Доклады Академии наук СССР
1975. Том 223, № 1

УДК 621.391.15

КИБЕРНЕТИКА И ТЕОРИЯ РЕГУЛИРОВАНИЯ

Р. Р. ВАРШАМОВ

О ВОЗМОЖНОСТЯХ УВЕЛИЧЕНИЯ МОЩНОСТИ ЛИНЕЙНЫХ КОРРЕКТИРУЮЩИХ КОДОВ

(Представлено академиком Б. Н. Петровым 3 VII 1974)

Одной из основных задач алгебраической теории кодов является проблема разработки конструктивных методов построения помехоустойчивых систем кодирования, обладающих максимальной скоростью передачи информации (*или, что то же самое,* максимальной мощностью кодовых подмножеств) при заданных ее основных параметрах n, t и q, где n — блоковая длина кода, t — число исправляемых ошибок, q — основание кода. В заметке приводятся некоторые результаты относительно возможностей построения в метрике Хемминга помехоустойчивых систем сигналов, мощность кодовых подмножеств которых намного превосходит мощность всех аналогичных известных в литературе наилучших линейных кодов.

Наша основная концепция заключается в следующем.

Теорема 1. *Как бы велико ни было число* θ *и каков бы ни был метод построения линейных корректирующих кодов, исправляющих* t *симметрических ошибок, опираясь на него, всегда можно указать такие значения параметров* n *и* q, *для которых можно строить новые классы кодов, мощность кодовых подмножеств которых более чем в* θ *раз будет превосходить мощность соответствующих кодов, построенных первоначальным способом; при этом сохраняется их прежняя корректирующая способность.*

Мы будем считать, что задан метод построения систем кодирования, исправляющих фиксированное число t ошибок, если указан вполне определенный способ, позволяющий для произвольных n и q строить такие системы.

Рассмотрим на примерах кодов Хемминга и Боуза — Чоудхури — Хоквингема, какую физическую интерпретацию допускает теорема 1.

1. Коды Хемминга. Как известно [1], кодами Хемминга называют класс линейных кодов, исправляющих одиночные симметрические ошибки. Эти коды, хотя и являются оптимальными в классе линейных кодов, однако относятся к разряду кодов, для которых разработан метод построения. А поэтому согласно утверждениям теоремы 1 должна существовать конструктивная возможность, позволяющая увеличивать (даже неограниченно) их мощность.

Условимся в дальнейшем через $g(n, q)$ обозначать мощность наилучшего кода Хемминга длины n и основания q, а также $\varepsilon_q(n)=q^{[\log_q n]}$, где $[x]$ — наименьшее целое, не превосходящее x, и $\{x\}=x-[x]$.

Случай $q=3$ *.

Теорема 2. *Для любых целых значений* n, *удовлетворяющих условиям*

$$\log_3 {}^3/_2<\{\log_3 n\}<2\log_3(3\sqrt{5}),$$

существуют системы сигналов с основанием 3, *корректирующие одиночные симметрические ошибки, мощности кодовых подмножеств* $b(n, 3)$ *которых строго превосходят мощности соответствующих кодов Хемминга и удовлетворяют неравенству*

$$b(n, 3)>3^{1-(\log_3 5n)}g(n, 3).$$

* В случае $q=2$ наш метод неэффективен.

Этот результат допускает также и некоторое усиление, а именно справедлива

Теорема 3. *Всегда найдутся такие значения параметра n, для которых можно строить системы кодирования с основанием 3, исправляющие одиночные ошибки, мощности кодовых подмножеств $b(n, 3)$ которых удовлетворяли бы неравенству*

$$b(n, 3) > 3^{1-\{\log_3((n+\delta(n))\}} g(n, 3),$$

где $\delta(n)=1$ или 2.

Так, например, справедлива

Теорема 4. *Пусть $m=p_1 \dots p_\sigma$, p_s, $s=1, \dots, \sigma$,— простые числа вида $8k+5$, g_s — первообразный корень по модулю p_s,*

$$Q_s=p_1 \dots p_s \ (Q_0=1), \quad m_s=Q_s^{-1} m, \quad M_s=\frac{m-m_s}{4},$$

$$p_s'=\frac{p_s-1}{4}, \quad \{\log_3 m\} > \log_3 2.$$

Тогда для любых целых α и n $(\varepsilon_3(m)<2n<m/2)$ множество всевозможных решений сравнения

$$\sum_{s=1}^{\sigma} \sum_{v=0}^{m_s-1} \sum_{u=1}^{p_s'} Q_{s-1}(g_s^{iu}+p_s v) x_{M_s+p_s' v+u} \equiv \alpha \pmod m,$$

*где x_u, $u \leqslant n$ *, принимает произвольно значения 0, 1 и 2, является кодом длины n с основанием 3, исправляющим одиночные симметрические ошибки, мощность наилучшего среди которых*

$$b(n, 3) > 3^{1-\{\log_3 m\}} g(n, 3), \quad \delta(n)=1.$$

Или же справедлива

Теорема 5. *Пусть $m=p_1 \dots p_\sigma$, где p_s — простые числа вида $8k+3$, $m > \varepsilon_3(2m)$ и $q=3$.*

Тогда для произвольных целых чисел α, β и n $(\varepsilon_3(2n)<2n<m)$ множество всевозможных решений системы сравнений

$$\sum_{s=1}^{\sigma} \sum_{v=0}^{m_s-1} \sum_{u=1}^{2p_s'} Q_{s-1}(g_s^{2u}+p_s v) x_{2M_s+2p_s' v+u} \equiv \alpha \pmod m,$$

$$\sum_{u=1}^{n} x_u \equiv \beta \pmod 2.$$

где $x_u=0, 1$ и 2 $(u \leqslant n)$ и $x_u=0$ $(u>n)$, является кодом длины n, исправляющим одиночные симметрические ошибки, мощность наилучшего среди которых

$$b(n, 3) > 3^{1-\{\log_3 2m\}} g(n, 3), \quad \delta(n)=2.$$

Рассмотрим теперь общий случай произвольного $q=p^\nu$ **

Теорема 6 $(\nu>1)$. *Для любых целых значений n, удовлетворяющих условиям*

$$\log_q (q-1)^{-1} q \leqslant \{\log_q n\} \leqslant 1/\nu,$$

существуют системы сигналов с основанием q, исправляющие одиночные симметрические ошибки, мощность кодовых подмножеств которых $b(n, q)$ удовлетворяет соотношению

$$b(n, q)=p^{\nu-1} g(n, q).$$

---

* $x_u=0$ для всех $u>n$.

** p — простое нечетное число.

Теорема 7 (v=1). *Для любых целых значений n, удовлетворяющих условиям*

$$\log_p (p-1)^{-1} p \leqslant \{\log_p n\} \leqslant \log_p p/\omega(n), \quad 2 \leqslant \omega(n) < 4,$$

существуют системы сигналов с основанием p, исправляющие одиночные симметрические ошибки, мощность кодовых подмножеств $b(n, p)$ которых удовлетворяет неравенству

$$b(n, p) > p^{1-\{\log_p n\omega(n)\}} g(n, p).$$

Этот результат допускает некоторое усиление.

Теорема 8. *Существуют такие значения n, для которых можно строить коды с основанием p, исправляющие одиночные симметрические ошибки, мощность кодовых подмножеств которых*

$$b(n, p) > p^{1-\{\log_p 2n\}} g(n, p).$$

2. Коды Боуза — Чоудхури — Хоквингема (Б.Ч.Х.). Коды Б.Ч.Х. являются обобщением кодов Хемминга на случай исправления многократных ошибок, причем аналогично кодам Хемминга они относятся к разряду кодов, для которых существует метод их построения. А поэтому, согласно нашей концепции, должна существовать конструктивная возможность, позволяющая на их основе строить новые, более мощные коды, исправляющие многократные ошибки.

Обозначим через $G_t(n, q)$ мощность наилучших кодов Б.Ч.Х. длины n с основанием q, исправляющие t симметрических ошибок.

Случай $q=2, t=2$.

Теорема 9. *Для любых целых значений n ($\{\log_2 n\} < \log_2 (2/\sqrt{3})$) и $q=2$ можно строить коды, исправляющие двойные симметрические ошибки, мощность $B_2(n, 2)$ которых будет строго превосходить мощность соответствующих кодов Б.Ч.Х., исправляющих аналогичное число ошибок, и удовлетворять неравенству*

$$B_2(n, 2) > 4^{1-\{\log_2 n\sqrt{3}\}} G_2(n, 2). \tag{1}$$

Так, например, справедлива

Теорема 10. *Пусть p — простое число вида $6k-1$, удовлетворяющее условию $\{\log_2 p\} < \log_2 (2/\sqrt{3})$.*

Тогда для любых целых чисел α, β, γ и n ($\varepsilon_2(p) \leqslant n \leqslant p$) множество всевозможных решений системы сравнений

$$\sum_{u=1}^{n} u x_u \equiv \alpha \pmod p,$$

$$\sum_{u=1}^{n} u^2 x_u \equiv \beta \pmod p,$$

$$\sum_{u=1}^{n} x_u \equiv \gamma \pmod 3,$$

где $x_u=0$ или 1, является кодом длины n с основанием 2, исправляющим две симметрические ошибки, мощность наилучших среди которых строго превосходит мощность аналогичных кодов Б.Ч.Х. и удовлетворяет неравенству (1).

Случай $q=3, t=2$.

Теорема 11. *Пусть n — любое целое, удовлетворяющее условию $\{\log_3 n\} < \log_3 {}^3/_2$, и g — примитивный элемент поля Галуа $\mathrm{GF}(\varepsilon_3(3n))$.*

Тогда множество всевозможных решений уравнений

$$\sum_{u=1}^{n} g^{-u}x_u=a, \quad \sum_{u=1}^{n} g^{u}x_u=b,$$

где $x_u \notin \mathrm{GF}(3)$, a, $b \notin \mathrm{GF}(\varepsilon_3(3n))$, *является кодом длины* n *с основанием* 3, *исправляющим две симметрические ошибки, мощность* $B_2(n, 3)$ *которого*

$$B_2(n, 3)=(\sqrt{3})^{1-(-1)^{[\log_3 n]}}G_2(n, 3).$$

Случай $q=4$, $t=2$.

Теорема 12. *Пусть даны произвольное натуральное число* $n>5$ *и* g *— примитивный элемент поля Галуа* $\mathrm{GF}(\varepsilon_4(12n))$.

Тогда множество всевозможных решений системы уравнений

$$\sum_{u=1}^{n} g^{-u}x_u=a, \quad \sum_{u=1}^{n} g^{u}x_u=b,$$

где $x_u \notin \mathrm{GF}(4)$, a, $b \notin \mathrm{GF}(\varepsilon_4(12n))$, *является кодом длины* n *с основанием* 4, *исправляющим две симметрические ошибки, мощность* $B_2(n, 4)$ *которого строго превосходит мощность аналогичного кода Б.Ч.Х. и удовлетворяет соотношению*

$$B_2(n, 4)=4^{h(n)}G_2(n, 4),$$

где $h(n)=[\log_4 n]-(-1)^{[\varepsilon_4(n)/3n]}$.

Однако, если опираться только на результаты Боуза — Чоудхури — Хоквингема, то можно получить также и следующее утверждение

Случай произвольного p.

Теорема 13. *Для любых произвольных значений* $t\geqslant 2$, $p\geqslant 2t$ *и* n ($\{\log_p n\}<\log_p (p/\nu(n))$, $1\leqslant\nu(n)<2$) *можно строить коды длины* n *с основанием* p, *исправляющие* t *симметрических ошибок, мощность* $B_t(n, p)$ *которых будет строго превосходить мощность соответствующих кодов Б.Ч.Х., исправляющих аналогичное число ошибок, и удовлетворять неравенству*

$$B_t(n, p)>(p^{1-\{\log_p \nu(n) n\}})^{2t-1}G_t(n, p).$$

Следует отметить, что при неограниченном возрастании n количество $\nu(n)$ бесконечное число раз принимает значение 1, так что справедлива

Теорема 14. *При фиксированных* t *и* $p\geqslant 2t$ *и неограниченном возрастании* n *бесконечное число раз удовлетворяется неравенство*

$$B_t(n, p)>(p^{1-\{\log_p n\}})^{2t-1}G_t(n, p).$$

Вычислительный центр
Академии наук АрмССР и
Ереванского государственного университета
Ереван

Поступило
28 VI 1974

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] *У. Питерсон,* Коды, исправляющие ошибки, «Мир», М., 1964.