Доклады Академии наук СССР
1971. Том 196, № 3

УДК 519.1

МАТЕМАТИКА

В. М. СИДЕЛЬНИКОВ

О ВЗАИМНОЙ КОРРЕЛЯЦИИ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

(Представлено академиком П. С. Новиковым 26 VI 1970)

1. Пусть E_n^k — множество всех векторов длины n, координаты которых суть числа $0, 1, \ldots, k-1$, $W \subset E_n^k$ и $|W|$ — число элементов множества W. В теории кодирования W называют k-значным кодом и рассматривают функцию

$$d(W) = \min_{\mathbf{x}, \mathbf{y} \in W,\ \mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y}),$$

называемую кодовым расстоянием, где $d(\mathbf{x}, \mathbf{y})$ — число различных координат у векторов $\mathbf{x}$ и $\mathbf{y}$. Вместе с тем для ряда приложений представляют интерес две другие функции множества W.

Определим скалярное произведение векторов $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ и $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ из E_n^k как

$$(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} \exp \frac{2\pi i (x_j - y_j)}{k},$$

обозначим через $\mathbf{x}^{(t)}$ циклический сдвиг вектора $\mathbf{x}$ на t разрядов вправо и положим

$$\eta(W) = \max_{\mathbf{x}, \mathbf{y} \in W,\ \mathbf{x} \neq \mathbf{y}} |(\mathbf{x}, \mathbf{y})|, \quad \tau(W) = \max_{\substack{\mathbf{x}, \mathbf{y} \in W, 0 \leqslant t < n \\ t \neq 0, \text{ если } \mathbf{y} = \mathbf{x}}} |(\mathbf{x}^{(t)}, \mathbf{y})|.$$

В том случае, когда W состоит из одной последовательности $\mathbf{x}$, функция $\tau(W) = \tau(\mathbf{x})$ характеризует максимум модуля автокорреляции последовательности $\mathbf{x}$; в случае $|W| > 1$ функция $\tau(W)$ характеризует максимум модуля взаимной корреляции и автокорреляции последовательностей из W.

В работе ([2]) приведены некоторые двоичные последовательности нечетной длины, а в ([3]) — четной длины, для которых $\tau(\mathbf{x})$ принимает минимальное значение.

Обозначим через W^* любое максимальное подмножество множества $W \subset E_n^k$, обладающее тем свойством, что если некоторая последовательность принадлежит W^*, то любой ее нетривиальный циклический сдвиг не принадлежит W^*. В частности, ни одна из последовательностей, период которой меньше n, не принадлежит W^*. Очевидно, что если W — циклический код, то $\tau(W^*) \leqslant \eta(W)$. Заметим также, что если k — простое число и W ($W \subset E_n^k$) является линейным пространством над полем вычетов по mod k, то

$$d(W) \geqslant \frac{k-1}{k}(n - \eta(W)).$$

В настоящей работе найдены нижние оценки величин

$$\eta_k(n, m) = \min_{W \subset E_n^k,\ |W| = m} \eta(W), \quad \tau_k(n, m) = \min_{W \subset E_n^k,\ |W| = m} \tau(W).$$

Получена также верхняя оценка величины $d_k(n, m) = \max_{W \subset E_n^k,\ |W| = m} d(W)$,

которая лучше ранее известных в случае, когда m растет как степенная функция n. Кроме того, построены множества W, у которых величины

$\eta(W)$ и $\tau(W)$ близки к полученным нижним оценкам, а в некоторых случаях достигают их.

2. Оценки для величин $\eta_k(n, m)$, $\tau_k(n, m)$, $d_k(n, m)$. Обозначим через $\nu(n, s, k)$ s-ый момент случайной величины $S_n = \left|\sum_{t=1}^{n} \beta_t\right|^2$, где β_t $(t = 1, \ldots, n)$ — независимые комплекснозначные случайные величины, принимающие значение $\exp 2\pi ir/k$ $(r = 0, \ldots, k-1)$ с вероятностью $1/k$.

Лемма 1. *Для любого* $W \subset E_n^k$ *и любого целого* s, $s \geqslant 0$

$$\sum_{x,\, y \in W} |(x, y)|^{2s} \geqslant |W|^2 \nu(n, s, k).$$

Теорема 1. *Для любого целого неотрицательного* s $(s < n/2)$

$$(\eta_2(n, m))^2 > (2s+1)(n-s) + s - 2^s n^{2s+2}/m(2s)!\binom{n}{s}; \tag{1}$$

$$(\eta_k(n, m))^2 > \frac{s+1}{2}(2n-s) - 2^s n^{2s+2}/m(s!)^2\binom{2n}{s}; \tag{2}$$

$$(\tau_2(n, m))^2 > (2s+1)(n-s) + s - 2^s n^{2s+1}/m(2s)!\binom{n}{s}; \tag{3}$$

$$(\tau_k(n, m))^2 > \frac{s+1}{2}(2n-s) - 2^s n^{2s+1}/m(s!)^2\binom{2n}{s}. \tag{4}$$

При $s = 0$ и $m = 2$ оценка (3) совпадает с оценкой, полученной в [4].

Следствие. *Для любого целого* s $(s \geqslant 1)$

$$\tau_2(n, n^s) \geqslant \eta_2(n, n^{s+1}) > \sqrt{2s(n-s)}. \tag{5}$$

Обозначим через $\pi(n, s, k)$ s-й момент случайной величины $Q_n = \sum_{i=1}^{n} \alpha_i$, где α_i $(i = 1, \ldots, n)$ — независимые случайные величины, каждая из которых равна $k-1$ с вероятностью $1/k$ и -1 с вероятностью $(k-1)/k$.

Лемма 2. *Для любого* $W \subset E_n^k$ *и любого целого* s $(s \geqslant 0)$

$$\sum_{x,\, y \in W} ((k-1)n - kd(x, y))^{2s} \geqslant |W|^2 \pi(n, s, k).$$

Теорема 2. *Пусть* $\sigma_k(t, n, m) = \dfrac{m\pi(n, t, k) - n^t}{m-1}$, $m > n^{s/2} + {}^3/_2 n$, *и* s *— любое целое положительное число, для которого* $\sigma_k(t, n, m) > 0$ *и*

$$\Phi_k(s, n, m) = (\sigma_k(2s, n, m))^{(2s+1)/2s} + \sigma_k(2s+1, n, m) > 0.$$

Тогда

$$d_k(n, m) \leqslant \frac{n(k-1)}{k} - \frac{1}{k}({}^1/_2\Phi_k(s, n, m))^{1/(2s+1)}. \tag{6}$$

Из этой теоремы, в частности, следует, что если $m \geqslant Cn^{1/2}$, где $C > 1$, то существует константа C_1 $(C_1 > 0)$ такая, что

$$d_2(n, m) \leqslant n/2 - C_1\sqrt{n}.$$

С другой стороны, приведенная ниже теорема 7 дает (при $r = 2$) последовательность кодов, для которых $m \sim n^{s/2}$ и $(n/2 - d) \sim {}^1/_2 n^{1/2}$ при $n \to \infty$.

3. Величины $\eta(W)$, $\tau(W^*)$, $d(W)$ для линейных циклических кодов W. Для произвольного многочлена $f(x)$ над $\mathrm{GF}(p)$ обозначим через $n = n(f(x))$ минимальное число такое, что $f(x)$ делит $x^n - 1$. Известно [1], что идеал, порожденный многочленом $(x^n - 1)/f(x)$, в кольце вычетов многочленов по mod $(x^n - 1)$ образует линейный циклический код в E_n^p, который мы обозначим через $W(f(x))$. Положим также $(W(f(x)))^* = W^*(f(x))$.

Теорема 3. *Пусть* $f(x)$ *— минимальная функция элементов* $\alpha, \alpha^2, \ldots, \alpha^t$ *поля* $\mathrm{GF}(q)$, $q = p^l$, *и* $n = n(f(x))$.

Тогда *

---

* Ниже $[x]$ — целая часть числа x, $\mu(\cdot)$ — функция Мёбиуса.

1) *если* $\frac{q-1}{n}t < p^{[(l+1)/2]}$, *то* $|W(f(x))| = q^{t-[t/p]}$ и $|W^*(f(x))| =$

$$= \frac{1}{n}\sum_{d|n}\mu(d)\,q^{[t/d]-[t/dp]} \geqslant \frac{q-1}{n}\,q^{t-[t/d]-1};$$

2) $\tau(W^*(f(x))) \leqslant \eta(W(f(x))) \leqslant (t-n/(q-1))\sqrt{q} + n/(q-1)$; (7)

3) *для любых* $\mathbf{x}, \mathbf{y} \in W(f(x))$, $\mathbf{x} \neq \mathbf{y}$,

$$\frac{p-1}{p}\left(n + \frac{n}{q-1} - \left(t - \frac{n}{q-1}\right)\sqrt{q}\right) \leqslant d(\mathbf{x}, \mathbf{y}) \leqslant \frac{p-1}{p}\left(n + \frac{n}{q-1} + \left(t - \frac{n}{q-1}\right)\sqrt{q}\right). \quad (8)$$

Сравним оценку (7) в двоичном случае с нижними оценками п. 2. Если α — первообразный корень поля $\mathrm{GF}(2^l)$ и $t = 2s+1 < 2^{[(l+1)/2]}$, то $n = 2^l - 1$, $|W(f(x))| = (n+1)^{s+1}$, $|W^*(f(x))| \geqslant (n+1)^s$ и $\tau(W^*(f(x))) \leqslant \eta(W(f(x))) \leqslant 2s\sqrt{n+1} + 1$. С другой стороны, из следствия теоремы 1 следует, что при $s \geqslant 1$ $\tau_2(n, (n+1)^s) > \sqrt{2s(n-s)}$, $\eta_2(n, (n+1)^{s+1}) > \sqrt{2s(n-s)}$.

При небольших значениях t оценки теоремы 3 уточняются в п. 4.

4. Теорема 4. *Пусть* $f(x)$ — *минимальная функция элементов* α *и* α^2, *где* α — *первообразный корень поля* $\mathrm{GF}(q)$, $q = p^l$, $p > 2$.

Тогда $n = q - 1$,

1) $|W(f(x))| = (n+1)^2$ *и* $|W^*(f(x))| = n+1$;

2) $\sqrt{n} < \eta_p(n, (n+1)^2) \leqslant \eta(W(f(x))) \leqslant \sqrt{n+1} + 1$; (9)

3) $\sqrt{n-1} < \tau_p(n, n+1) \leqslant \tau(W^*(f(x))) \leqslant \sqrt{n+1} + 1$; (10)

4) *код* $W(f(x))$ *имеет спектр весов, указанный в табл.* 1.

Теорема 5. *Пусть* $f(x)$ — *минимальная функция элемента* $\alpha = \theta^2$, *где* θ — *первообразный корень поля* $\mathrm{GF}(q)$, $q = p^l$, $p > 2$.

Тогда $n = {}^1/_2(q-1)$,

1) $|W(f(x))| = 2n+1$ *и* $|W^*(f(x))| = 2$;

2) $\sqrt{{}^1/_2 n} < \eta_p(n, 2n+1) \leqslant \eta(W(f(x))) < \sqrt{{}^1/_2(n+1)} + {}^1/_2$; (11)

3) $\sqrt{{}^1/_2 n} < \tau_p(n, 2) \leqslant \tau(W^*(f(x))) < \sqrt{{}^1/_2(n+1)} + {}^1/_2$;

4) *для любых* $\mathbf{x}, \mathbf{y} \in W(f(x))$, $\mathbf{x} \neq \mathbf{y}$

$$d(\mathbf{x}, \mathbf{y}) = \begin{cases} \frac{1}{2p}(p-1)\,q, & \text{если } l = 2t+1, \\ \frac{1}{2p}(p-1)\,q \pm {}^1/_2(q-1)\,p^{t-1}, & \text{если } l = 2t. \end{cases}$$

Теорема 6. *Пусть* $f(x)$ — *минимальная функция элементов* α, α^2 *и* α^3, *где* α — *первообразный корень поля* $\mathrm{GF}(q)$, $q = 2^{2r+1}$, $r \geqslant 1$.

Тогда $n = q - 1$,

1) $|W(f(x))| = (n+1)^2$ и $|W^*(f(x))| = n+2$;

2) $\eta(W(f(x))) = \eta_2(n, (n+1)^2) = 2^{r+1} + 1$;

3) $\tau(W^*(f(x))) = \tau_2(n, n+2) = 2^{r+1} + 1$;

4) *двоичный линейный циклический код* $W(f(x))$ *образован* $(2^{4r+1} + 2^{3r} - 1)$ *векторами веса* 2^{3r}, $(2^{4r} + 2^{3r} - 2^{2r-1} - 2^{r-1})$ *векторами веса* $2^{3r} - 2^r$, $(2^{4r} - 2^{3r} - 2^{2r-1} + 2^{r-1})$ *векторами веса* $2^{3r} + 2^r$ *и нулевым вектором.*

Отметим, что Голд ([5]) рассмотрел множество W, состоящее из двух последовательностей кода $W(f(x))$, и установил, что $\tau(W) = 2^{r+1} + 1$.

Теорема 7. *Пусть* $f(x)$ — *минимальная функция элемента* $\alpha = \theta^{2t+1}$, *где* θ — *первообразный корень поля* $\mathrm{GF}(q)$, $q = 2^{2rt}$, $r \geqslant 2$, $t \geqslant 1$.

Тогда $n = (2^t+1)^{-1}(q-1)$ *и двоичный линейный циклический код* $W(f(x))$ *образован* n *векторами веса* $(2^t+1)^{-1}(2^{2rt-1} + (-1)^r 2^{rt+t-1})$, $q - n - 1$ *векторами веса* $(2^t+1)^{-1}(2^{2rt-1} - (-1)^r 2^{rt-1})$ *и нулевым вектором.*

Таблица 1

Вес кодовых векторов	Число кодовых векторов с данным весом
$l = 2t$	
$\frac{(p-1)q}{p} + (-1)^k p^{t-1}$, $k = 0,1$.	$\frac{(p-1)(q-1)}{2p}(q + (-1)^{k+1} p^t)$
$\frac{(p-1)q}{p} + (-1)^k (p-1) p^{t-1}$, $k = 0,1$.	$\frac{(q-1)}{2p}(q + (-1)^{k+1}(p-1)\, p^t)$
$\frac{(p-1)q}{p}$	$q-1$
0	1
$l = 2t+1$	
$\frac{(p-1)q}{p} + (-1)^k p^t$, $k = 0,1$.	$\frac{(p-1)(q-1)}{2p}(q + (-1)^{k+1} p^{t+1})$
$\frac{(p-1)q}{p}$	$\frac{q(q-1)}{p} + (q-1)$
0	1

При $r = 2$, $t = 2$ множество $W^*(f(x))$ векторов длины 51 состоит из четырех векторов веса 24 и одного вектора веса 32. Функции автокорреляции и взаимной корреляции этих векторов принимают два значения: $+3$ и -13. Отметим, что в [2] показано, что максимальное значение автокорреляционной функции двоичной последовательности длины 51 не может быть меньше 3.

В заключение приношу благодарность В. И. Левенштейну, под руководством которого выполнена эта работа.

Поступило
14 VI 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] У. Питерсон, Коды, направляющие ошибки, М., 1964. [2] R. C. Titsworts, International Telemetric Conference, London, 1963. [3] В. М. Сидельников, Пробл. передачи информ., 5, 1, 16 (1969). [4] J. E. Stalder, C. R. Cahn, Proc. of the IEEE, 52, 10, 1262 (1964). [5] R. Gold, Proc. of the IEEE on Inform. Theory, 14, 1, 154 (1968).