, подставив $\log_2 n$ вместо k, получим требуемую оценку.

Следствие 1. *Справедлива оценка*

$$L_{\text{pnf}}^n < \frac{2^n(2\log_2 n + 2)}{n}$$

Доказательство. Введем обозначение $m = 2^{\lfloor \log_2 n \rfloor}$. Тогда $2m > n$. Из очевидной оценки $L^{n+1}_{\text{pnf}} \leqslant 2L^{n}_{\text{pnf}}$, теоремы 1 и теоремы 2 получаем, что

$$L^{n}_{\text{p.n.f.}} \leqslant 2^{n-m} L^{m}_{\text{p.n.f.}} \leqslant 2^{n-m} \frac{2^m(\log_2 m + 1)}{m} \leqslant \frac{2^n(2\log_2 m + 2)}{2m} < \frac{2^n(2\log_2 n + 2)}{n}.$$

Хорошо известно, что асимптотика сложности почти всех булевых функций в классе дизъюнктивных нормальных форм по порядку составляет

$$\frac{2^n}{\log_2 n \log_2 \log_2 n}$$

(см. [3, 2]). Таким образом, здесь доказано, что класс п.н.ф. асимптотически лучше класса д.н.ф. для реализации булевых функций.

Список литературы

1. Винокуров С. Ф., Перязев Н. А., Полиномиальные разложения булевых функций. *Кибернетика и системный анализ* (1993) **6**, 34–47.

2. Коршунов А. Д., О сложности кратчайших дизъюнктивных нормальных форм случайных булевых функций. *Методы дискретного анализа в оптимизации управляющих систем* (1983) **40**, 25–53.

3. Кузнецов С. Е., О нижней оценке длины кратчайшей д.н.ф. почти всех булевых функций. *Вероятностные методы и кибернетика* (1983) **19**, 44–47.

4. Перязев Н. А., *Основы теории булевых функций.* Физматлит, Москва, 1999.

5. Even S., Kohavi I., Paz A., On minimal modulo 2 sums of products for switching functions. *IEEE Trans. Elect. Comput.* (1967), 671–674.

6. Koda N., Sasao T., An upper bound on the number of products in minimum ESOPs. In: *Representations of discrete functions (Sasao T., Fujita M., Eds.).* Kluwer, Boston, 1996, pp. 94–101.

Статья поступила 26.06.2004.