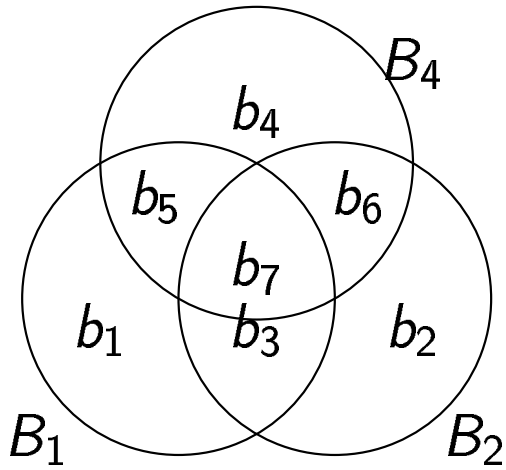
Kódelméleti és kriptográfiai alkalmazások

Wettl Ferenc

2015. május 14.

Bináris $[7, 4, 3]_2$ Hamming-kód

- $\mathbb{F}_2^4 \to \mathbb{F}_2^7 : (b_3, b_5, b_6, b_7) \mapsto (b_1, \ldots, b_7)$, ahol $b_1 = b_3 + b_5 + b_7$, $b_2 = b_3 + b_6 + b_7$, $b_4 = b_5 + b_6 + b_7$. Legyen B_1, B_2, B_4 három halmaz. B_{2^k} pontosan akkor tartalmazza a b_i bitet, ha i bináris alakjában a k-adik bit 1.



- Egy $(b_1, \ldots, b_7)$ bitsorozat pontosan akkor kódszó, ha a B_j $(j = 1, 2, 4)$ halmazok mindegyikében páros sok bit egyes.
- Bármely $\mathbb{F}_2^7$-beli vektor vagy kódszó, vagy egyértelműen kódszóvá változtatható egyetlen bit megváltoztatásával, azaz e kód képes egy bithibát javítani.

Feladat

7 halálraítélt körben ül, mindegyikük fején egy véletlenül kiválasztott piros vagy fekete sapka. Mindenki látja a többiek sapkáját, de senki se látja a sajátját. Semmi módon nem kommunikálhatnak egymással. Egy idő után egyszerre mindegyiküknek tippelnie kell a saját sapkája színére. Három válasz lehetséges: „nem tudom”, „fekete”, „piros”. Ha senki nem találja el, vagy csak egy is akad, aki téved, mind meghalnak, egyébként mind megmenekülnek. Tudunk-e számukra olyan eljárást javasolni, ami 1/2-nél nagyobb valószínűséggel megmenekíti őket. Mi a legnagyobb valószínűség, amit el tudunk érni?

Lineáris kód, generátormátrix

D Az $\mathbb{F}_q$ test fölött értelmezett $\mathcal{C} \subseteq \mathbb{F}_q^n$ kódot lineáris $[n, k]$-kódnak nevezzük, ha $\mathcal{C}$ az $\mathbb{F}_q^n$ vektortér egy k-dimenziós altere (ha d a minimális távolság, akkor $[n, k, d]_q$).

D Legyen $g_1, g_2, \ldots, g_k$ a $\mathcal{C}$ egy bázisa. Egy tetszőleges $x \in \mathbb{F}_q^k$ vektor (üzenet) $c \in \mathcal{C}$ kódja legyen $c = x_1 g_1 + x_2 g_2 + \cdots + x_k g_k$. Ez egy egyszerű mátrixszorzással is előállítható:

$$c = xG,$$

ahol a $k \times n$-es G mátrix – az úgynevezett generátormátrix – sorvektorai $\mathcal{C}$ bázisának elemei.

Hamming-kód használata

P Az $\mathbb{F}_2^4 \to \mathbb{F}_2^7 : (b_3, b_5, b_6, b_7) \mapsto (b_1, \ldots, b_7)$, ahol $b_1 = b_3 + b_5 + b_7$, $b_2 = b_3 + b_6 + b_7$, $b_4 = b_5 + b_6 + b_7$ leképezés mátrixa

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Például az $x = (0, 1, 1, 0)$ üzenet kódja

$$c = xG = \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Ellenőrző mátrix

D A $\mathcal{C}$ kód duálisán a

$$\mathcal{C}^{\perp} = \{ v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ minden } c \in \mathcal{C} \text{ kódszóra} \}$$

kódot értjük, mely egy lineáris kód. A $\mathcal{C}^{\perp}$ kód H generátormátrixát a $\mathcal{C}$ kód ellenőrző mátrixának nevezzük. (paritásmátrix, paritásellenőrző mátrix).

T Ha $\mathcal{C}$ egy lineáris $[n, k]$-kód, akkor

(1) $\mathcal{C}^{\perp} = \{ v \in \mathbb{F}_q^n : vG^T = 0 \}$,
(2) $\mathcal{C}^{\perp}$ egy $[n, n-k]$-kód,
(3) $\mathcal{C}^{\perp\perp} := (\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$,
(4) $\mathcal{C} = \{ c \in \mathbb{F}_q^n : cH^T = 0 \}$,
(5) $GH^T = O_{k \times n-k}$, $HG^T = O_{n-k \times k}$,
(6) ha $G = [I_k | A]$ a $\mathcal{C}$ kód standard alakú generátormátrixa, akkor ellenőrző mátrixa $H = [-A^T | I_{n-k}]$.

Bináris Hamming-kód ellenőrző mátrixa

- A generátormátrix a (34) permutációval $[A|I]$ alakot ölt, amelyhez az $[I|-A^T]$ ellenőrző mátrix tartozik. Ezen a (34) permutáció inverze – ami önmaga – a következő mátrixot adja:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{1}$$

Bináris Hamming-kód ellenőrző mátrixa

D Vegyünk egy olyan H mátrixot, melynek oszlopai között $\mathbb{F}_q^r$ minden nemnulla vektorának pontosan egy nem nulla konstansszorosa szerepel. Azt a kódot, melynek a H mátrix az ellenőrző mátrixa, r paraméterű $\mathbb{F}_q$ feletti $\mathrm{H}_{r,q}$ Hamming-kódnak nevezzük.

T A $\mathrm{H}_{r,q}$ Hamming-kód

$$\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1}-r, 3\right]_q$$

paraméterű perfekt kód (azaz a kódszó közepű r-sugarú gömbök egyrétűen lefedik a teret).

Általánosított Reed–Solomon-kód

- Reed és Solomon 1960-ban definiálta.

D Legyen $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}^n$ nemnulla elemű, $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$ csupa különböző elemből álló vektor ($n \leqslant |\mathbb{F}|$), és legyen $0 \leqslant k \leqslant n$ egész. Ekkor a

$$\mathrm{GRS}_{n,k}(a, v) = \{ (v_1 c(a_1), v_2 c(a_2), \ldots, v_n c(a_n)) \mid c(x) \in \mathbb{F}[x]_k \}$$

kódot általánosított Reed–Solomon-kódnak nevezzük. Itt a $c(x)$ polinomhoz tartozó kódszót fogjuk c-vel jelölni. (A $v = (1, 1, \ldots, 1)$ esetben e kódot Reed–Solomon-kódnak nevezzük.)

T $\mathrm{GRS}_{n,k}(a, v)$ lineáris $[n, k, n - k + 1]$-kód.