НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ БИНАРНЫМИ ПРОГРАММАМИ

Окольнишникова Е.А., Новосибирск

Рассматривается реализация булевых функций бинарными программами. Получены нелинейные нижние оценки сложности реализации последовательностей характеристических функций двоичных кодов с большим числом кодовых вершин и с растущим (с ростом n) кодовым расстоянием в классе бинарных программ. В частности, получена оценка $Cn\ln n/\ln\ln n$ для характеристических функций БЧХ-кодов (с кодовым расстоянием $\ln n/\ln\ln n$) в классе бинарных программ [1].

Пусть BP_k - класс бинарных программ, в которых каждый путь содержит не более k проверок одной и той же переменной. Сложность реализации булевых функций f в классе бинарных программ BP_k обозначим через $B_k(f)$, а в классе бинарных программ без ограничений - через $B(f)$. Показано, что при $k = C_1 \ln n/\ln\ln n$, где $0 < C_1 < 1$, существует двоичный линейный код H_{r_n}, для которого $B_k(H_{r_n}) \gtrsim \exp(n^{(1-C_1)/2})$ и $B(H_{r_n}) < 2n^2$, т.е. ограничение на количество проверок в цепи по каждой из переменных дает экспоненциальный, относительно числа переменных, рост сложности бинарной программы.

Кратко поясним основную идею метода получения нижних оценок сложности в классе бинарных программ, предложенную в настоящей работе. Пусть $\mathcal{P}$ - произвольная бинарная программа, реализующая булеву функцию $f(x_1, \ldots, x_n)$. Если для какой-то переменной x_i число проверок по этой переменной в некоторой цепи (пути) превышает k, тогда число вершин бинарной программы $\mathcal{P}$, помеченных переменной x_i, больше чем k. Ясно,

что при большом количестве таких переменных, сложность $B(\mathcal{P})$ бинарной программы должна быть немалой. Если число таких переменных невелико, то, заменяя эти переменные константами, можно от бинарной программы $\mathcal{P}$ перейти к $\mathcal{P}'$, реализующей некоторую подфункцию булевой функции f и принадлежащей классу BP_k. В связи с этим представляет интерес получение нелинейных нижних оценок сложности реализации булевых функций и в классе BP_k.

Через $F_1, F_2, \ldots, F_n, \ldots$ обозначим последовательность характеристических функций для двоичных $(n, 2^{n-1_n}, d_n)$-кодов, где $d_n \geq 2r_n + 1$, а

$$\frac{n^2}{r_n^2 \cdot 2^{\ln/r_n}} \to \infty, \qquad r_n \ln\left[\frac{n^2}{r_n^2 \cdot 2^{\ln/r_n}}\right] \to \infty$$

при $n \to \infty$.

Зафиксируем константу C, $0 < C < 1$, и положим

$$K(n) = C\,\frac{\ln(n^2/(r_n^2 \cdot 2^{\ln/r_n}))}{\frac{2\ln n}{r_n} + \ln\ln(n^2/(r_n^2 \cdot 2^{\ln/r_n}))}. \qquad (1)$$

Ясно, что для последовательности булевых функций $\{F_n\}$ функция $K(n) \to \infty$ при $n \to \infty$.

ТЕОРЕМА 1. *Для сложности реализации последовательности булевых функций* $\{F_n\}$ *в классе бинарных программ имеет место оценка* $B(F_n) \geq C\,K(n)n$, *где* $K(n)$ *задается формулой (1).*

СЛЕДСТВИЕ 1. *Пусть* H_{r_n} *- характеристическая функция БЧХ-кода с параметрами* (n, M_n, d_n), *где*

$d_n \geq 2r_n + 1$, $M_n \geq 2^n/(n+1)^{r_n}$. *Если* $n/r_n^2 \to \infty$ *и* $r_n \to \infty$ *при* $n \to \infty$, *то для любой константы* C, $0 < C < 1$, *справедливы неравенства*

$$C \cdot n \cdot \frac{\ln(n/r_n^2)}{\frac{2\ln n}{r_n} + \ln\ln(n/r_n^2)} \lesssim B(H_{r_n}) \lesssim 2r_n n \ln n.$$

Из этого следствия непосредственно получаем

СЛЕДСТВИЕ 2. *Для характеристической функции БЧХ-кода* $H_{r'_n}$ *при* $r'_n = \ln n/\ln\ln n$ *справедливы оценки*

$$n \frac{\ln n}{\ln\ln n} \lesssim B(H_{r'_n}) \lesssim n \frac{\ln^2 n}{\ln\ln n}.$$

Пусть $\lambda_k(f) = B_k(f)/B(f)$ и $\lambda_k(n) = \max \lambda_k(f)$, где максимум берется по всем булевым функциям от n переменных.

Пусть $K_0(n) = C_1 \ln n/\ln\ln n$, $0 < C_1 < 1$. Рассмотрим последовательность характеристических функций БЧХ-кодов с параметрами $(n, 2^{n-l_n}, 2r_n+1)$, где $r_n = \lceil \sqrt{n/(K_0 e^{3K_0/2} e^2)} \rceil$, $l_n \geq r_n \log_2(n+1)$. Показано, что

$$B_{K_0}(H_{r_n}) \gtrsim \exp(n^{(1-C_1)/2}) n^2$$

и

$$B(H_{r_n}) \leq 2r \cdot \log_2(n+1) < n^2.$$

Отсюда следует

ТЕОРЕМА 2. *Для любой константы* C_1, $0 < C_1 < 1$, *выполняется соотношение*

$$\lambda_{C_1 \ln n / \ln\ln n} \gtrsim \exp(n^{(1-C_1)/2}).$$

Литература

1. ОКОЛЬНИШНИКОВА Е.А. Нижние оценки сложности реализации характеристических функций двоичных кодов бинарными программами //Методы дискретного анализа в синтезе реализаций булевых функций. - Новосибирск, 1991. - Вып. 51. -С. 61-83.

ВЫЧИСЛЕНИЕ СЕРИЙ РЕШЕНИЙ НА ОСНОВЕ ПЕРЕМЕШАННОГО ПОЛНОГО ПЕРЕБОРА ВАРИАНТОВ

Перетятькин М.Г., Алма-Ата

Как известно, встроенный механизм унификации для поиска решений задачи в системах типа "Пролог" основан на полном переборе возможных вариантов значений свободных переменных. В определенном смысле эти варианты просматриваются в лексикографическом порядке до тех пор, пока не будет обнаружен набор значений переменных, удовлетворяющий условиям задачи. Если нужны другие решения, то процесс перебора вариантов продолжается дальше. В том случае, когда задачей определено лишь конечное число вариантов значений переменных, процесс поиска решений в конце концов будет завершен, и все решения будут получены,причем в лексикографическом порядке. При необходимости строгий лексикографический порядок рассмотрения вариантов может быть изменен специальными приемами программирования. При этом следует лишь позаботиться, чтобы ни один из возможных вариантов значений переменных не оказался пропущенным.

Можно указать широкий класс задач, для поиска решений которых целесообразно наличие специальных системных (и даже аппаратных) средств для реализации так называемого *перемешанного (т.е. квазислучайного) полного перебора* вариантов значений для свободных переменных. Сюда относятся, например, задачи, в которых необходимо, по возможности,полное представление решений, однако их общее количество слишком велико и не может быть реально получено.

Дадим некоторое уточнение введенного понятия. Предположим, что $x_1,\ldots,x_2$ являются свободными переменными, для которых задачей задана область возможных значений R, и эта область является конечной, Card(R) = r, $r < w$. Речь идет о том,чтобы включить в систему специальный оператор

$$\mathrm{MIXUP}(X_1,\ldots,X_n), \qquad (1)$$