Kody korekcyjne, czyli jak można wykryć i poprawić błąd w przesyłanej informacji

MiNI Akademii Matematyki
Wydział Matematyki i Nauk Informacyjnych PW
Agata Pilitowska

Metody kodowania

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Dla $\boldsymbol{c} = (c_1, \ldots, c_n)$ i $\boldsymbol{f} = (f_1, \ldots, f_n)$, gdzie $c_i, f_i \in \{0, 1\}$, definiujemy działania:

$$\boldsymbol{c} + \boldsymbol{f} := (c_1 +_2 f_1, \ldots, c_n +_2 f_n)$$

$$\boldsymbol{c} \cdot \boldsymbol{f} := (c_1 \cdot_2 f_1, \ldots, c_n \cdot_2 f_n)$$

Kod $\mathcal{C}$ nazywamy *liniowym*, jeśli dla $\boldsymbol{c}, \boldsymbol{f} \in \mathcal{C}$, również $\boldsymbol{c} + \boldsymbol{f} \in \mathcal{C}$.

1. Binarny kod kontroli parzystości długości n powstaje przez dodanie na końcu każdej wysyłanej wiadomości $(c_1, \ldots, c_{n-1})$, dodatkowego symbolu $c_n := \sum_{i=1}^{n-1} c_i (mod 2)$.

   (a) Znaleźć wszystkie słowa kodowe binarnego kodu kontroli parzystości dla $n = 4$.
   Jaka jest odległość takiego kodu?

   (b) Znaleźć odległość binarnego kodu kontroli parzystości dla dowolnego $n \in \mathbb{N}$.

2. Niech H_m będzie tablicą, której i-ta kolumna jest binarną reprezentacją liczby $1 \leqslant i \leqslant 2^m - 1$ zapisaną "z dołu do góry". Niech dla $i = 1, \ldots, m$, $\boldsymbol{w}_i = (w_{i1}, \ldots, w_{in})$ będzie i-tym wierszem tej tablicy. Dla każdego $i = 1, \ldots, m$ utwórzmy równanie o $n = 2^m - 1$ zmiennych $c_1, \ldots, c_n$:

$$w_{i1}c_1 + w_{i2}c_2 + \ldots + w_{in}c_n = 0. \tag{0.0.1}$$

Kodem Hamminga $\mathcal{H}_m$ nazywamy kod długości $n = 2^m - 1$ o m symbolach sprawdzających: $c_1, c_2, c_4, \ldots, c_{2^{m-1}}$, dla którego wektor $\boldsymbol{c} \in \mathcal{H}_m$ wtedy i tylko wtedy, gdy spełnia każde z równań (**??**).

(a) Znaleźć równania definiujące symbole sprawdzajace (c_1, c_2, c_4) w kodzie Hamminga $\mathcal{H}_3$.

(b) Sprawdzić, czy $\boldsymbol{c} = (1, 1, 1, 1, 0, 0, 1, 1)$ i $\boldsymbol{f} = (1, 1, 0, 0, 1, 0, 1, 1)$ są słowami kodowymi kodu $\mathcal{H}_3$.

(c) Wiedząc, że podczas transmisji został popełniony tylko jeden błąd odkodować wektor: $(0, 0, 1, 1, 1, 1, 1)$.

(d) Znaleźć wszystkie słowa kodowe kodu $\mathcal{H}_3$.

(e) Jaka jest odległość kodu $\mathcal{H}_3$?

(f) Obliczyć, ile jest wszystkich słów kodowych wagi $w = 1, 2, 3, 4, 5, 6, 7$ w kodzie Hamminga $\mathcal{H}_3$.

3. Pokazać, że w liniowym kodzie binarnym albo wszystkie słowa kodowe mają parzystą wagę, albo dokładnie połowa z nich ma wagę parzystą a połowa nieparzystą.

Odległość kodu

Niech $\boldsymbol{c}$ i $\boldsymbol{f}$ będą wektorami binarnymi długości n.

1. Pokazać, że $wt(\boldsymbol{c} + \boldsymbol{f}) = wt(\boldsymbol{c}) + wt(\boldsymbol{f}) - 2wt(\boldsymbol{c} \cdot \boldsymbol{f})$.

2. Pokazać, że jeśli $wt(\boldsymbol{c}) = wt(\boldsymbol{f})$ to $d(\boldsymbol{c}, \boldsymbol{f})$ jest liczbą parzystą.

3. Sprawdzić, czy kod kontroli parzystości jest kodem liniowym.

4. Pokazać, że odległość kodu liniowego równa jest minimalnej wadze niezerowych słów kodowych.

5. Niech $\mathcal{C}$ będzie kodem binarnym, którego odległość d jest liczbą nieparzystą i niech $\widehat{\mathcal{C}} := \{(c_1, \ldots, c_n, c_{n+1}) \mid (c_1, \ldots, c_n) \in \mathcal{C},\ c_{n+1} = \sum_{i=1}^{n} c_i (mod 2)\}$ ($\widehat{\mathcal{C}}$ jest tzw. kodem rozszerzonym kodu $\mathcal{C}$). Pokazać, że $d(\widehat{\mathcal{C}}) = d + 1$.

6. Niech X będzie zbiorem n-elementowym zaś $\mathcal{B} = \{B_1, \ldots, B_n\}$ rodziną jego podzbiorów (zawnych blokami) taką, że $|B_i| = k < n - 1$ dla $1 \leqslant i \leqslant n$ oraz każdy dwu-elementowy zbiór $\{x, y\} \subseteq X$ jest podzbiorem dokładnie $\lambda > 0$ zbiorów spośród $B_1, \ldots, B_n$. Utwórzmy tablicę $A = (a_{ij})$,
$$a_{ij} := \begin{cases} 1, & \text{jeśli } x_i \in B_j, \\ 0, & \text{jeśli } x_i \notin B_j. \end{cases}$$
Niech $\boldsymbol{c}$ i $\boldsymbol{f}$ będą wierszmi tej tablicy traktowanymi jako wektory binarne długości n. Pokazać, że $d(\boldsymbol{c}, \boldsymbol{f}) = 2(k - \lambda)$.

Liczba słów kodowych

1. Obliczyć, jaka jest maksymalna liczba binarnych wektorów długości n, odległości co najmniej $2d$ i wagi równej $w < d$.

2. Obliczyć, jaka jest maksymalna liczba binarnych wektorów długości n, odległości co najmniej $2d$ i wagi równej $w = d$.

3. Pokazać, że binarnych wektorów długości n, odległości co najmniej $2d-1$ i wagi równej w jest tyle samo, co wszystkich binarnych wektorów długości n, odległości co najmniej $2d$ i wagi równej w.

Kody doskonałe

Niech $\mathcal{C}$ będzie binarnym kodem długości n, odległości co najmniej d, który ma 2^k słów kodowych. Kule $K(\boldsymbol{c}, t)$ o promieniu $t = [\frac{d-1}{2}]$ wokół słów kodowych $\boldsymbol{c} \in \mathcal{C}$ są rozłączne. Jeżeli w tych kulach $K(\boldsymbol{c}, t)$ mieszczą się wszystkie wektory binarne długości n, kod $\mathcal{C}$ nazywamy doskonałym.

1. Jaką długość muszą mieć binarne kody doskonałe poprawiające błędy pojedyncze?

2. Czy istnieje binarny kod doskonały poprawiajacy błędy podwójne?

3. Niech A_i będzie liczbą słów kodowych wagi i w binarnym kodzie $\mathcal{C}$. Niech $\mathcal{C}$ będzie kodem doskonałym długości n, poprawiającym błędy

pojedyncze. Pokazać, że dla każdego $0 \leqslant i \leqslant n$,

$$(i+1)A_{i+1} + A_i + (n-i+1)A_{i-1} = \binom{n}{i}.$$

4. Niech $\mathcal{C}$ będzie binarnym liniowym kodem doskonalym długości $n = 23$ i odległości $d = 7$. Obliczyć $A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9$.

5. Niech $\mathcal{C}$ będzie binarnym kodem doskonałym długości n, poprawiającym t błędów oraz zawierającym wektor zerowy $\mathbf{0}_n$. Niech $\boldsymbol{f}$ będzie binarnym wektorem długości n i wagi $t+1$. Pokazać, że istnieje dokładnie jedno słowo kodowe $\boldsymbol{c} \in \mathcal{C}$ wagi $2t+1$, które posiada 1 na tych samych pozycjach co wektor $\boldsymbol{f}$.