МЕТОДЫ ДИСКРЕТНОГО АНАЛИЗА
В ТЕОРИИ ГРАФОВ И СХЕМ

Сборник трудов
1985 г. Института математики СО АН СССР Выпуск 42

УДК 51.0116

МОДИФИКАЦИЯ МЕТОДА В.М.ХРАПЧЕНКО И ПРИМЕНЕНИЕ ЕЕ К ОЦЕНКАМ СЛОЖНОСТИ Π-СХЕМ ДЛЯ КОДОВЫХ ФУНКЦИЙ

К.Л.Рычков

Статья посвящена развитию метода В.М.Храпченко [2] для получения нижних оценок сложности Π-схем. В предлагаемой новой и более общей форме метод В.М.Храпченко развит по двум взаимосвязанным направлениям. При сохранении основных идей этого метода, во-первых, в более простой и общей форме представлено то, к чему сводится в нем оценка сложности схем, т.е. более отчетливо выявлено, что в этом методе оценивается.

Пусть N^1 и N^0 – соответственно множество единичных и нулевых вершин булевой функции $f(x_1,\dots,x_n)$. Задача о нижней оценке сложности функции $f(x_1,\dots,x_n)$ в классе Π-схем сведена к задаче о нижней оценке числа L таких подмножеств $T_i = N_i^0 \times N_i^1$ множества $N^0 \times N^1$ для всех (0-1)-пар функции $f(x_1,\dots,x_n)$, которые обладают следующими свойствами:

1) $N^0 \times N^1 = \bigcup\limits_{i=1}^{L} T_i$;

2) при $i \neq j$, $T_i \cap T_j = \varnothing$;

3) для любого множества T_i существует такое $j\,(1 \leq j \leq n)$, что в любой паре (α,β) из T_i составляющие ее вершины $\alpha = (\alpha_1,\dots,\alpha_n)$ и $\beta = (\beta_1,\dots,\beta_n)$ различаются по j-й координате ("локальная самосопряженность" множеств T_i).

Во-вторых, достигнут некоторый прогресс в том, как получать оценки для числа L. В общей форме к этому не видно никаких подходов. Метод В.М.Храпченко можно трактовать как весьма интересный способ оценки L за счет сужения множества $N^0 \times N^1$ до некоторого его специального подмножества R. Упомянутый прогресс состоит в обнаружении возможности варьировать это сужение с учетом специфики рассматриваемых булевых функций и получать отсюда нетривиальные нижние оценки таких булевых функций, для которых метод В.М.Храпченко в исходной форме давал лишь тривиальные оценки.

В случае, когда в качестве R взято множество (0-I)-ребер, выведена известная формула В.М.Храпченко. При получении нижних оценок для кодовых функций $(n, 2t+1)$ -кодов (здесь $2t+1$ - кодовое расстояние) в качестве R выбрано множество (0-I)-пар с расстоянием, не превышающим $t+1$. В результате найдены формулы, которые дают для достаточно мощных кодов (близких по мощности к плотно упакованным кодам) квадратичные по n нижние оценки. В частности, для кодовой функции $\varphi(x_1, \dots, x_n)$, отвечающей произвольному плотно упакованному $(n,3)$-коду, имеет место нижняя оценка $L_\pi(\varphi(x_1, \dots, x_n)) \geqslant \frac{(n+1)^2}{4}$. Такую же нижнюю оценку, но только для некоторых специальных плотно упакованных $(n,3)$ -кодов ранее получил А.К.Пулатов [I].

Пусть S - произвольная Π -схема. Обозначим через $L(S)$ число контактов в схеме и занумеруем все контакты от I до $L(S)$. Множество контактов, входящих в простую цепь, соединяющую полюса схемы S, будем называть ц е п ь ю. С е ч е н и е м схемы S называется множество контактов схемы, которое содержит хотя бы по одному контакту из каждой цепи. Сечение называется т у п и к о в ы м, если любое его собственное подмножество не является сечением. Обозначим через A множество тупиковых сечений схемы S, через B - множество цепей схемы S. Как показано в [3], в Π -схеме каждая цепь и каждое тупиковое сечение имеют ровно один общий контакт. Это означает, что на множестве пар $A \times B$ задано следующее отношение эквивалентности. Пусть $(\alpha_1, \beta_1) \in A \times B$ и $(\alpha_2, \beta_2) \in A \times B$. Тогда $(\alpha_1, \beta_1) \sim (\alpha_2, \beta_2)$ в том и только в том случае, если в схеме S имеется такой контакт x, что $\alpha_1 \cap \beta_1 = x$ и $\alpha_2 \cap \beta_2 = x$.

В порождаемом этой эквивалентностью разбиении множества $A \times B$ на классы эквивалентности совокупность классов $\mathcal{P} = (\Pi_1, \Pi_2, \ldots)$ находится во взаимно-однозначном соответствии со множеством контактов схемы S (классу Π_i соответствует кон акт с номером i). Так что можно написать $A \times B = \Pi_1 \cup \ldots \cup \Pi_{L(S)}$. Более того, для любого $i = 1, \ldots, L(S)$ имеем $\Pi_i = A_i \times B_i$, где A_i – множество тупиковых сечений, содержащих контакт с номером i, B_i – множество цепей, содержащих контакт с номером i. Таким образом,

$$A \times B = \bigcup_{i=1}^{L(S)} (A_i \times B_i)$$

и $(A_i \times B_i) \cap (A_j \times B_j) = \varnothing$ при $i \neq j$.

Пусть $f(x_1, \ldots, x_n)$ – произвольная булева функция и П-схема S реализует эту функцию. Обозначим через N^1 множество вершин единичного n-мерного куба, на которых $f(x_1, \ldots, x_n)$ равна I, и через N^0 – множество вершин единичного n-мерного куба, на которых $f(x_1, \ldots, x_n)$ равна 0. Каждой вершине $(\sigma_1, \ldots, \sigma_n) \in N^1$ поставим в соответствие (какую-нибудь одну) цепь схемы S, все контакты которой замкнуты на наборе $(\sigma_1, \ldots, \sigma_n)$. Каждой вершине $(\sigma_1, \ldots, \sigma_n) \in N^0$ поставим в соответствие (какое-нибудь одно тупиковое сечение схемы S, все контакты которого разомкнуты на наборе $(\sigma_1, \ldots, \sigma_n)$. Очевидно, такое соответствие всегда можно установить. Пользуясь им, перенесем разбиение с $A \times B$ на $N^0 \times N^1$.

Рассмотрим множество $N^0 \times N^1$, элементы которого будем называть (0-I)-парами функции $f(x_1, \ldots, x_n)$. Обозначим через T_i множество таких (0-I)-пар $\cancel{(\alpha, \beta) \in N^0} \times N^1$, что вершине α поставлено в соответствие тупиковое сечение из A_i, а вершине β – цепь из B_i. Так как множество $A \times B$ разбито на классы эквивалентности

$$A \times B = \bigcup_{i=1}^{L(S)} (A_i \times B_i),$$

то множество (0-I)-пар функции $f(x_1, \ldots, x_n)$ разбито на непересекающиеся подмножества

$$N^0 \times N^1 = \bigcup_{i=1}^{L(S)} T_i .$$

Поскольку множество классов эквивалентности $\{A_i \times B_i\}$ находится во взаимно-однозначном соответствии со множеством контактов схемы S, то совокупность множеств T_i также находится во взаимно-однозначном соответствии со множеством контактов схемы S. Более того, для каждого $i = 1, \dots, L(S)$ имеем $T_i = N_i^0 \times N_i^1$, где $N_i^0 = \{\alpha \mid (\alpha, \beta) \in T_i\}$, $N_i^1 = \{\beta \mid (\alpha, \beta) \in T_i\}$.

Справедливо следующее утверждение: для каждого непустого множества T_i существует такое j $(1 \leq j \leq n)$, что в любой паре (α, β), принадлежащей T_i, составляющие ее вершины $\alpha = (\alpha_1, \dots, \alpha_n)$ и $\beta = (\beta_1, \dots, \beta_n)$ различаются по j-й координате. Действительно, пусть контакт вида x_j^σ имеет номер i и пусть $(\alpha, \beta) \in T_i$. Тогда вершине α соответствует тупиковое сечение, содержащее контакт с номером i, и все контакты этого сечения разомкнуты на наборе α. Но тогда разомкнут на наборе α и контакт вида x_j^σ, имеющий номер i, т.е. $\alpha_j = \bar{\sigma}$. Аналогично вершине β соответствует цепь, содержащая контакт с номером i, и все вершины этой цепи замкнуты на наборе β. Значит, замкнут на наборе β контакт вида x_j^σ, т.е. $\beta_j = \sigma$. Этим утверждение доказано.

Таким образом, имеем: Π-схема S, реализующая функцию $f(x_1, \dots, x_n)$, индуцирует разбиение множества $N^0 \times N^1$(0-I)-пар функции $f(x_1, \dots, x_n)$ на подмножества $N_i^0 \times N_i^1$, обладающие следующими тремя свойствами:

I) $N^0 \times N^1 = \bigcup_{i=1}^{L(S)} (N_i^0 \times N_i^1)$;

2) при $i \neq j$ $(N_i^0 \times N_i^1) \cap (N_j^0 \times N_j^1) = \varnothing$;

3) для каждого непустого множества $N_i^0 \times N_i^1$ существуют такие j и σ $(1 \leq j \leq n,\ \sigma = 0$ или $\sigma = 1)$, что для любой пары (α, β), принадлежащей $N_i^0 \times N_i^1$, имеют место $\alpha_j = \bar{\sigma}$, $\beta_j = \sigma$.

Кроме того, существует инъективное отображение множества непустых множеств $N_i^0 \times N_i^1$ в множество контактов Π-схемы S.

В итоге задачу о нижней оценке сложности Π-схемы S, реализующей булеву функцию $f(x_1, \dots, x_n)$, можно свести к задаче о нижней оценке числа L непустых подмножеств $N_i^0 \times N_i^1$ множества $N^0 \times N^1$, обладающих перечисленными тремя свойствами.

Для вывода известной формулы В.М.Храпченко [I] рассмотрим множество (0-I)-ребер функции $f(x_1, \dots, x_n)$, т.е. множество таких (0-I)-пар (α, β) , что вершины α и β различаются только в одном разряде. Обозначим это множество через R . Далее, пусть

$$N^0 \times N^1 = \bigcup_{i=1}^{L} (N_i^0 \times N_i^1) -$$

произвольное разбиение всех (0-I)-пар функции $f(x_1,\dots,x_n)$, удовлетворяющее свойствам I,2,3. Оценим снизу число L . Поскольку $R \in N^0 \times N^1$, то множество R также разбито на подмножества $R_i = R \cap (N_i^0 \times N_0^1)$, обладающие следующими свойствами:

а) $R = \bigcup_{i=1}^{L} R_i$ и $R_i \cap R_j = \emptyset$ при $i \neq j$,

б) $R_i^0 \times R_i^1 \subset N_i^0 \times N_i^1$,

в) $|R_i^0| = |R_i^1| = |R_i|$,

где R_i^0 - множество нулевых вершин, инцидентных (0-I)-ребрам из R_i ; R_i^1 - множество единичных вершин, инцидентных (0-I)-ребрам из R_i .

Свойства "а" и "б" очевидны.

Проверим справедливость равенств "в". Действительно, R_i состоит из (0-I)-ребер и $R_i \subset N_i^0 \times N_i^1$, поэтому свойство 3, которому удовлетворяет $N_i^0 \times N_i^1$, означает, что каждая вершина из R_i^0 инцидентна ровно одному (0-I)-ребру, принадлежащему R_i, и каждая вершина из R_i^1 инцидентна ровно одному (0-I)-ребру, принадлежащему R_i . Откуда заключаем справедливость равенств "в".

Учитывая "б", получаем

$$\sum_{i=1}^{L} |R_i^0 \times R_i^1| \leq \sum_{i=1}^{L} |N_i^0 \times N_i^1| = |N^0 \times N^1| .$$

Далее, учитывая "в", получаем

$$\sum_{i=1}^{L} |R_i|^2 \leq |N^0|\ |N^1| .$$

Применяя к левой части неравенство Коши-Буняковского и учитывая "а", получаем следующее неравенство:

$$L \geq \frac{|R|^2}{|N^0|\ |N^1|}$$ — это и есть формула В.М.Храпченко.

Аналогично можно получить обобщение формулы В.М.Храпченко для кодовых функций, однако множество R будет теперь иным.

Пусть $f(x_1,\dots,x_n)$ - кодовая функция $(n, 2t+1)$-кода ($2t+1$ - кодовое расстояние). Рассмотрим множество (0-I)-пар функции $f(x_1,\dots,x_n)$ с расстоянием, не превышающим $t+1$, т.е. множество таких (0-I)-пар (α,β) функции $f(x_1,\dots,x_n)$, что вершины α и β различаются в $t+1$ разрядах или меньшем их числе. Обозначим это множество через R. Далее, пусть

$$N^0 \times N^1 = \bigcup_{i=1}^{L} (N_i^0 \times N_i^1) -$$

произвольное разбиение всех (0-I)-пар функции $f(x_1,\dots,x_n)$, удовлетворяющее свойствам I,2,3. Оценим снизу число L. Поскольку $R \subset N^0 \times N^1$, то множество R также разбито на подмножества $R_i = R \cap (N_i^0 \times N_i^1)$, обладающие следующими свойствами:

а) $R = \bigcup_{i=1}^{L} R_i$ и $R_i \cap R_j = 0$ при $i \neq j$;

б) $R_i^0 \times R_i^1 \subset N_i^0 \times N_i^1$;

в) $|R_i^0| = |R_i|$, $|R_i^1| \geq \dfrac{|R_i|}{1+C_{n-1}^1+\dots+C_{n-1}^t}$,

где R_i^0 - множество нулевых вершин, инцидентных (0-I)-парам из R_i; R_i^1 - множество единичных вершин, инцидентных (0-I)-парам из R_i.

Свойства "а", "б" очевидны.

Проверим справедливость "в". Для этого рассмотрим произвольную вершину β, принадлежащую R_i^1. Так как $R_i \subset N_i^0 \times N_i^1$, то в силу свойства 3, которому удовлетворяет $N_i^0 \times N_i^1$, существует такое j $(1 \leq j \leq n)$, что для любой пары $(\alpha,\beta) \in R_i$, инцидентной вершине β, имеет место $\alpha_j \neq \beta_j$. Кроме того, по определению, для любой пары $(\alpha,\beta) \in R_i$ вершины α и β различаются не более чем в $t+1$ разрядах. Следовательно, количество всевозможных пар (α,β), принадлежащих R_i и инцидентных β, не превосходит $1+C_{n-1}^1+C_{n-1}^2+\dots+C_{n-1}^t$. Отсюда следует справедливость неравенства

$$|R_i^1| \geq \frac{|R_i|}{1+C_{n-1}^1+\dots+C_{n-1}^t}.$$

Для доказательства равенства $|R_i^0| = |R_i|$ покажем, что любая вершина α из R_i^0 инцидентна ровно одной паре из R_i. Действительно, предположим, что вершина α принадлежит R_i^0 и инцидентна двум парам из R_i: (α,β) и (α,γ). В силу свойства 3, существует такое $j(1\le j\le n)$, что $\alpha_j \ne \beta_j$ и $\alpha_j \ne \gamma_j$, т.е. $\beta_j = \gamma_j$. Но так как вершины α и γ различаются не более чем в $t+1$ разрядах и вершины α и β различаются не более чем в $t+1$ разрядах, то вершины β и γ различаются не более чем в $2t$ разрядах. Поскольку вершины β и γ принадлежат R_i^1, т.е. являются единичными вершинами, то это противоречит тому, что $f(x_1,\dots,x_n)$ – кодовая функция кода с расстоянием $2t+1$. Таким образом, справедливость равенства $|R_i^0| = |R_i|$ установлена, и свойство "в" полностью доказано.

Учитывая "б", получаем

$$\sum_{i=1}^{L} |R_i^0 \times R_i^1| \le \sum_{i=1}^{L} |N_i^0 \times N_i^1| = |N^0 \times N^1| .$$

Далее, учитывая "в", получаем

$$\frac{1}{1+C_{n-1}^1+\dots+C_{n-1}^t} \cdot \sum_{i=1}^{L} |R_i|^2 \le |N^0|\,|N^1| .$$

Применяя к левой части неравенство Коши-Буняковского и учитывая "а", получаем

$$\frac{1}{1+C_{n-1}^1+\dots+C_{n-1}^t} \cdot \frac{1}{L} \cdot \Big(\sum_{i=1}^{L} |R_i|\Big)^2 \le |N^0|\,|N^1|,$$

откуда

$$L \ge \frac{|R|^2}{(1+C_{n-1}^1+\dots+C_{n-1}^t)|N^0||N^1|} .$$

Отметим, что в отличие от формулы В.М.Храпченко в данном случае R представляет собой множество (0-I)-пар с расстоянием, не превышающим $t+1$. В случае достаточно мощных $(n,2t+1)$ кодов эта формула позволяет получать квадратичные оценки. Например, рассмотрев <u>произвольный</u> плотно упакованный $(n,3)$-код, имеем

$$t=1,\ |N^0| = n\cdot\frac{2^n}{n+1},\ |N^1| = \frac{2^n}{n+1},\ |R| = (n+C_n^2)\cdot\frac{2^n}{n+1} .$$

Следовательно,

$$L \ge \frac{\Big((n+C_n^2)\frac{2^n}{n+1}\Big)^2}{n\cdot n\frac{2^n}{n+1}\cdot\frac{2^n}{n+1}} = \frac{(n+1)^2}{4} .$$

Л и т е р а т у р а

1. ПУЛАТОВ А.К. О сложности реализации характеристических функций плотно упакованных $(n,3)$-кодов в классе П-схем. - В кн.: Дискретный анализ, Новосибирск, 1973, вып. 22, с. 53-56.

2. ХРАПЧЕНКО В.М. Об одном методе получения нижних оценок сложности П-схем. - Мат.заметки, 1971, 10, № 1, с. 83-92.

3. ХРАПЧЕНКО В.М. О сложности реализации линейной функции в классе П-схем. - Мат.заметки, 1971, 9, № 1, с. 35-40.

Поступила в ред.-изд.отдел
29 августа 1985 г.