ZASTOSOWANIA MATEMATYKI
VII (1963)

J. NOWAK i M. WOJTAS (Wrocław)

*O KODACH MAKSYMALNYCH KORYGUJĄCYCH BŁĘDY**

Macierz prostokątną

$$\begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{bmatrix},$$

której każdy element jest 0 lub 1, nazywać będziemy *kodem*. *Odległością* d_{ij} między wierszami i-tym oraz j-tym kodu nazywać będziemy liczbę miejsc, w których te wiersze się różnią. Przez $A(n, d)$ oznaczmy każdy kod spełniający warunek $d_{ij} \geqslant d$ dla $1 \leqslant i, j \leqslant m$ $i \neq j$. Kod taki będziemy nazywali *kodem korygującym błędy*. Przez $\bar{A}(n, d)$ oznaczamy ilość wierszy kodu $A(n, d)$, a więc $\bar{A}(n, d) = m$. $B(n, d)$ oznacza macierz $[b_{ij}]$ zależną od kodu $A(n, d)$, gdzie

$$b_{ij} = \begin{cases} 1, & \text{gdy} \quad a_{ij} = 1, \\ -1, & \text{gdy} \quad a_{ij} = 0. \end{cases}$$

Wprowadźmy następujące dwa oznaczenia:

$$k_{ij} = \sum_{l=1}^{n} b_{il} b_{jl} \tag{1}$$

oraz

$$B^2(n, d) = B(n, d) B^T(n, d),$$

gdzie $B^T(n, d)$ jest macierzą transponowaną macierzy $B(n, d)$.

LEMAT 1. $\qquad k_{ij} = n - 2d_{ij}.$

Dowód. Wybierzmy wiersz i-ty oraz j-ty kodu $A(n, d)$ i odpowiadające im dwa wiersze macierzy $B(n, d)$. Wiersze te różnią się w d_{ij} miejscach, a w $n - d_{ij}$ są identyczne. Stąd $k_{ij} = -d_{ij} + (n - d_{ij}) = n - 2d_{ij}$.

---

* Praca referowana na seminarium kierowanym przez doc. J. Bromirskiego i prof. dra J. Słupeckiego.

LEMAT 2. *Jeżeli macierz kwadratowa symetryczna* $[a_{ij}]$ *stopnia* n *jest nieujemnie określona, to*

$$\sum_{1\leqslant i,j\leqslant n} a_{ij} \geqslant 0.$$

Dowód. Dodajmy do n-tego wiersza macierzy $[a_{ij}]$ wszystkie pozostałe wiersze, a w otrzymanej macierzy dodajmy do n-tej kolumny wszystkie pozostałe kolumny. Jak łatwo zauważyć, otrzymana macierz

$$\begin{bmatrix} a_{11} & a_{12} & \dots & \sum_{j=1}^{n} a_{1j} \\ a_{21} & a_{22} & \dots & \sum_{j=1}^{n} a_{2j} \\ \dots & \dots & \dots & \dots \\ \sum_{i=1}^{n} a_{i1} & \sum_{i=1}^{n} a_{i2} & \dots & \sum_{1\leqslant i,j\leqslant n} a_{ij} \end{bmatrix}$$

jest znowu nieujemnie określona, a więc $\sum_{1\leqslant i,j\leqslant n} a_{ij} \geqslant 0$, jako minor główny stopnia pierwszego.

TWIERDZENIE 1.

$$\bar{A}(n,d) \leqslant \frac{2d}{2d-n} \qquad dla \qquad 2d > n.$$

Dowód. Rozpatrzmy macierz

$$B^2(n,d) = \begin{bmatrix} n & k_{12} & \dots & k_{1m} \\ k_{21} & n & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & n \end{bmatrix}, \qquad m = \bar{A}(n,d),$$

gdzie k_{ij} jest określone przez (1). Macierz $B^2(n,d)$ jest nieujemnie określona, a więc na podstawie lematu 2

$$mn + \sum_{i\neq j} k_{ij} \geqslant 0.$$

Stąd i z lematu 1 wynika, że

$$mn + \sum_{i\neq j} (n - 2d_{ij}) \geqslant 0.$$

Ponieważ dla $i \neq j$ $d_{ij} \geqslant d$, więc $mn+m(m-1)(n-2d) \geqslant 0$ i ostatecznie

$$m = \bar{A}(n, d) \leqslant \frac{2d}{2d-n} \quad \text{dla} \quad 2d > n.$$

Inny dowód tego twierdzenia podał M. Płotkin w pracy [1].

Kod o parametrach n, d mający maksymalną ilość wierszy nazywamy *maksymalnym*. Odtąd przez $A(n, d)$ będziemy oznaczali kod maksymalny.

Dla kodów maksymalnych $\bar{A}(n, d)$ jest liczbą parzystą [1]. Z twierdzenia 1 wynika więc, że

$$\bar{A}(n, d) \leqslant 2\left[\frac{d}{2d-n}\right] \quad \text{dla} \quad 2d > n. \tag{1a}$$

Korzystając z tej nierówności i nierówności (por. [1])

$$\bar{A}(n+1, d) \leqslant 2\bar{A}(n, d) \tag{2}$$

w przypadku, gdy $n = 2d$, otrzymujemy

$$\bar{A}(n, d) = \bar{A}\big((n-1)+1, d\big) \leqslant 2\bar{A}(n-1, d) \leqslant$$

$$\leqslant 4\frac{d}{2d-(n-1)} = 4d = 2n,$$

to znaczy

$$\bar{A}(n, d) \leqslant 2n. \tag{1b}$$

Dla d nieparzystych oszacowania te można poprawić wykorzystując równość (por. [2])

$$\bar{A}(n+1, d+1) = \bar{A}(n, d), \quad d \text{ nieparzyste},$$

a mianowicie

$$\bar{A}(n, d) \leqslant 2\left[\frac{d+1}{2d+1-n}\right] \quad \text{dla} \quad 2d+1 > n, \tag{1c}$$

$$\bar{A}(n, d) \leqslant 2(n+1) \quad \text{dla} \quad 2d+1 = n. \tag{1d}$$

W. J. Lewensztejn w pracy [3] podał warunki dostateczne na to, by w (1a)-(1d) zachodziły równości.

Macierzą regularną (por. [3]) stopnia n nazywamy macierz, która powstaje z macierzy typu Hadamarda (1) przez zamianę w niej elementów -1 na 0. Jeżeli W_n jest macierzą regularną rzędu n, to przez $-W_n$ będziemy

(1) *Macierzą typu Hadamarda* nazywamy macierz kwadratową $[b_{ij}]$, $1 < i, j < n$, $b_{ij} = \pm 1$, której wiersze są ortogonalne, tj. $\sum_{j=1}^{n} b_{ij}b_{kj} = 0$ dla $i \neq k$.

oznaczali macierz, która powstaje z W_n przez zamianę w niej 0 na 1 oraz 1 na 0.

LEMAT 3. *Łatwo sprawdzić, że zachodzi równość*

$$\begin{vmatrix} n & & 0 & a_1 \\ & \ddots & & \vdots \\ 0 & & \ddots & \\ & & n & a_n \\ a_1 & \dots & a_n & n \end{vmatrix} = n^{n-1}\Big(n^2 - \sum_{i=1}^{n} a_i^2\Big).$$

LEMAT 4. *Jeżeli zachodzi następująca nierówność*

$$|a_{ii}| > \sum_{\substack{j=1 \\ j\neq 1}}^{n} |a_{ij}|$$

dla $i = 1, 2, \dots n$, *to*

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} \neq 0.$$

Dowód lematu można znaleźć w pracy [4].

LEMAT 5. *Jeżeli d jest liczbą parzystą, to wśród kodów maksymalnych* $A(n, d)$ *istnieje taki, w którym* d_{ij} *są liczbami parzystymi* (2).

Dowód. Zauważmy, że jeżeli łączna ilość jedynek w dwóch wierszach jest liczbą parzystą (nieparzystą), to odległość między tymi wierszami jest też liczbą parzystą (nieparzystą). Podzielmy wiersze kodu $A(n, d)$ na dwie grupy. Do pierwszej zaliczmy te wiersze, które mają parzystą ilość jedynek, a do drugiej te, które mają nieparzystą ilość jedynek. Odległości między wierszami w każdej z grup, jak uczy uwaga, są liczbami parzystymi, a między wierszami z grup różnych są liczbami nieparzystymi, a więc są równe co najmniej $d+1$. Negując (3) w jednej z grup dowolną kolumnę otrzymujemy żądany kod.

TWIERDZENIE 2. *Jeżeli d jest liczbą parzystą,* $2d = n$, *oraz istnieje macierz typu Hadamarda stopnia n, to*

$$A(n, d) = \begin{bmatrix} W_n \\ -W_n \end{bmatrix}.$$

---

(2) Dowód tego lematu, podany przez prof. J. Słupeckiego, nie był nigdzie publikowany.

(3) Przez *negację* kolumny (wiersza) rozumiemy zamianę w tej kolumnie (wierszu) wszystkich 0 na 1, a 1 na 0.

Dowód. Wystarczy wykazać, iż macierz $B^2(n, d)$ jest postaci

$$\left[\begin{array}{cc:cc} n & & -n & \\ & n & & -n \\ & \ddots & & \ddots \\ 0 & n & 0 & -n \\ \hdashline -n & & n & \\ & -n & & n \\ & \ddots & & \ddots \\ 0 & -n & 0 & n \end{array}\right]$$

Ilość jedynek w ostatniej kolumnie kodu $A(n, d)$ jest równa ilości zer, tzn. n. Gdyby tak nie było, istniałby wbrew (1a) kod spełniający warunek $\bar{A}(n-1, d) > n$. Rozpatrzmy kod złożony z tych wierszy kodu $A(n, d)$, których ostatnie elementy są 0. Udowodnimy, że kod ten jest macierzą regularną; oznaczymy ją przez W_n^0 (kod złożony z pozostałych wierszy kodu $A(n, d)$ oznaczymy przez W_n^1). Usuńmy z W_n^0 ostatnią kolumnę. Jak łatwo zauważyć, otrzymaliśmy kod maksymalny $A(n-1, d)$. Macierz $B^2(n-1, d)$ zależna od kodu $A(n-1, d)$ jest postaci

$$\begin{bmatrix} n-1 & k_{12} & \dots & k_{1n} \\ k_{21} & n-1 & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{n1} & k_{n2} & \dots & n-1 \end{bmatrix},$$

gdzie, w myśl lematu 1,

$$k_{ij} = (n-1)-2d_{ij} \leqslant (n-1)-n = -1 \quad \text{dla} \quad i \neq j. \tag{3}$$

Z lematu 2 otrzymujemy

$$n(n-1)+\sum_{1\leqslant i,j\leqslant n, i\neq j} k_{ij} \geqslant 0,$$

a na podstawie (3)

$$0 \leqslant n(n-1)+\sum_{1\leqslant i,j\leqslant n, i\neq j} k_{ij} \leqslant n(n-1)+n(n-1)(-1) = 0.$$

Stąd i z (3) wynika, że $k_{ij} = -1$ dla $1 \leqslant i, j \leqslant n, i \neq j$, tzn.

$$B^2(n-1, d) = \begin{bmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \dots & -1 \\ \dots & \dots & \dots & \dots \\ -1 & -1 & \dots & n-1 \end{bmatrix},$$

a więc iloczyn macierzy zależnej od W_n^0 i jej macierzy transponowanej jest równy

$$\begin{bmatrix} n & & 0 \\ & n & \\ & \ddots & \\ 0 & & n \end{bmatrix},$$

czyli W_n^0 jest macierzą regularną. Należy jeszcze wykazać, że $W_n^1 = -W_n^0$. Weźmy kod złożony z W_n^0 oraz i-tego wiersza kodu W_n^1 $(n+1 \leqslant i \leqslant 2n)$. Macierz zależną od tego kodu oznaczmy przez $B_i(n, d)$. Zbadajmy macierz

$$B_i^2(n, d) = \left[\begin{array}{ccc:c} n & & 0 & k_{1i} \\ & n & & \vdots \\ & \ddots & & \\ 0 & & n & k_{ni} \\ \hdashline k_{i1} & \dots & k_{in} & n \end{array}\right],$$

gdzie k_{ij} jest określone przez (1). Wyznacznik tej macierzy jest równy 0, gdyż ilość wierszy macierzy $B_i(n, d)$ jest większa od ilości kolumn. Wobec lematu 3

$$B_i^2(n, d) = n^{n-1}\left(n^2 - \sum_{j=1}^{n} k_{ij}^2\right) = 0,$$

a więc

$$\sum_{j=1}^{n} k_{ij}^2 = n^2 \quad \text{dla} \quad n+1 \leqslant i \leqslant 2n.$$

Z lematu 4 otrzymujemy

$$\sum_{j=1}^{n} |k_{ij}| \geqslant n \quad \text{dla} \quad n+1 \leqslant i \leqslant 2n. \tag{4}$$

Ponieważ $2d_{ij} \geqslant n$, więc $k_{ij} = n - 2d_{ij} \leqslant 0$ dla $i \neq j$. Stąd i z (4) wynika, że

$$\sum_{j=1}^{n} k_{ij} \leqslant -n, \quad n+1 \leqslant i \leqslant 2n, \tag{5}$$

a z (5), że

$$\sum_{1 \leqslant i,j \leqslant 2n, i \neq j} k_{ij} \leqslant -2n^2,$$

a więc suma wszystkich elementów macierzy $B^2(n, d)$ spełnia nierówność

$$2n^2 + \sum_{1 \leqslant i,j \leqslant 2n, i \neq j} k_{ij} \leqslant 0. \tag{6}$$

Wobec lematu 2 suma ta musi być nieujemna. W (6), a zatem i w (5), musi więc zachodzić równość. Z warunków

$$\sum_{j=1}^{n} k_{ij}^2 = n^2 \quad \text{i} \quad \sum_{j=1}^{n} k_{ij} = -n \quad \text{dla} \quad n+1 \leqslant i \leqslant 2n$$

wynika, że dla każdego i spełniającego nierówność $n+1 \leqslant i \leqslant 2n$ w ciągu $k_{i1}, k_{i2}, \ldots, k_{in}$ dokładnie jeden wyraz jest równy $-n$, a pozostałe są równe 0. W podobny sposób wykazujemy, że dla każdego j spełniającego nierówność $n+1 \leqslant j \leqslant 2n$ w ciągu $k_{1j}, k_{2j}, \ldots, k_{nj}$ dokładnie jeden wyraz jest równy $-n$, a pozostałe są równe 0. Stąd w każdym wierszu i w każdej kolumnie macierzy $B(n, d)$ poza główną przekątną jest tylko jeden element równy $-n$, pozostałe są równe 0. Po ewentualnym przestawieniu wierszy w kodzie $A(n, d)$ macierz $B(n, d)$ zależna od tego kodu przybierze postać (4). Tym sposobem zakończono dowód twierdzenia.

Niech w_i będzie i-tym wierszem kodu $A(n, d)$, $-w_i$ jego negacją. Zauważmy, że jeżeli odległość dwóch wierszy w_i oraz w_j kodu jest równa d_{ij}, to odległość wierszy $-w_i$ oraz w_j jest równa $n-d_{ij}$.

TWIERDZENIE 3. *Jeżeli d jest liczbą parzystą, $n = 2d$ oraz $\bar{A}(n, d) = 2n$, to $\bar{A}(n+1, d) < 4n$ dla $n > 4$.*

Dowód: Z (2) i (1b) wynika, że $\bar{A}(n+1, d) \leqslant 4n$. Wykażemy, że $\bar{A}(n+1, d) < 4n$ dla $n > 4$([4]). Przypuśćmy, że $\bar{A}(n+1, d) = 4n$. Wybierzmy taki kod maksymalny $A(n+1, d)$, żeby dla $1 \leqslant i, j \leqslant 4n$, $i \neq j$, d_{ij} były liczbami parzystymi. Istnienie takiego kodu zapewnia lemat 5. Rozpatrzmy jedną z kolumn kodu $A(n+1, d)$, np. ostatnią. Ilości jedynek i zer w tej kolumnie są równe. Gdyby tak nie było mielibyśmy $\bar{A}(n, d) > 2n$. Po ewentualnym przestawieniu wierszy kod $A(n+1, d)$ można przedstawić w postaci

$$A(n+1, d) = \left[\begin{array}{c|c} & 0 \\ A_0 & \vdots \\ & 0 \\ \hline & 1 \\ A_1 & \vdots \\ & 1 \end{array}\right],$$

gdzie macierze A_0 i A_1 są kodami maksymalnymi $A(n, d)$, przy czym $n = 2d$.

W kodzie

$$A'(n+1, d) = \left[\begin{array}{c} A_0 \\ \hline A_1 \end{array}\right]$$

([4]) Dla $n = 4$ wykazano w [2], że $\bar{A}(n+1, d) = 4n$, tzn. $\bar{A}(5,2) = 16$.

odległości d_{ij} spełniają warunki

$$d_{ij} \geqslant d-1 \tag{7}$$

dla

$$\begin{aligned} &1 \leqslant i \leqslant 2n \quad \text{i} \quad 2n+1 \leqslant j \leqslant 4n; \\ &2n+1 \leqslant i \leqslant 4n \quad \text{i} \quad 1 \leqslant j \leqslant 2n, \end{aligned} \tag{8}$$

oraz $d_{ij} \geqslant d$ dla pozostałych i, j.

Jeżeli w macierzy A_1 występuje wiersz w_i, to z twierdzenia 2 wynika, że występuje w niej też wiersz $-w_i$. Aby dowolny wiersz w_i macierzy A_0 spełniał z wierszem w_j tej macierzy oraz z negacją tego wiersza warunki (7), muszą zachodzić nierówności $d-1 \leqslant d_{ij} \leqslant d+1$ dla i, j spełniających (8). Wynikają one z uwagi podanej bezpośrednio przed twierdzeniem 3. Weźmy teraz macierz $B'(n+1, d)$ zależną od $A'(n+1, d)$, a następnie $B'^2(n+1, d)$. Elementy k_{ij} tej macierzy spełniają nierówności $-2 \leqslant k_{ij} \leqslant 2$ dla i, j spełniających (8).

Równocześnie $k_{ij} \neq 0$, gdyż $k_{ij} = n-2d_{ij}$, liczba n jest podzielna przez 4, a d_{ij} są liczbami nieparzystymi. Stąd $k_{ij} = \pm 2$. Z twierdzenia 2 wynika, że A_1 można przedstawić w postaci

$$\begin{bmatrix} W_n^0 \\ \cdots \\ -W_n^0 \end{bmatrix},$$

gdzie W_n^0 jest macierzą regularną.

Utwórzmy kod z n wierszy kodu W_n^0 i dowolnego, np. 1-ego, wiersza macierzy A_0; iloczyn macierzy zależnej od tego kodu i jej macierzy transponowanej jest

$$\left[\begin{array}{ccc:c} n & & 0 & k_{1n} \\ & n & & \vdots \\ & & \ddots & \\ 0 & & n & k_{nn} \\ \hdashline k_{n1} & \cdots & k_{nn} & n \end{array}\right],$$

gdzie $k_{in} = k_{ni} = \pm 2$, $i = 1, 2, \ldots, n$.

Wyznacznik W ostatniej macierzy jest równy 0; równocześnie z lematu 3 otrzymujemy

$$W = n^{n-1}\left(n^2 - \sum_{i=1}^{n} k_{in}^2\right) = n^{n-1}(n^2-4n) \neq 0 \quad \text{dla} \quad n \neq 4,$$

a więc nie może być $\bar{A}(n+1, d) = 4n$, gdy $n = 2d \neq 4$.

WNIOSEK. *Gdy* $A(n+1, d)$ *jest kodem grupowym*(5), $n = 2d = 2^k$, $k > 2$, *to*

$$\bar{A}(n+1, d) \leqslant 2n.$$

Wykorzystując wielokrotnie (2) otrzymujemy

$$\bar{A}(n, d) \leqslant 2^{n-2d+1}d \quad \text{dla} \quad n \geqslant 2d+1.$$

Prace cytowane

[1] M. Plotkin, *Binary codes with specified minimum distance*, IRE Trans. on Information Theory IT-6 (1960), str. 445-460.

[2] R. W. Hamming, *Error detecting and error correcting codes*, Bell Syst. Tech. J. 29 (1950), str. 147-160.

[3] В. И. Левенштейн, *Применение матриц Адамара к одной задаче кодирования*, Проблемы кибернетики 5 (1961), str. 123-136.

[4] M. Parodi, *La localisation des valeurs caractéristiques des matrices et ses applications*, Paris 1959, str. 15-16.

Praca wpłynęła 7. 11. 1962

Е. НОВАК и М. ВОЙТАС (Вроцлав)

О МАКСИМАЛЬНЫХ КОДАХ ИСПРАВЛЯЮЩИХ ОШИБКИ

РЕЗЮМЕ

Главным результатом работы является

ТЕОРЕМА. *Пусть* d *— чётное число,* $n = 2d$, *и пусть* $A(n, d)$ *будет максимальным двоичным кодом с* n*-битовыми строками, расстояние которых не меньше* d. *Предположим, что существует* n*-мерная матрица Адамара порядка* n (см. [3]). *Тогда* $A(n, d)$ *отличается, по крайней мере только очередностью строк от матрицы* $\begin{bmatrix} W_n \\ -W_n \end{bmatrix}$, *где* W_n *— правильная матрица* (см. [3]) *с* n*-строками, а* $(-W_n)$ *есть матрицей, которая одразуется из* W_n *посредством замены* 0 *на* 1 *и* 1 *на* 0.

Из этой теоремы следуют некоторые выводы относящиеся к количеству строк в максимальных кодах.

В работе приводится простое доказательство неравенства Плоткина (см.[1]).

---

(5) Pojęcie kodu grupowego omówione jest w pracy [2].

J. NOWAK and M. WOJTAS (Wrocław)

ON MAXIMAL ERROR-CORRECTING CODES

SUMMARY

The main result of this paper is the following

THEOREM: *Let d be an even integer, $n = 2d$, and let $A(n, d)$ be a maximal binary code with rows of length n, all of whose distances are not less than d. Let us suppose that there exists a Hadamard matrix* (see [3]) *of order n. Then $A(n, d)$ differs at most in the successive order of rows from the matrix* $\begin{bmatrix} W_n \\ -W_n \end{bmatrix}$, *where W_n denotes a regular matrix* (see [3]) *of order n and $-W_n$ is the matrix obtained from W_n by replacing* 0 *by* 1 *and* 1 *by* 0.

This theorem implies certain conclusions regarding the number of rows in maximal codes.

The paper contains also a simple proof of an inequality of Plotkin (see [1]).