ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXXVI 1988 5

УДК 519.7

ПРИКЛАДНАЯ МАТЕМАТИКА

А. А. Александян

Нельсоновские системы булевых уравнений и функции с малым числом нулей

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 12/XI 1987)

Одной из широко распространенных на практике моделей алгоритмов распознавания является модель алгоритмов с представительными наборами. Важной и трудоемкой частью алгоритмов данной модели является реализация с помощью дизъюнктивной нормальной формы (д. н. ф) функции, заданной таблицей нулей и эквивалентной произведению левых частей Нельсоновской системы булевых уравнений:

$$x_1^{\beta_{i1}} \vee x_2^{\beta_{i2}} \vee \ldots \vee x_n^{\beta_{in}} = 1,\ i = 1, 2, \ldots, k, \text{ где } x^{\beta} = \begin{cases} x, & \beta = 1 \\ x+1, & \beta = 0 \end{cases} \qquad (1)$$

(Здесь и далее $+$ обозначает сложение по $\mathrm{mod}\,2$.)

Эта задача исследована в работах ([1, 2]), из которых следует возможность практического уменьшения количества уравнений в системе (1) без существенного увеличения числа членов в уравнениях.

В настоящей работе рассмотрен новый способ реализации функций с малым числом нулей, позволяющий уменьшать количество уравнений Нельсоновской системы не менее, чем в 10 раз.

Все не определяемые понятия теории д. н. ф. изложены в ([3]). Через E^n обозначается множество вершин n-мерного единичного куба $\{x = (x_1, x_2, \ldots, x_n) | x_i \in \{0, 1\},\ i = 1, 2, \ldots, n\}$. Множество булевых функций, зависящих от n переменных, обозначается через $P(n)$. Множество единиц функции f — это $N_f = \{x \in E^n | f(x) = 1\}$. Множество нулей — это $E^n \setminus N_f$.

Определение. Функция $f \in P(n)$ называется *линеаризируемой*, если $f = \prod_i g_i$, где g_i — линейная функция переменных $x_1, x_2, \ldots, x_n$ над полем Галуа $GF(2)$.

Класс линеаризируемых функций обозначается через $\Pi L(n)$.

Пусть $M_f = \{g | g$ — линейная функция и $g \cdot f = 0\}$ — линейное подпространство $n+1$-мерного пространства линейных над $GF(2)$ функций.

Определение. Пусть $f \in \Pi L(n)$. Размерность $\dim f$ определяется как число $n - \dim M_f$.

Предложение. *Пусть $f \in \Pi L(n)$, тогда кратчайшее в смысле*

количества сомножителей представление f имеет вид $f=\prod_{g\in B}(g+1)$, *где* B*—базис* M_f, *а* $|N_f|=2^{\dim f}$.

Определение. Выражение $f_1\vee f_2\vee\ldots\vee f_m$ называется *линеаризированной дизъюнктивной нормальной формой* (л. д. н. ф.), если $f_i\in\Pi L(n)$. Число m называется длиной л. д. н. ф.

Следует особо отметить, что длина л. д. н. ф. инвариантна относительно действия аффинной группы преобразований вида $y=Ax+b$ вершин куба E^n.

Задача реализации булевой функции f, заданной матрицей нулей, ставится следующим образом. Задана бинарная матрица M_0 размера $k\times n$ с попарно различными строками (каждая строка соответствует нулю функции f). Требуется построить л. д. н. ф. возможно меньшей длины, реализующую функцию f. Очевидно, что f эквивалентна произведению левых частей Нельсоновской системы (1), для которой $(\beta_{i1}, \beta_{i2}, \ldots, \beta_{in})$—$i$-ая строка матрицы M_0.

Пусть $m\leqslant n+1$.

Определение. Система векторов $\{x_1, x_2, \ldots, x_m\}\subseteq E^n$ находится в общем положении, если из условий $\lambda_1x_1+\lambda_2x_2+\ldots+\lambda_mx_m=0$ и $\lambda_1+\lambda_2+\ldots+\lambda_m=0$ следует: $\lambda_1=\lambda_2=\ldots=\lambda_m=0$, где $\lambda_i\in\{0, 1\}$. Эквивалентным является следующее определение: векторы $x_1, x_2, \ldots, x_m$ находятся в общем положении, если размерность наименьшей в $\Pi L(n)$ функции, содержащей $\{x_1, x_2, \ldots, x_m\}$, равна $m-1$.

Опишем метод л. д. н. ф.-реализации функции f, заданной матрицей k нулей M_0.

Пусть $r=\operatorname{rank}M_0$, тогда $\lceil\log_2k\rceil\leqslant r\leqslant k$, где $\lceil a\rceil$—наименьшее целое, не меньшее a. Для простоты предположим, что линейно-независимы первые столбцы в M_0. Столбцу с номером i сопоставим переменную x_i. Все столбцы с номерами, большими r, представляются в виде линейных комбинаций первых r столбцов. Поэтому строки матрицы M_0 удовлетворяют системе линейных уравнений над $GF(2)$: $x_{r+i}=a_{i1}x_1+\ldots+a_{ir}x_r$, $i=1, 2, \ldots, n-r$, $a_{ij}\in\{0, 1\}$. Ясно, что $g=\prod_{i=1}^{n-r}(a_{i1}x_1+\ldots+a_{ir}x_r+x_{r+i}+1)$—функция из $\Pi L(n)$, содержащая M_0. Поэтому $N_{k+1}\subseteq E^n\setminus M_0$ и $g+1\equiv\bigvee_{i=1}^{n-r}(a_{i1}x_1+\ldots+a_{ir}x_r+x_{r+i})$ покрывает часть N_f. Для получения покрытия N_f достаточно покрыть $N_k\setminus M_0$. Но N_k—смежный класс размерности r, и он изоморфен E^r, следовательно, задача сводится к построению л. д. н. ф. функции, зависящей от переменных $x_1, x_2, \ldots, x_r$, имеющей матрицу нулей, состоящую из первых r столбцов матрицы M_0.

Обозначим через $L(n, r, k)$ наибольшую длину кратчайшей л. д. н. ф., реализующей функцию от n переменных с k нулями, ранг матрицы нулей которой равен r. Из вышеизложенного следует, что

$$L(n, r, k)\leqslant n-r+L(r, r, k) \text{ и } L(n, r, k)\leqslant n-r+\lceil 2^{r-1}-\frac{k}{2}\rceil.$$

Последнее неравенство следует из того факта, что в $N_k\setminus M_0$ содер-

жится 2^r-k векторов, а всякие два вектора образуют функцию из $\Pi L(n)$.

Всюду далее через $\varphi(n)$ обозначается функция, сколь угодно медленно стремящаяся к $+\infty$ при $n\to+\infty$.

Теорема 1. *Если* $r\leqslant\log_2 n-\varphi(n)$ *или* $2^r-k=o(n)$, *то*

$$L(n,\ r,\ k)\leqslant n(1+o(1)).$$

Пусть $k\leqslant n+1$ и матрица нулей M_0 состоит из строк, находящихся в общем положении. Тогда подходящим аффинным преобразованием подматрица матрицы M_0, состоящая из $k-1$-го линейно-независимого столбца, переводится в матрицу, состоящую из k различных строк, содержащих не более одной 1. Следовательно, л. д. н. ф. функции f имеет длину не более, чем $n-(k-1)+d$, где d—длина л. д. н. ф. функции h, зависящей от $k-1$ переменной, равной 1 на всех векторах длины $k-1$, содержащих не менее двух 1. Нетрудно видеть, что $h=x_1x_2\vee(x_1+x_2)x_3\vee(x_1+x_2+x_3)x_4\vee\ldots\vee(x_1+\ldots+x_{k-2})x_{k-1}$ и $d=k-2$. Следовательно, длина л. д. н. ф. функции f равна $n-1$.

Теорема 2. *Если* $f\in P(n)$ *и имеет* $k\leqslant n+1$ *нулей, находящихся в общем положении, то* f *реализуется л. д. н. ф. длины* $n-1$.

Рассмотрим теперь функции $f\in P(n)$ с k нулями при $k\leqslant 10$. Ясно, что длина $l(f)$ л. д. н. ф. функции f не больше $n-r+d$, где $r=\operatorname{rank} M_0$, d—длина л. д. н. ф. функции $h\in P(r)$, множество нулей которой содержит все r-мерные векторы с не более, чем одной 1. Ввиду того, что $\lceil\log_2 k\rceil\leqslant r\leqslant k$, для получения $l(f)$ необходимо рассмотреть следующие случаи:

а) $k=1$, тогда $h=x_1\vee x_2\vee\ldots\vee x_r$ и $l(f)=n$;

б) $k=2, 3$, векторы находятся в общем положении и $l(f)=n-1$;

в) $k=4$, при $r=3$—общее положение— $l(f)=n-1$, при $r=2$ нули составляют подпространство размерности 2, поэтому $l(f)=n-2$;

г) $k=5$, при $r=4$—общее положение— $l(f)=n-1$, а при $r=3$ имеем $2^r-k=3$, для покрытия достаточно 2 смежных класса и $l(f)=n-1$;

д) $k=6$, при $r=5$—общее положение— $l(f)=n-1$, при $r=4$ в E^4 можно выбрать 3 смежных класса, покрывающих N_h и $l(f)=n-1$, при $r=3$ имеем $2^r-k=2$ и $l(f)=n-2$:

е) $k=7$, при $r=6$—общее положение— $l(f)=n-1$, при $r=5$ в E^5 можно выбрать 5 смежных классов, покрывающих N_h и $l(f)=n$, при $r=4$ в E^4 N_h покрывают 3 класса и $l(f)=n-1$, при $r=3$ имеем $2^r-k=1$ и $l(f)=n-2$.

Для $k=8, 9, 10$ был использован алгоритм построения л. д. н. ф. функции, заданной таблицей нулей. $PL/1(O)$-реализация этого алгоритма была применена ко всем функциям h, получающимся при $k=8, 9, 10$ и не переводящимся друг в друга перестановкой переменных. При $k=8$ таких функций имеется 37, при $k=9$—107, при $k=10$—582. Получены следующие результаты:

а) $k=8$, при $r=4$—$l(f)=n-1$, при $r=5$—$l(f)=n+1$, при $r=6$ —$l(f)=$

$=n+1$, при $r=3$ имеем $2^r-k=0$ и $l(f)=n-3$, при $r=7$—общее положение $-l(f)=n-1$;

б) $k=9$, при $r=4$ имеем $2^r-k=7$ и для покрытия N_h достаточно 4 члена— $l(f)=n$, при $r=5$ — $l(f)=n+1$, при $r=6$ — $l(f)=n+2$, при $r=7$ — $l(f)=n+1$, при $r=8$ — общее положение— $l(f)=n-1$;

в) $k=10$, при $r=4$ имеем $2^r-k=6$ и достаточно для покрытия N_h всего 3 члена и $l(f)=n-1$, при $r=5$ — $l(f)=n+1$, при $r=6$— $l(f)=n+2$, при $r=7$ — $l(f)=n+2$, при $r=8$ — $l(f)=n+1$, при $r=9$—общее положение — $l(f)=n-1$.

Итак, всякая Нельсоновская система может быть сокращена в 10 раз, при этом количество членов в одном уравнении не больше, чем $n+2$.

Изложим теперь „частотное" решение поставленной задачи.

Теорема 3. *Пусть* $m\cdot k=o(2^{n/2})$, $m=o(2^{n-k})$ *и* $k\leqslant n$. *Тогда почти все бинарные матрицы, состоящие из* $m\cdot k$ *строк и* n *столбцов, состоят из последовательных групп из* k, *находящихся в общем положении строк.*

Следствие. а) *если* $k\leqslant n-\varphi(n)$, *то почти все наборы из* k *векторов находятся в общем положении;*

б) *если* $k=\mathrm{const}$, *то утверждение теоремы* 3 *верно при* $m=o(2^{n/2})$.

Отсюда получаем, что почти все функции $f\in P(n)$ с $k\leqslant n-\varphi(n)$ нулями реализуются л. д. н. ф. длины не более, чем $n-1$. Для любой постоянной k количество уравнений системы (1) может быть почти всегда уменьшено в k раз. если общее количество уравнений системы имеет порядок $o(2^{n/2})$, причем количество членов в новых уравнениях не больше, чем $n-1$.

Сравним теперь полученные результаты с результатами работ [1,2] относительно д. н. ф.-реализации функций с малым числом нулей.

В [1] показано, что при $k\leqslant\log_2 n-\varphi(n)$ длина д. н. ф. функции f асимптотически равна n. Следствие теоремы 3 улучшает эту оценку. Далее, в [2] отмечается. что л. н. ф.-реализация почти всегда неэффективна, в то время как л. д. н. ф.-реализация почти всегда дает длину $n-1$. Более того, почти всегда количество уравнений системы (1) уменьшается в любое постоянное число раз. В [3] получено, что при л. н. ф.-реализации получаются формулы длины $n+m(k)$, где $m(k)$ принимает следующие значения:

$k=4, 5, 6, 7, 8, 9, 10$;

$m(k)=4, 14, 31, 66, 133, 271, 537$.

В случае л. д. н. ф. имеем: $m(k)=-1, -1, -1, 0, 1, 2, 2$. Т. е. система (1) практически уменьшается в 10 раз. И, наконец, оценка для $L(n, r, k)$ в худшем случае равна $n-k+\left\lceil 2^{k-1}-\frac{k}{2}\right\rceil$, что лучше соответствующей оценки для длины л. н. ф.—$n+2^{k-1}+2^{\left\lfloor\frac{k}{2}\right\rfloor}+2^{\left\lfloor\frac{k}{2}\right\rfloor}-3$.

Ереванский государственный университет

Ա. Ա. ԱԼԵՔՍԱՆՅԱՆ

Բուլյան հավասարումների նելսոնի համակարգեր և վտմ բահակությամբ զրոնեով ֆունկցիաներ

Աշխատանքում հետազոտված են Նելսոնի համակարգերի կրճատման և նրանց համապատասխանող բուլյան ֆունկցիաների հարակից դասերի միավորումով ներկայացման հարցերը։ Յույց է տրված, որ կամայական Նելսոնի համակարգը կարելի է կրճատել 10 անգամ։ Եթե համակարգը կազմված է $m \cdot k = o(2^{n/2})$ հավասարումներից և $m = o(2^{n-k})$, $k \le n$, ապա համարյա միշտ այն կարելի է կրճատել k անգամ։ Եթե բուլյան ֆունկցիաների զրոները գտնվում են ընդհանուր վիճակում, ապա այն ներկայացվում է $n-1$ հարակից դասերի միավորումով։ Համարյա բոլոր $k < n - \varphi(n)$ որ պարունակող բուլյան ֆունկցիաները ներկայացվում են $n-1$ հարակից դասերի միավորումով, այստեղ $\varphi(n) = o(n)$.

ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1 *Ю. И. Журавлев, А. Ю. Коган*, ДАН СССР, т. 285, № 4, с. 795—799 (1985).
2 *Ю. И. Журавлев, А. Ю. Коган*, ЖВМ и МФ, т. 26, № 8, с. 1243—1249 (1986).
3 *Ю. И. Журавлев*. Проблемы кибернетики, вып. 8, с. 5—44 (1962). 4 Дискретная математика и математические вопросы кибернетики. Наука, М., т. 1, 1974.