Serdica
Bulgariacae mathematicae publicationes

Сердика
Българско математическо списание

ДВЕ ИНФОРМАЦИОННЫЕ ЗАДАЧИ ОБ ОБОБЩЕННЫХ БЧХ КОДАХ

РОСИЦА Д. ДОДУНЕКОВА

В работе показывается, что два результата Гоппы [1; 2], устанавливающих информационные характеристики кодов Гоппы, верны и для обобщенных БЧХ кодов [3].

Пусть $F=GF(q)$ — конечное поле с $q=p^t$ элементами, p — простое число, и пусть V_n — векторное пространство размерности n над полем $GF(q)$. Обозначим через K_n фактор-кольцо кольца полиномов над полем $K=GF(q^m)$ по модулю идеала (x^m-1), где m — мультипликативный порядок q по модулю n, $K_n=K[x]/(x^n-1)$. Аналогично обозначим $F_n=F[x]/(x^n-1)$. Преобразование Фурье для многочлена $a(x)\in K_n$ задается равенством $\Phi_\alpha\{a(x)\}=A(x)=\Sigma_{j=0}^{n-1}A_jx^j$, где $A_j=a(\alpha^j)$, α — примитивный корень из единицы степени n в поле $GF(q^m)$. Пусть $P(x)$, $G(x)\in K_n$ таковы, что $(P(x), x^n-1)=(G(x), x^n-1)=1$.

Определение 1 [3]. Множество $GBCH(P, G)=\{v(x)\in F_n/[P(x).V(x)]_n=0 \pmod{G(x)}\}$ *называется обобщенным БЧХ кодом, ассоциированным с упорядоченной парой* $(P(x), G(x))$. (Здесь $[f(x)]_n$ обозначает остаток полинома $f(x)$ по модулю x^n-1 и $V(x)=\Phi_\alpha\{v(x)\}$.)

Пусть A и B — подмножества V_n. Будем говорить, что A исправляет B, если представление любого элемента $y\in V_n$ в виде $y=l_1+l_2$, $l_1\in A, l_2\in B$, единственно, когда существует. Множество $B\in V_n$, содержащее 0, будем называть шумом.

Следуя [1], обозначим через $A\bigcirc_c B$ бинарное отношение „A исправляет B“. Положим
$A-A=\{l\in V_n: l=a-b, a, b\in A\}$. Ясно, что $A\bigcirc_c B$ тогда и только тогда, когда $(A-A)\bigcap(B-B)=\{0\}$.

Теорема 1. *Пусть* B_n *— последовательность шумов, таковых, что* $\lim_{n\to\infty}n^{-1}\log_q|B_n-B_n|=\eta$. *Тогда для любого* $\varepsilon>0$ *существует последовательность* A_n *обобщенных БЧХ кодов и число* $N(\varepsilon)$ *таковы, что для* $n>N(\varepsilon)$ *выполняется* $A_n\bigcirc_c B_n$ *и* $|A_n|\geq q^{(1-2\eta-\varepsilon)}$.

Доказательство. Покажем, что такая последовательность A_n существует среди неприводимых обобщенных БЧХ кодов (код называется неприводимым, если многочлен $G(x)$ — неприводим). Пусть

$$t_n=[(\log|B_n-B_n|+\varepsilon n)/\log(n+1)] \tag{1}$$

(здесь и далее опускаем основание q, по которому берется логарифм). Ввиду условия теоремы имеем $\lim_{n\to\infty}t_n=\infty$ и $t_n<n-1$, если n достаточно большое.

Пусть $P=(P_0, \ldots, P_{n-1})$, $P_i\neq 0$, $P_i\in GF(q^m)$, $\forall i=0, \ldots, n-1$, и $\mathsf{P}(x)=\Phi_\alpha\{P(x)\}$, $P(x)=\Sigma_{i=0}^{n-1}P_ix^i$. Пусть $R_n=\{\Sigma_{i=0}^{n-1}a_iP_i\alpha^{-i}(x-\alpha^{-1})^{-1}, a_i\in GF(q)\}$ и

СЕРДИКА Българско математическо списание. Том 8, 1932, с. 32–34.

рассмотрим взаимно-однозначное отображение $\varphi : V_n \to R_n$, задаваемое следующим образом: $a=(a_0, \ldots, a_{n-1}) \to \sum_{i=0}^{n-1} a_i p_i \alpha^{-i}(x-\alpha^{-i})^{-1}$. φ является изометрией пространств V_n и R_n относительно метрики Хемминга. Будем считать, что $B_n \subset R_n$.

Обозначим через $N_\mu^t n$ множество всех неприводимых делителей числителей дробей из $B_n - B_n$ степени t_n. Ясно, что

$$|N_n^{t_n}| \cdot t_n < |B_n - B_n| n. \tag{2}$$

Обозначим через K_n^t множество всех неприводимых многочленов степени t с коэффициентами из поля $GF(q^m)$. Для $|K_n^t|$ известна формула [5] $|K_n^t| = t^{-1}\sum_{\delta/t}\mu(\delta)(n+1)^{t/\delta}$, где $n+1=q^m$ есть число элементов поля $GF(q^m)$ и $\mu(\delta)$ — функция Мебиуса. Для больших n имеем $|K_n^t| \sim (n+1)^t/t$. Пусть $t=t_n$. Тогда

$$\log t_n/n + \log |K_n^{t_n}|/n \sim t_n \log (n+1)/n$$

$$= (\log |B_n - B_n| + \varepsilon n)/n.$$

Легко проверить, что $\log t_n/n_{n\to\infty} \to 0$. Тогда

$$\log |K_n^{t_n}|/n \sim \log |B_n - B_n|/n + \varepsilon. \tag{3}$$

Используя (1), (2) и (3), покажем, что $K_n^{t_n} \setminus N_n^{t_n} \neq \Phi$. Имеем

$$|N_n^{t_n}|/|K_n^{t_n}| < n |B_n - B_n|/t_n |K_n^{t_n}| \sim \log (n+1)/(\eta+\varepsilon) q^{\varepsilon} \xrightarrow[n\to\infty]{} 0.$$

Пусть $g(x) \in K_n^{t_n} \setminus N_n^{t_n}$. Обозначим $A_n = GBCH(\mathrm{P}(x), g(x))$. Тогда $A_n \cap (B_n - B_n) = \{0\}$. Как показано в [4], A_n — подпространство R_n, т. е. $A_n = \{\xi(x) \in R_n \mid \xi(x) \equiv 0 \pmod{g(x)}\}$. Следовательно, A_n является обобщенным БЧХ кодом, исправляющим B_n.

Для A_n справедлива оценка

$$|A_n| \geq q^{n - t_n \log (n+1)}. \tag{4}$$

Имеем

$$t_n \log (n+1)/n = \log |B_n - B_n|/n + \varepsilon \leqq 2\eta + \varepsilon, \tag{5}$$

если n достаточно большое. Подставляя (5) в (4), получаем $|A_n| \geq q^{n(1-2\eta-\varepsilon)}$. Теорема доказана.

В [2] Гоппа показал, что на классе неприводимых кодов Гоппы асимптотически достигается пропускная способность двоичного симметричного канала.

Теорема 2. *На классе неприводимых обобщенных БЧХ кодов асимптотически достигается пропускная способность двоичного симметричного канала.*

Учитывая дробно-рациональное представление неприводимых обобщенных БЧХ кодов [4], доказательство проводится вполне аналогично соответствующему доказательству для неприводимых кодов Гоппы [2].

ЛИТЕРАТУРА

1. В. Д. Гоппа. Об исправлении произвольных шумов неприводимыми кодами. *Проблемы передачи информации*, **10**, 1974, № 3, 118-119.
2. В. Д. Гоппа. На неприводимых кодах достигается пропускная способность ДСК. *Проблемы передачи информации*, **10**, 1974, № 3, 111-112.
3. R. T. Chen, D. M. Choy. Algebraic generalization of BCH-Goppa-Helgert codes. *IEEE Trans. Inform. Theory*, **21**, 1975, 70-79.
4. S. M. Dodunekov. On the connection between GBCH and Goppa codes. *C. r. Acad. bulg. Sci.*, **32**, 1979, 407-410.
5. Е. Р. Берлекэми. Алгебраическая теория кодирования. Москва, 1971.

Единый центр математики и механики
1090 София П. Я. 373

Поступила 7. 4. 1980