ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXXVII 1988 1

УДК 519.7

МАТЕМАТИКА

А. А. Алексанян

# Оценки, связанные с представлением булевых функций посредством линеаризированных дизъюнктивных нормальных форм

(Представлено чл.-корр. АН Армянской ССР А. Б. Нерсесяном 25/II 1988)

Линеаризированные дизъюнктивные нормальные формы (л.д.н.ф.) введены в качестве естественного обобщения обычных дизъюнктивных нормальных форм (д.н.ф.) (см. [1,2]) в связи с задачей решения систем булевых уравнений и представляют собой дизъюнктивные формы, составленные из произведений линейных функций.

Л.д.н.ф. обладают основными теоретико-множественными и структурными свойствами обычных д.н.ф. и в то же время имеют существенные отличия от последних. Например, понятия связности и протяженности д.н.ф. ([1]) не имеют аналогов для л.д.н.ф., многие сложно реализуемые в классе д.н.ф. функции весьма просто реализуются посредством л.д.н.ф. Естественное алгебраическое описание л.д.н.ф. позволяет строить удобные алгоритмы и даже получать аналитические решения задач, для решения которых средства алгебры д.н.ф. оказываются недостаточно богатыми.

Настоящая работа посвящена изучению метрических (количественных) характеристик, связанных со сложностью реализации булевых функций в классе л.д.н.ф.

1. *Основные понятия.* Пусть $E^n$ — множество вершин $n$-мерного единичного куба, т. е.

$$E^n = \{x = (x_1, \ldots, x_n) | x_i \in \{0, 1\},\ i = 1, \ldots, n\} \text{ и}$$

$$E^n_\beta = \{x = (x_1, \ldots, x_n) | x \in E^n,\ x_1 = \beta\},\ \beta \in \{0, 1\}.$$

Множество булевых функций, отображающих $E^n$ в $\{0, 1\}$, зависящих от не более чем $n$ переменных, обозначим через $P(n)$. Каждая функция из $P(n)$ однозначно представима полиномом Жегалкина (многочленом по mod 2 над полем Галуа $GF(2)$) ([1]).

Класс линейных функций $a_0 + a_1x_1 + \ldots + a_nx_n$ обозначается через $L(n)$.

Определение. Функция $f \in P(n)$ называется *линеаризируемой*, если $f = \prod_{i=1}^{m} g_i$, где $g_i \in L(n)$, $i = 1, \ldots, m$.

Класс линеаризируемых функций, зависящих от не более чем $n$ переменных, обозначим через $\Pi L(n)$.

Определение. Выражение $f_1 \vee \ldots \vee f_m$, где $f_i \in \Pi L(n)$, $i =$

$=1, \ldots, m$, называется *линеаризированной дизъюнктивной нормальной формой* (л. д. н. ф.), а число $m$—длиной л. д. н. ф.

Определение. Л. д. н. ф., имеющая наименьшую длину среди всех л. д. н. ф., реализующих ту же булеву функцию, называется *кратчайшей*.

Определение. Функция $g \in \Pi L(n)$ называется *максимальной* для $f \in P(n)$, если $g \leqslant f$ и из $g \leqslant g' \leqslant f$, $g' \in \Pi L(n)$ следует $g \equiv g'$.

Определение. *Сокращенной л. д. н. ф.* функции $f \in P(n)$ называется л. д. н. ф., составленная из всех максимальных для $f$ функций.

*Примеры.* Пусть $f \equiv x_1 + \ldots + x_n$. Кратчайшая л. н. ф. имеет длину $2^{n-1}$, а длина кратчайшей л. д. н. ф. равна 1.

Пусть $f \equiv x_1 x_2 + x_3 x_4 + \ldots + x_{2n-1} x_{2n}$. Длина кратчайшей д. н. ф. равна $\frac{1}{2}(3^n - 1)$, а длина кратчайшей л. д. н. ф. равна $2^n - 1$.

Пусть $f \equiv x_1 \vee x_2 \vee \ldots \vee x_n$, тогда длины кратчайших л. д. н. ф. и д. н. ф. совпадают и равны $n$.

Задача минимизации булевых функций в классе л. д. н. ф. состоит в построении кратчайшей или близкой к ней по длине л. д. н. ф.

В дальнейшем $E^n$ и $L(n)$ рассматриваются в качестве линейных пространств над полем $GF(2)$.

2. *Класс* $\Pi L(n)$. Введем множества $N_f = \{x \in E^n \mid f(x) = 1\}$ и $M(f) = \{g \mid g \in L(n),\ g \cdot f = 0\}$. Очевидно, что $M(f)$ является линейным подпространством в $L(n)$.

Предложение. *Пусть* $f \in \Pi L(n)$, *тогда кратчайшее* (*в смысле количества сомножителей*) *представление* $f$ *в виде произведения линейных форм имеет вид* $f = \prod_{g \in B} (g + 1)$, $B$—*произвольный базис в* $M(f)$.

Размерность ($\dim f$) функции $f \in \Pi L(n)$ определяется как число $n - \dim M(f)$, а степень ($\deg f$)—это степень соответствующего многочлена Жегалкина. Для $f \not\equiv 0$ имеем $\deg f = \dim M(f)$.

Количество $m$-мерных линейных подпространств $n$-мерного линейного пространства над $GF(2)$ обозначим через $\begin{bmatrix} n \\ m \end{bmatrix}$-коэффициент Гаусса ([3]).

Обозначим через $|A|$ мощность множества $A$. Основные свойства линеаризируемых функций описывает следующая

Теорема 1. *Пусть* $f \in \Pi L(n)$, *тогда*

а) *если* $f \equiv 0$, *то* $\dim M(f) = n - 1$;

б) *если* $f \not\equiv 0$, *то* $N_f = M^{\perp}(f) \cap E_1^{n+1}$—*смежный класс по подпространству* $M^{\perp}(f) \cap E_0^{n+1}$. *Если* $\deg f = m$, *то* $|N_f| = 2^{n-m}$ *и* $|M^{\perp}(f)| = 2 \cdot |N_f|$;

в) $|\{f \mid \deg f = m,\ f \in \Pi L(n)\}| = 2^m \cdot \begin{bmatrix} n \\ m \end{bmatrix}$;

г) $|\Pi L(n)| = 1 + \sum_{m=0}^{n} 2^m \cdot \begin{bmatrix} n \\ m \end{bmatrix}$ и

$$2^{\frac{n^2}{4}\left(1-o\left(\frac{1}{n}\right)\right)} \leqslant |\Pi L(n)| < 2^{\frac{n^2}{4}\left(1+o\left(\frac{1}{n}\right)\right)}$$

3. *Метрические характеристики.* Оценки, излагаемые в этом пункте, получены с помощью методов развитых в работах ([4,5]). Принято говорить, что некоторое свойство выполнено для почти всех $f \in P(n)$, если доля функций, для которых указанное свойство выполняется, стремится к 1 при $n \to \infty$.

Пусть $l(n, m, f)$ – количество функций $g \in \Pi L(n)$ таких, что $g \leqslant f$ и $\dim g = m$.

Теорема 2. *Для почти всех $f \in P(n)$ верно*

$$\left|\begin{matrix} n \\ m \end{matrix}\right| \left(\frac{2^{n-m}}{2^{2^m}} - n\sqrt{\frac{2^{n-m}}{2^{2^m}}}\right) \leqslant l(n, m, f) \leqslant \left|\begin{matrix} n \\ m \end{matrix}\right| \left(\frac{2^{n-m}}{2^{2^m}} + n\sqrt{\frac{2^{n-m}}{2^{2^m}}}\right).$$

В случае д. н. ф. соответствующая оценка получается заменой $\left|\begin{matrix} n \\ m \end{matrix}\right|$ на $C_n^m$ ([4]).

Пусть $[x]$—целая часть числа $x$.

Теорема 3 *Для почти всех функций $f \in P(n)$ имеет место* $\dim g \leqslant |\log_2 n + \log_2 \log_2 n| + 1$ *для всех $g \leqslant f$, $g \in \Pi l(n)$.*

Для д. н. ф. максимальная размерность допустимого интервала у почти всех функций равна $|\log_2 n| + 1$ (см. [1, 2]).

Теорема 4. *Для почти всех $f \in P(n)$ длина $l(f)$ сокращенной л. д. н. ф. удовлетворяет неравенствам*

$$n^{n(1-\alpha_n)} \leqslant l(f) \leqslant n^{n(1+\alpha_n)},$$

*где* $\alpha_n = \frac{\alpha}{\log_2 n}$, $\beta_n = \frac{\beta}{\log_2 n}$ *и* $3 < \alpha, \beta < 3+\varepsilon$.

Соответствующая оценка длины сокращенной д. н. ф. для почти всех функций имеет вид ([1,4])

$$n^{(1-\delta_n)\log_2\log_2 n} \cdot 2^n \leqslant l(f) \leqslant n^{(1+\gamma_n)\log_2\log_2 n} \cdot 2^n,$$

где $\lim\limits_{n\to\infty} \delta_n = \lim\limits_{n\to\infty} \gamma_n = 0$.

Пусть $l(n) = \max\limits_{f \in P(n)} l(f)$.

Теорема 5.

$$2^{\left(1-o\left(\frac{1}{\log_2 n}\right)\right)n\log_2 n} < l(n) \leqslant 2^{\frac{n^2}{4}\left(1+o\left(\frac{1}{n}\right)\right)}.$$

Максимальная длина сокращенной д. н. ф. удовлетворяет неравенствам ([1])

$$\frac{3^n}{n} \leqslant l(n) \leqslant \frac{3^n}{\sqrt{n}}.$$

Теорема 6. *Почти все максимальные для $l$ функции $g \in \Pi L(n)$ для почти всех функций $f \in P(n)$ имеют размерность, удовлетворяющую неравенствам*

$$\log_2 n - 4 \leqslant \dim g \leqslant \log_2 n + 3.$$

Здесь следует особо отметить важное отличие л. д. н. ф. от д.

н. ф. В случае д. н. ф. у почти всех функций почти все члены сокращенной д. н. ф. имеют размерность, близкую к $\log_2\log_2 n$ см. (⁶), в то время как максимальная размерность равна $[\log_2 n]+1$. Из теоремы 6 следует, что почти все члены сокращенной л. д. н. ф. имеют размерность порядка максимально возможной — $O(\log_2 n)$.

В изложенных ниже результатах получены оценки для важнейшей характеристики класса л. д. н. ф. — длины кратчайшей л. д. н. ф.

Обозначим через $F(n)$ множество симметрических функций из $P(n)$, т. е. функций, инвариантных относительно любой перестановки переменных.

Пусть $S(f)$ — длина кратчайшей л. д. н. ф. функции $f\in P(n)$. Обозначим через $SF(n)=\max_{f\in F(n)} S(f)$.

Теорема 7 (⁷).

$$\frac{1}{n+2}\left(\frac{3}{2}\right)^n \leqslant SF(n) \leqslant \text{const}\cdot n\left(\frac{3}{2}\right)^n.$$

Теорема 8. *Для почти всех $f\in P(n)$ имеет место*

$$\frac{(1-\varepsilon_n)\cdot 2^{n-1}}{2n\cdot\log_2 n} \leqslant S(f) \leqslant \text{const}\cdot\frac{2^n\cdot\log_2 n}{n}, \text{ где } \lim_{n\to\infty}\varepsilon_n = 0.$$

Отметим, что в классе симметрических функций достигается максимум длины кратчайшей д. н. ф. Теоремы 7 и 8 показывают, что симметрические функции реализуются в классе л. д. н. ф. существенно проще, чем почти все функции из $P(n)$. Порядок длины кратчайшей д. н. ф. для почти всех функций равен $2^{n-1}/(\log_2 n\cdot\log_2\log_2 n)$ (см. (⁴⁻⁶)). Отсюда и из теоремы 8 следует, что почти все функции из $P(n)$ реализуются в классе л. д. н. ф. по крайней мере в $n/(\log_2^2 n\cdot\log_2\log_2 n)$ раз проще, чем в классе д. н. ф.

Автор выражает глубокую благодарность чл.-корр. АН СССР Ю. И. Журавлеву за стимулирующие обсуждения.

Ереванский государственный университет

Ա. Ա. ԱՆԴՐԵԱՍՅԱՆ

## Դծայնացված դիզյունկտիվ նորմալ ձևերով բուլյան ֆունկցիաների ներկայացման հետ կապված գնահատականներ

*Հետազոտված են բուլյան ֆունկցիաների գծայնացված դիզյունկտիվ նորմալ ձևերի (գ. դ. ն. ձ.) մետրիկական բնութագրիչները՝ կրճատված գ. դ. ն. ձ.-ի երկարությունը և անդամների չափը, կարճագույն գ. դ. ն. ձ.-ի երկարությունը և այլն։ Ցույց է տրված, որ համարյա բոլոր ֆունկցիաները կարելի է իրականացնել գ. դ. ն. ձ.-ի պատում առնվազն $\frac{n}{\log_2^2 n\cdot\log_2\log_2 n}$ անգամ ա-*

վելի կարճ բանաձևի օգնությամբ, քան սովորական դիզյունկտիվ նորմալ ձևերի դասում։ Սիմետրիկ ֆունկցիաների դասի կարճագույն գ. դ. Ն. Ձ.—ների կայացման համար ստացված է բարդության լոգարիթմի ասիմպտոտիկ արժեքը՝ $n(\log_2 3-1)$.

## ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] Дискретная математика и математические вопросы кибернетики, т. I. М., Наука, 1974. [2] *Ю. И. Журавлев*, Проблемы кибернетики, вып. 8, с. 5—44 (1962). [3] *М. Айгнер*, Комбинаторная теория, Мир, М., 1982. [4] *В. В. Глаголев* Проблемы кибернетики, вып. 19, с. 75—94 (1967). [5] *А. А. Сапоженко*, Дискретный анализ, вып. 21, с. 62—71 (1972). [6] *А. Е. Андреев*, Вестн. Моск. ун-та. Математика, механика, № 3, с. 29—35 (1985). [7] *Л. А. Алексанян*, ДАН АрмССР, т. 84, № 5, с. 195—197 (1987).