# Kody korekcyjne: Lista 3

18 października 2023

**Definicja .1.**

$$A_q(n,d) = \max\{M : \text{ istnieje } (n,M,d)_q \text{ kod}\}$$
$$B_q(n,d) = \max\{q^k : \text{ istnieje } [n,k,d]_q \text{ kod}\}$$

**Zadanie 1.** Pokaż, że $A_q(n,d) \leq qA_q(n-1,d)$.

**Zadanie 2.** Pokaż, że jeśli $d$ jest nieparzyste, to:

1. $(n,M,d)_2$-kod istnieje $\iff$ $(n+1,M,d+1)_2$ kod istnieje.
2. $[n,k,d]_2$-kod istnieje $\iff$ $[n+1,k,d+1]_2$ kod istnieje.

*Wskazówka*: Kod rozszerzony i dziurawienie kodu.

**Zadanie 3.** Niech $C$ będzie $[n,k,2e+1]_2$-kodem.

1. Pokaż, że $C$ jest doskonały wtedy i tylko wtedy, gdy każdy wektor $v \in \mathbb{F}_2^{n-k}$ można przedstawić w jedyny sposób jako sumę najwyżej $e$ kolumn z $H_C$.
2. Pokaż, że jeśli $C$ jest doskonały, to niezerowe słowa kodowe w $C^\perp$ przyjmują co najwyżej $e$ różnych wag (Hamminga).

Użyj części 1.
Co mniesz powiedzieć o kodzie, którego macierz parzystości ma jako kolumny wszystkie sumy najwyżej $e$ kolumn $H$?
*Wskazówka*: Część 1 jest prosta.
Część 2: najpierw pokaż dla $e = 1$.

**Zadanie 4.** Pokaż, że dla wybranej losowo macierzy parzystości $H$ rozmiaru $(n-k) \times n$ o elementach z $\mathbb{F}_q$ jej kod osiąga ograniczenie GV (wersja Verschamova).

Losowo, czyli każdy element losujemy jednostajnie nad $\mathbb{F}_q$.

**Zadanie 5** (Ograniczenie Griesmera)**.** Pokaż, że jeśli istnieje $[n,k,d]_q$-kod, to istnieje również $[n-d, k-1, d']_q$ kod dla pewnego $d' \geq \lceil d/q \rceil$.

Wywniskuj z tego, że jeśli istnieje $[n,k,d]_q$-kodem, to

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

**Zadanie 6.** Ograniczenie Singletona w wersji dla kodów liniowych tłumaczy się na stwierdzenie, że $[n,k,d]$ kod spełnia warunek $k+d \leq n+1$. Udowodnij to twierdzenie rozważając macierz parzystości $H_C$ kodu $C$.

*Wskazówka*: Ile kolumn niezależnych może mieć $H_C$?

**Zadanie 7.** Niech $C$ będzie $[n,k,d]_q$ kodem liniowym. Niech $G, H$ będą, odpowiednio, jego macierzami generującymi oraz macierzą parzystości. Pokaż, że następujące warunki są równoważne:

1. $C$ jest MDS (z zadania powyżej: spełnia warunek $k+d = n+1$);
2. każde $n-k$ kolumn $H$ jest liniowo niezależnych;
3. każde $k$ wierszy $G$ jest liniowo niezależnych;
4. $C^\perp$ jest MDS.

Wskazówki, bez nich trochę trudniej:
Co możesz powiedzieć o powstałej w ten sposób macierzy $k \times k$?
Pokaż, że wymazanie $n-k$ współrzędnych odpowiada wymazaniu $n-k$ wierszy z macierzy generatorów. Co możesz powiedzieć o kolumnach tej macierzy, w których $w$ ma 0?
Alternatywnie: pokaż implikację 1 w 4: skoro kod ma odległość $n+1-k$ to poprawia $n-k$ błędów wymazania.
Rozważ $w \in C^\perp$ o minimalnej wadze. Ile ma zer? Weź macierz parzystości, w której $w$ jest wierszem. Co możesz powiedzieć o kolumnach tej macierzy, w których $w$ ma 0?
*Wskazówka*: Równoważność 1 i 2 wynika z poprzedniego zadania, podobnie 3 i 4. Implikacja 1 w 4:

**Zadanie 8.** Pokaż, że jeśli $C$ jest binarnym kodem MDS, to

- $C = \mathbb{F}_q^n$ lub
- $C$ jest generowany przez $(1, \ldots, 1)^T$ lub
- $C$ jest dualny do powyższego kodu.

**Zadanie 9.** Pokaż, że dla dodatnich liczb $n_1, \ldots, n_q$ zachodzi

$$\sum_{i=1}^{q} n_i^2 \geq \frac{(\sum_i n_i)^2}{q} \ .$$

**Zadanie 10.** Pokaż, że dla $q = 2$ istnieją tylko następujące liniowe kody MDS:

- $\mathbb{F}_q^n$
- kod powtórzeniowy, czyli generowany przez $(1, \ldots, 1)^T$
- kod dualny do kodu generowany przez $(1, \ldots, 1)^T$ (czyli kod kontroli parzystości).

*Wskazówka:* Zadanie 7, rozważ macierze w postaci standardowej.

**Zadanie 11** (Ograniczenie Plotkina dla $q = 2$)**.** Pokaż, że jeśli $d$ jest parzyste, to

$$A_2(n,d) \leq \begin{cases} 2\left\lfloor \frac{d}{2d-n} \right\rfloor & \text{, dla } n < 2d \\ 4d & \text{, dla } n = 2d \end{cases} \ .$$

Pokaż, że jeśli $d$ jest nieparzyste, to

$$A_2(n,d) \leq \begin{cases} 2\left\lfloor \frac{d+1}{2d+1-n} \right\rfloor & \text{, dla } n < 2d+1 \\ 4d+4 & \text{, dla } n = 2d+1 \end{cases} \ .$$

*Wskazówka:* Przypadek $p$ nieparzystego sprowadź do parzystego przez Zadanie 2. W parzystym dokładnej przeanalizuj szacowania, użyj Zadania 1.

**Zadanie 12.** Głównym problemem ograniczenia Plotkina jest to, że działa tylko dla kodów o dużych odległościach.

Udowodnij, że można z niego wywnioskować wersję, która działa też dla mniejszych odległości: Jeśli $d = \Delta(C) \leq \frac{q-1}{q} n$, gdzie $n$ to długość kodu a $q$-rozmiar alfabetu, to

$$|C| \leq q^{n - \lceil d \frac{q}{q-1} \rceil d} \ .$$

*Wskazówka:* Podziel kod na wiele kodów, grupując wg. prefiksów odpowiedniej długości, tak aby móc dla każdego z nich zastosować ograniczenie Plotkina. Zsumuj ograniczenia i oszacuj.