Kody korekcyjne: Lista 2

10 października 2019

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

Zadanie 2. Dla kodu liniowego C jego kod rozszerzony powstaje przez dopisanie bitu kontroli parzystości, formalnie:

$$\overline{C} = \{(c_1, \ldots, c_k, -\sum_{i=1}^{k} c_i) \ : \ c_1, \ldots, c_k \in C\} \ .$$

Pokaż, że jest to kod liniowy. Jak wygląda jego macierz parzystości? Pokaż też, że

$$\mathrm{d_H}(C) \leq \mathrm{d_H}(\overline{C}) \leq \mathrm{d_H}(C) + 1 \ .$$

Jak jest odległość rozszerzonego kodu Hamminga? Zinterpretuj kod Hadamarda jako kod rozszerzony.

Zadanie 3. Pokaż, że jeśli d jest nieparzyste, to:

1. $(n,M,d)_2$-kod istnieje $\iff$ $(n+1,M,d+1)_2$ kod istnieje. W szczególności:

$$A_2(n+1,d+1) = A_2(n,d) \ .$$

2. $[n,k,d]_2$-kod istnieje $\iff$ $[n+1,k,d+1]_2$ kod istnieje. W szczególności:

$$B_2(n+1,d+1) = B_2(n,d) \ .$$

Wskazówka: Zadanie 2 oraz „odwrotność”, tj. usuwanie pewnej współrzędnej.

Zadanie 4. Pokaż, że jeśli macierz generatorów jest w postaci standardowej $G_C = \begin{bmatrix} X \\ \mathrm{Id} \end{bmatrix}$, to macierz

$$[\mathrm{Id} \,|\, -X]$$

jest macierzą parzystości tego kodu.

Zadanie 5. Pokaż, że jeśli $(n,M,d)_q$-kod jest maksymalny i nietrywialny (tj. nie jest całą przestrzenią, ani nie jest jednoelementowy), to d jest nieparzyste.

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:

Wskazówka: Równoważność 1 i 2 wynika z poprzedniego zadania, podobnie 3 i 4. Implikacja 1 w 4: rozważ niezerowe słowo kodowe $w \in C^\perp$ 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? Alternatywnie: pokaż implikację 1 w 4: skoro kod ma odległość $n+1-k$ to poprawia $n-k$ błędów wymazania. Pokaż, że wymazanie $n-k$ współrzędnych odpowiada wymazaniu $n-k$ wierszy z macierzy generatorów. Co możesz powiedzieć o powstałej w ten sposób macierzy $k \times k$?

Zadanie 8. 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 9 (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 d nieparzystego sprowadź do parzystego przez Zadanie 3. W parzystym dokładniej przeanalizuj szacowania, użyj Zadania 1.

Zadanie 10 (Być może trudne)**.** 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).

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

Zadanie 11. Porównaj dwie wersje ograniczenia GV.