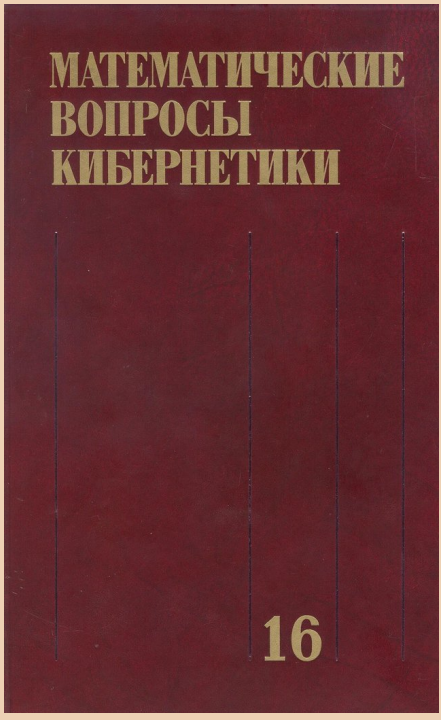
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 16



В. М. Храпченко

Квадратичная нижняя оценка сложности формул над базисом $\{\&, \vee, \bar{}\}$ для БЧХ-кодов

Рекомендуемая форма библиографической ссылки: Храпченко В. М. Квадратичная нижняя оценка сложности формул над базисом $\{\&, \vee, \bar{}\}$ для БЧХ-кодов // Математические вопросы кибернетики. Вып. 16. — М.: ФИЗМАТЛИТ, 2007. — С. 239–241. URL: http://library.keldysh.ru/mvk.asp?id=2007-239

КРАТКИЕ СООБЩЕНИЯ

КВАДРАТИЧНАЯ НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ ФОРМУЛ НАД БАЗИСОМ $\{\&, \vee, {}^-\}$ ДЛЯ БЧХ-КОДОВ*)

В. М. ХРАПЧЕНКО

(МОСКВА)

К. Л. Рычков доказал [2] неравенство

$$L(f_n) \geqslant \frac{|R|^2}{(1 + C_{n-1}^1 + \ldots + C_{n-1}^t)|N^0||N^1|}, \tag{1}$$

где f_n — характеристическая функция двоичного кода (т. е. булева функция равная 1 в точках, принадлежащих коду, и только в них) длины n с расстоянием $2t+1$, $L(f_n)$ — сложность минимальной формулы над базисом $\{\&, \vee, {}^-\}$, реализующей функцию f_n, N^0 — множество вершин n-мерного единичного куба, в которых функция f_n равна 0, N^1 — множество вершин n-мерного единичного куба, в которых функция f_n равна 1, R — множество таких пар вершин (α, β), что $\alpha \in N^0$, $\beta \in N^1$ и расстояние между ними (число координат, в которых они различаются) не превосходит $t+1$; как обычно, $|M|$ обозначает мощность множества M.

Изучение сложности реализации характеристической функции кода обусловлено тем, что в режиме, когда код используется не для исправления ошибок, а только для их обнаружения, именно вычисление характеристической функции позволяет определить наличие ошибок в сообщении.

Немного ослабим оценку (1), чтобы сделать ее более удобной для применения.

Из определения множества R следует, что

$$|R| = |N^1| \sum_{i=1}^{t+1} C_n^i.$$

*) Работа выполнена при финансовой поддержке Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики», проект «Синтез и сложность управляющих систем» и Программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.1).

Получим для этой суммы две различные нижние оценки:

$$\sum_{i=1}^{t+1} C_n^i = \sum_{i=0}^{t} C_n^{i+1} = \sum_{i=0}^{t} \frac{n\dots(n-i+1)(n-i)}{(i+1)!} \geqslant$$

$$\geqslant \frac{n-t}{t+1} \sum_{i=0}^{t} \frac{n\dots(n-i+1)}{i!} = \frac{n-t}{t+1} \sum_{i=0}^{t} C_n^i$$

и

$$\sum_{i=1}^{t+1} C_n^i \geqslant C_n^{t+1} = \frac{n}{t+1} C_{n-1}^t.$$

Получим теперь верхнюю оценку для суммы в знаменателе правой части неравенства (1):

$$1 + C_{n-1}^1 + \dots + C_{n-1}^t =$$

$$= C_{n-1}^t \left(1 + \frac{t}{n-t} + \frac{t(t-1)}{(n-t)(n-t+1)} + \dots + \frac{t!}{(n-t)\dots(n-1)}\right) \leqslant$$

$$\leqslant C_{n-1}^t \left(1 + \frac{t}{n-t} + \left(\frac{t}{(n-t)}\right)^2 + \dots\right) = C_{n-1}^t \frac{1}{1 - \frac{1}{n-1}} = C_{n-1}^t \frac{n-t}{n-2t}.$$

Наконец, очевидно, что

$$|N^0| \leqslant 2^n.$$

Подставляя все эти соотношения в (1), получим

$$L(f_n) \geqslant \frac{|N^1|^2 \left(\sum_{i=1}^{t+1} C_n^i\right)^2}{(1 + C_{n-1}^1 + \dots + C_{n-1}^t)|N^0||N^1|} \geqslant \frac{|N^1| \ \frac{n-t}{t+1} \sum_{i=0}^{t} C_n^i \cdot \frac{n}{t+1} C_{n-1}^t}{C_{n-1}^t \cdot \frac{n-t}{n-2t} \cdot 2^n},$$

и в результате

$$L(f_n) \geqslant \frac{|N^1| \sum_{i=0}^{t} C_n^i}{2^n} \cdot \frac{n(n-2t)}{(t+1)^2}, \tag{2}$$

где первый сомножитель характеризует плотность соответствующего кода, а второй показывает зависимость нижней оценки от кодового расстояния.

Применим (2) к БЧХ-кодам (кодам Боуза— Рой-Чоудхури— Хоквингема). Рассмотрим БЧХ-коды с параметрами: $n = 2^m - 1$ (длина), $d = 2t + 1$ (кодовое расстояние), $k = n - mt$ (размерность) (см., например, [1]). Для них

$$|N^1| = 2^k = 2^{n-mt} = \frac{2^n}{(n+1)^t}.$$

Оценивая первый сомножитель в (2), получим

$$\frac{|N^1| \sum_{i=0}^{t} C_n^i}{2^n} \geqslant \frac{\frac{2^n}{(n+1)^t} C_n^t}{2^n} \geqslant \frac{(n-t+1)^t}{(n+1)^t \cdot t!} \geqslant \frac{1}{t!}\left(1 - \frac{t}{n+1}\right)^t \geqslant \frac{1}{t!}\left(1 - \frac{t}{n}\right)^t \geqslant \frac{1}{t!}\left(1 - \frac{t^2}{n}\right).$$

Подставляя эту оценку в (2), получаем нижнюю оценку для сложности характеристической функции БЧХ-кода:

$$L(f_n) \geqslant \left(1 - \frac{t^2}{n}\right) \cdot \frac{n(n-2t)}{t!\ (t+1)^2}.$$

Легко видеть, что оценка с ростом t, т. е. с ростом кодового расстояния, становится слабее. При небольших t это квадратичная нижняя оценка.

Конечно, это совсем простое следствие классического неравенства Рычкова. Для автора важно то, что оно побуждает снова вспомнить Олега Борисовича Лупанова, те его работы, в которых связь между сложностью и кодами тоже на видном месте, правда, связь значительно более глубокая. Попутно вспоминается, что и задачи собственно теории кодирования Олег Борисович держал под прицелом.

СПИСОК ЛИТЕРАТУРЫ

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.
2. Рычков К. Л. Модификация метода В. М. Храпченко и его применение к оценке сложности П-схем для кодовых функций // Методы дискретного анализа в теории графов и схем. — Вып. 42. — Новосибирск, ИМ СО АН СССР. — 1985. — С. 91–98.

Поступило в редакцию 5 VIII 2006