ՀԱՅԿԱԿԱՆ ԽՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР
Том 90 1990 № 2

УДК 519.7

МАТЕМАТИКА

А. А. Алексанян

# Об одной экстремальной задаче, связанной со сложностью реализации булевых функций в классе д. н. ф. над линейными функциями

(Представлено чл.-корр. АН Армянской ССР А. Б. Нерсесяном 9/I 1990)

В работах [1–6] введено и исследовано понятие дизъюнктивных нормальных форм (д. н. ф.) над линейными функциями в качестве естественного обобщения обычных д. н. ф. Задача построения кратчайшей реализации в новом классе формул равносильна кратчайшему покрытию множества единиц заданной функции смежными классами (сдвигами) по линейным подпространствам в множестве вершин $n$-мерного единичного куба, рассматриваемом в качестве линейного пространства над полем Галуа $GF(2)$.

В теории обычных д. н. ф. [7] сложнейшей функцией в смысле длины кратчайшей д. н. ф. является функция „счетчик четности" $1+x_1+x_2+\ldots+x_n \pmod 2$. Покрытие, соответствующее кратчайшей д. н. ф. данной функции, состоит из $2^{n-1}$ кульмерных, попарно непересекающихся интервалов. Таким образом, при реализации булевых функций в классе д. н. ф. максимум сложности достигается на симметрической функции, множество единиц которой состоит из изолированных вершин, взятых в максимально возможном количестве.

Из результатов работ [1,3] следует, что симметрические функции в классе д. н. ф. над линейными функциями реализуются гораздо проще, чем почти все булевы функции, и максимум сложности реализации не может быть достигнут на симметрической функции.

Естественным образом возникает вопрос о возможности построения функции, имеющей наибольшую сложность, множество единиц которой содержит лишь смежные классы нулевой или ограниченной (не зависящей от $n$) размерности. Иными словами, требуется построить аналог „счетчика четности" для нового класса формул, а также выяснить, сохраняется ли для него свойство максимальной сложности реализации.

1. Обозначим через $E^n$ множество вершин $n$-мерного единичного куба, рассматриваемого в качестве $n$-мерного линейного пространства над полем Галуа $GF(2)$, т. е. $E^n=\{x=(x_1, \ldots, x_n) \mid x_i \in \{0, 1\}\}$. Через $P(n)$ обозначается множество булевых функций, зависящих от не более чем $n$ переменных.

Пусть $f \in P(n)$, тогда множество $N_f \equiv \{x \in E^n \mid f(x)=1\}$ называется множеством единиц функции $f$.

Определение. *Функция $f \in P(n)$ называется линеаризируе-*

*мой, если $f$ представима в виде произведения конечного числа линейных над $GF(2)$ функций.*

Легко проверяется, что для линеаризируемой $f \in P(n)$ множество единиц $N_f$ — суть смежный класс (сдвиг) по некоторому линейному подпространству в $E^n$.

Определение. *Выражение вида $f_1 \vee f_2 \vee \ldots \vee f_m$, где $f_i$ — линеаризируемая функция, $i = 1, \ldots, m$, называется линеаризированной дизъюнктивной нормальной формой (л. д. н. ф.). Число $m$ называется длиной л. д. н. ф.*

Определение. *Л. д. н. ф. $f \equiv f_1 \vee f_2 \vee \ldots \vee f_m$ называется кратчайшей, если функция $f$ не может быть реализована с помощью л. д. н. ф. меньшей длины.*

Геометрически реализация функции $f$ посредством л. д. н. ф. соответствует покрытию множества $N_f$ системой смежных классов. Следует также отметить, что обычная д. н. ф. есть частный случай л. д. н. ф.

Очевидно, что всякая пара вершин из $E^n$ составляет смежный класс и, следовательно, является множеством единиц некоторой линеаризируемой функции. Поэтому, если $N_f$ не состоит из одной-единственной вершины, то размерность смежного класса, содержащегося в $N_f$ и не содержащегося ни в одном другом смежном классе в $N_f$, не меньше, чем 1. Т. е. каждая вершина из $N_f$ содержится в смежном классе, состоящем из двух вершин.

2. Рассмотрим теперь следующую задачу. Обозначим через $k(n) = \max |A|$, где $|A|$ — мощность множества $A$, пробегающего все подмножества в $E^n$, не содержащие смежных классов размерности 2. Требуется оценить величину $k(n)$.

Теорема.

$$c \cdot 2^{\frac{n}{2}} + 1 \leqslant k(n) \leqslant \sqrt{2} \cdot 2^{\frac{n}{2}} + \frac{1}{2}, \text{ где}$$

$$c = \begin{cases} 1, & \text{при } n \equiv 0 \bmod 2 \\ \dfrac{1}{\sqrt{2}}, & \text{при } n \equiv 1 \bmod 2 \end{cases}.$$

Доказательство. *Верхняя оценка.* Пусть $A = \{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq E^n$ и не содержит смежных классов размерности 2. Т. е. для любой тройки $\alpha$, $\beta$, $\gamma$ вершин из $A$ имеет место: $\alpha + \beta + \gamma \notin A$ (здесь $+$ — сложение по mod 2).

Рассмотрим множество всевозможных сумм вида $\alpha_1 + \alpha_i + \alpha_j$, где $p \neq j$ и $i, j \in \{2, 3, \ldots, k\}$. Нетрудно проверить что все такие суммы различны, ибо из $\alpha_1 + \alpha_i + \alpha_j = \alpha_1 + \alpha_p + \alpha_q$ следует $\alpha_i + \alpha_j + \alpha_p + \alpha_q = 0$. Если все $\alpha_i$, $\alpha_j$, $\alpha_q$ различны, то $\alpha_i + \alpha_j + \alpha_p = \alpha_q \in A$, что противоречит определению множества $A$. Если $\alpha_i = \alpha_p$, тогда $\alpha_j = \alpha_q$, т. е. тройки $(\alpha_1, \alpha_i, \alpha_j)$ и $(\alpha_1, \alpha_p, \alpha_q)$ совпадают. Всего имеем $\binom{k-1}{2} = \dfrac{(k-1)(k-2)}{2}$ различных сумм вида $\alpha_1 + \alpha_i + \alpha_j \notin A$. Следовательно,

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

Отсюда получаем $k^2-k+2\leqslant 2\cdot 2^n$ и $\left(k-\frac{1}{2}\right)^2\leqslant 2\cdot 2^n-\frac{7}{4}\leqslant 2\times$ $\times 2^n$. Окончательно $k\leqslant\sqrt{2}\cdot 2^{n/2}+\frac{1}{2}$.

*Нижняя оценка.* Нижняя оценка получается прямым построением. Пусть $n\equiv 0 \bmod 2$. Рассмотрим $E^n$ в качестве конечного поля $GF(2^n)$ (см. ([8])). Тогда имеем $2^n-1=(2^{n/2}-1)(2^{n/2}+1)$, и $n$ является наименьшей степенью двойки такой, что $2^n\equiv 1 \bmod(2^{n/2}+1)$, ибо при $2^s\equiv 1 \bmod(2^{n/2}+1)$ число $s$ делит $n$ и в то же время $\frac{n}{2}<s$, поэтому $s=n$.

Обозначим через $\Omega(n)$ группу корней $(2^{n/2}+1)$-ой степени из единицы в поле $GF(2^n)$, т. е. $\Omega(n)$—множество корней многочлена $x^{2^{n/2}+1}+1$. Очевидно (см. ([8])), что $|\Omega(n)|=2^{n/2}+1$ и $\Omega(n)$—циклическая подгруппа мультипликативной группы ненулевых элементов поля $GF(2^n)$, т. е. $\Omega(n)=\{1, \eta_1, \eta_1^2, \ldots, \eta_1^{2^{n/2}}\}$, где $\eta_1$—примитивный корень $(2^{n/2}+1)$-ой степени из единицы. Кроме того, степень расширения $GF(2)(\eta_1)$ над $GF(2)$ равна $n$, т. е. простое расширение $GF(2)(\eta_1)$ совпадает с $GF(2^n)$.

Покажем теперь, что $\Omega(n)$ не содержит смежных классов размерности 2.

Пусть $x$, $y$, $z$, $w$—различные элементы из $\Omega(n)$ и $x+y+z+w=0$, т. е. они образуют смежный класс размерности 2. Из $x+y+z+w=0$ следует $x+y+z=w\in\Omega(n)$ и $(x+y+z)^{2^{n/2}+1}=1$. Тогда

$1=(x+y+z)(x+y+z)^{2^{n/2}}=(x+y+z)(x^{2^{n/2}}+y^{2^{n/2}}+z^{2^{n/2}})$ и ввиду $x, y, z\in\Omega(n)$ получаем $x^{2^{n/2}}=x^{-1}$, $y^{2^{n/2}}=y^{-1}$, $z^{2^{n/2}}=z^{-1}$. Итак, $(x+y+z)\times$ $\times(x^{-1}+y^{-1}+z^{-1})=1$.

Пусть $x=\eta^\alpha$, $y=\eta^\beta$, $z=\eta^\gamma$, где $0\leqslant\alpha<\beta<\gamma\leqslant 2^{n/2}$. Тогда $(\eta^\alpha+\eta^\beta+$ $+\eta^\gamma)(\eta^{-\alpha}+\eta^{-\beta}+\eta^{-\gamma})=1$ и $1+\eta^{\alpha-\beta}+\eta^{\alpha-\gamma}+\eta^{\beta-\alpha}+1+\eta^{\beta-\gamma}+\eta^{\gamma-\alpha}+\eta^{\gamma-\beta}+1=1$, $\eta^{\alpha-\beta}+\eta^{\beta-\alpha}+\eta^{\alpha-\gamma}+\eta^{\gamma-\alpha}+\eta^{\beta-\gamma}+\eta^{\gamma-\beta}=0$. Обозначим $p=\beta-\alpha$, $q=\gamma-\alpha$. Ясно, что $p<q$ и $0<p<q\leqslant 2^{n/2}$. Далее получаем $\eta^{-p}+\eta^p+\eta^{-q}+\eta^q+$ $+\eta^{p-q}+\eta^{q-p}=0$. Умножим предыдущее равенство на $\eta^{p+q}$ и получим

$$\eta^q+\eta^{2p+q}+\eta^p+\eta^{p+2q}+\eta^{2p}+\eta^{2q}=0,$$

$$(\eta^p+\eta^q)+\eta^{p+q}(\eta^p+\eta^q)+(\eta^p+\eta^q)^2=0,$$

$$(\eta^p+\eta^q)(1+\eta^p+\eta^q+\eta^{p+q})=0, \quad \text{но}$$

$1+\eta^p+\eta^q+\eta^{p+q}=(1+\eta^p)(1+\eta^q)$, следовательно получаем $(\eta^p+\eta^q)(1+$ $+\eta^p)(1+\eta^q)=0$, что невозможно, ибо $p\neq q$ и $0<p<q\leqslant 2^{n/2}$, а $\eta$—примитивный корень $(2^{n/2}+1)$-ой степени из единицы.

Таким образом, $\Omega(n)$ не содержит смежного класса размерности 2 при $n\equiv 0 \bmod 2$.

При $n\equiv 1 \bmod 2$ аналогичное построение производится для $GF(2^{n-1})$, а далее множество $\Omega(n-1)$ погружается в один из $(n-1)$-мерных интервалов в $E^n$ и $|\Omega(n-1)|=\frac{2^{n/2}}{\sqrt{2}}+1$.

Следовательно, $k(n) = c \cdot 2^{n/2}+1$, где $c=1$ при $n\equiv 0 \bmod 2$ и $c=\frac{1}{\sqrt{2}}$ при $n\equiv 1 \bmod 2$.

Теорема доказана.

Замечание 1. При $n\equiv \bmod 4$ к $\Omega(n)$ можно добавить также и 0, ибо при $x+y+z=0$ для $x, y, z\in\Omega(n)$ имеем $x+y\in\Omega(n)$ и $(x+y)^{2^{n/2}+1}=1$, т. е. $(x+y)(x^{-1}+y^{-1})=1$.

Пусть $x=\gamma_1^{\alpha}$, $y=\gamma_1^{\beta}$, $0\leqslant\alpha<\beta\leqslant 2^{n/2}$ тогда $(\gamma_1^{\alpha}+\gamma_1^{\beta})(\gamma_1^{-\alpha}+\gamma_1^{-\beta})=1$ и $1+\gamma_1^{\alpha-\beta}+\gamma_1^{\beta-\alpha}+1=1$. Далее $\gamma_1^{\alpha-\beta}+\gamma_1^{\beta-\alpha}=1$ умножим на $\gamma_1^{\beta-\alpha}$ и получим $1+\gamma_1^{\beta-\alpha}+\gamma_1^{2(\beta-\alpha)}=0$. Последнее равенство умножим на $\gamma_1^{\beta-\alpha}+1\neq 0$, тогда получим $\gamma_1^{3(\beta-\alpha)}+1=0$, следовательно, $3(\beta-\alpha)\equiv 0 \bmod (2^{n/2}+1)$.

Однако наименьшее $p$ такое, что $3p\equiv 0 \bmod (2^{n/2}+1)$ — это $p=\frac{2^{n/2}+1}{(2^{n/2}+1,3)}$, где $(2^{n/2}+1,3)$ — наибольший общий делитель чисел $2^{n/2}+1$ и 3. Поэтому ввиду $n\equiv 0 \bmod 4$ имеем $\frac{n}{2}\equiv 0 \bmod 2$ и $2^{n/2}+1$ не делится на 3. Следовательно, $p=2^{n/2}+1$, но $0<\beta-\alpha<p=2^{n/2}+1$ и $\gamma_1^{3(\beta-\alpha)}\neq 1$ и получено противоречие.

Замечание 2. Естественным образом получается также решение двойственной задачи о „прокаливании" двумерных смежных классов в $E^n$. В самом деле, пусть $l(n)$ — наименьшая мощность множества вершин из $E^n$, пересекающегося с любым двумерным смежным классом в $E^n$. Очевидно, что $k(n)+l(n)=2^n$, поэтому $2^n-O(2^{n/2})\leqslant l(n)\leqslant 2^n$, т. е. получается асимптотика для $l(n)$.

3. Доказанная в предыдущем пункте теорема свидетельствует о том, что кратчайшее покрытие множества единиц функции, состоящего только лишь из одномерных смежных классов, имеет длину порядка $O(2^{n/2})$. Следовательно, функция наибольшей сложности в классе л. д. н. ф. не может состоять из смежных классов наименьшей возможной размерности, ибо, как это следует из (²), почти все функции из $P(n)$ имеют л. д. н. ф.-реализацию длины порядка не меньшего, чем $O\left(\frac{2^n}{n\log_2 n}\right)$. Таким образом, получено еще одно существенное отличие задачи кратчайшей л. д. н. ф.-реализации функции из $P(n)$ от задачи реализации булевых функций обычными д. н. ф. Следует также отметить, что функция, построенная в теореме (с множеством единиц, совпадающим с $\Omega(n)$—множеством корней $(2^{n/2}+1)$-ой степени из единицы в $GF(2^n)$), является прямым аналогом „счетчика четности" для класса д. н. ф. над линейными функциями.

Автор благодарит чл.-корр. АН СССР Ю. И. Журавлева за полезные обсуждения работы.

Ереванский государственный университет

Ա. Ա. ԱԼԵՔՍԱՆՅԱՆ

# Դծային ֆունկցիաների նկատմամբ դիզյունկտիվ նորմալ ձևերով բուլյան ֆունկցիաների իրականացման բարդության հետ կապված որոշ էքստրեմալ խնդրի վերաբերյալ

*Դիցուք $E^n$-ը $n$-չափանի միավոր խորանարդի գագաթների բազմությունն է, որը դիտարկվում է որպես $n$-չափանի գծային տարածություն $GF(2)$ դաշտի նկատմամբ։ Նշանակենք՝ $k(n)=\max|A|$, որտեղ $A\subseteq E^n$ և $\alpha, \beta, \gamma\in A\Rightarrow \alpha+\beta+\gamma\in A$:*

*Աշխատանքում ապացուցված է, որ $c\cdot 2^{n/2}+1\leqslant k(n)\leqslant\sqrt{2}\cdot 2^{n/2}+0{,}5$, որտեղ $c=1$ երբ $n\equiv 0 \bmod 2$, և $c=\frac{1}{\sqrt{2}}$ երբ $n\equiv 1 \bmod 2$:*

## ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. А. Алексанян*, ДАН АрмССР, т. 84, № 5, с.195—197 (1987). [2] *А. А. Алексанян*, ДАН АрмССР, т. 87, № 1, с. 5—9 (1988). [3] *А. А. Алексанян*, ДАН СССР, т. 304, № 4, с. 781—784 (1989). [4] *А. А. Алексанян*, Кибернетика, № 1, с. 9—14, 1989. [5] *А. А. Алексанян*, ДАН АрмССР, т. 86, № 5, с. 213—217 (1988). [6] *А. А. Алексанян*, Журн. вычислительной математики и мат. физики, т. 29, № 11 (1989). [7] Дискретная математика и математические вопросы кибернетики, т. I, Наука, М., 1974. [8] *Р. Лидл, Г. Нидеррайтер*. Конечные поля, в 2-х томах, Мир, М., 1988.