

Tiesiniai kodai

Baigtinio kūno sąvoka

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

$\mathbb{F}_p = \{0, 1, \dots, p-1\}$ - abėcėlė sudaryta iš p simbolių (p - pirminis).

Teorema. Aibėje \mathbb{F}_p suma ir sandauga modulių p turi šias savybes:

- 1) $(a + b) + c = a + (b + c)$;
- 2) $a + b = b + a$;
- 3) $a + 0 = a$;
- 4) $\forall a \in \mathbb{F}_p$ lygtis $a + x = 0$ turi vienintelį sprendinį;
- 5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- 6) $a \cdot b = b \cdot a$;
- 7) $a \cdot 1 = a$;
- 8) $\forall a \in \mathbb{F}_p, a \neq 0$, lygtis $a \cdot x = 1$ turi vienintelį sprendinį;
- 9) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Aibė, kurioje apibrėžti du veiksmi (sudėtis ir daugyba) turi teoremoje išvardytas savybes, vadinama kūnu.

Tiesinė erdvė

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

\mathbb{F}_p^n - abėcėlės \mathbb{F}_p ilgio n žodžių aibė. ($|\mathbb{F}_p^n| = p^n$)

- Žodžių $\mathbf{x} = x_1 \dots x_n \in \mathbb{F}_p^n$ ir $\mathbf{y} = y_1 \dots y_n \in \mathbb{F}_p^n$ suma vadinsime žodį $\mathbf{z} = z_1 \dots z_n \in \mathbb{F}_p^n$, čia $z_i = x_i + y_i$.
- Žodžio \mathbf{x} ir skaičiaus $\alpha \in \mathbb{F}_p$ sandauga vadinsime žodį $\mathbf{w} = w_1 \dots w_n \in \mathbb{F}_p^n$, $w_i = \alpha x_i$.

Tiesinė erdvė

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Teorema. Tegu $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_p^n$ ir $\alpha, \beta \in \mathbb{F}_p$. Teisingi šie teiginiai:

1) $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z});$

2) $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x};$

3) egzistuoja $\mathbf{0} \in \mathbb{F}_p^n$ kad $\mathbf{x} + \mathbf{0} = \mathbf{x};$

4) egzistuoja $\bar{\mathbf{x}} \in \mathbb{F}_p^n$ kad $\mathbf{x} + \bar{\mathbf{x}} = \mathbf{0};$

5) $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y};$

6) $(\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x};$

7) $(\alpha\beta)\mathbf{x} = \alpha(\beta\mathbf{x});$

8) $1\mathbf{x} = \mathbf{x}.$

Aibė su elementų sudėties ir daugybos iš kūno elementų operacijomis, tenkinančiomis 1) - 8) savybes, vadinama *tiesine erdve*.

Taigi \mathbb{F}_p^n yra tiesinė erdvė.

Tiesinis poerdvis

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Tiesinės erdvės \mathbb{F}_p^n poaibį \mathbf{L} vadinsime tiesiniu poerdviu, jeigu:

- $\mathbf{x}, \mathbf{y} \in \mathbf{L} \Rightarrow \mathbf{x} + \mathbf{y} \in \mathbf{L};$
- $\alpha \in \mathbb{F}_p, \mathbf{x} \in \mathbf{L} \Rightarrow \alpha \mathbf{x} \in \mathbf{L}.$

Apibrėžimas. Elementų $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m \in \mathbb{F}_p^n$ tiesiniu apvalku vadinsime aibę

$$\mathcal{L}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m) = \{\alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_m \mathbf{x}_m \mid \alpha_i \in \mathbb{F}_p\}$$

Tiesinis apvalkas $\mathcal{L}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m)$ yra \mathbb{F}_p^n tiesinis poerdvis.

Jei $\mathbf{e}_1 = 100\dots 00$, $\mathbf{e}_2 = 010\dots 00$, ..., $\mathbf{e}_n = 000\dots 01$,
tai $\mathcal{L}(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n) = \mathbb{F}_p^n$.

Tiesinio poerdvio dimensija

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Sakysime, kad žodžiai $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m \in \mathbb{F}_p^n$ yra tiesiškai nepriklausomi, jeigu lygybė

$$\alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_m \mathbf{x}_m = \mathbf{0}, \quad \mathbf{0} = 00\dots 0, \quad \alpha_i \in \mathbb{F}_p,$$

teisinga tik tuomet, kai $\alpha_1 = \alpha_2 = \dots = \alpha_m = 0$. Priešingu atveju sakysime, kad žodžiai yra tiesiškai priklausomi.

Tiesinio poerdvio dimensija

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Sakysime, kad žodžiai $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m \in \mathbb{F}_p^n$ yra tiesiškai nepriklausomi, jeigu lygybė

$$\alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_m \mathbf{x}_m = \mathbf{0}, \quad \mathbf{0} = 00\dots 0, \quad \alpha_i \in \mathbb{F}_p,$$

teisinga tik tuomet, kai $\alpha_1 = \alpha_2 = \dots = \alpha_m = 0$. Priešingu atveju sakysime, kad žodžiai yra tiesiškai priklausomi.

Apibrėžimas. Tiesiškai nepriklausomų žodžių sistemą $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m$ vadinsime tiesinio poerdvio $\mathbf{L} \subset \mathbb{F}_p^n$ baze, jei $\mathbf{L} = \mathcal{L}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m)$.

Tiesinio poerdvio dimensija

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Sakysime, kad žodžiai $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m \in \mathbb{F}_p^n$ yra tiesiškai nepriklausomi, jeigu lygybė

$$\alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_m \mathbf{x}_m = \mathbf{0}, \quad \mathbf{0} = 00\dots 0, \quad \alpha_i \in \mathbb{F}_p,$$

teisinga tik tuomet, kai $\alpha_1 = \alpha_2 = \dots = \alpha_m = 0$. Priešingu atveju sakysime, kad žodžiai yra tiesiškai priklausomi.

Apibrėžimas. Tiesiškai nepriklausomų žodžių sistemą $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m$ vadinsime tiesinio poerdvio $\mathbf{L} \subset \mathbb{F}_p^n$ baze, jei $\mathbf{L} = \mathcal{L}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m)$.

Teorema. Bet kuris poerdvis $\mathbf{L} \subset \mathbb{F}_p^n$ turi bazę. Visos poerdvio bazės turi tą patį žodžių skaičių.

Tiesinio poerdvio \mathbf{L} bazės žodžių skaičius $\dim(\mathbf{L})$ vadinamas jo dimensija.

Tiesiniai kodai

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Abėcėlė - baigtinis kūnas \mathbb{F}_q , čia $q = p^m$ – pirminio skaičiaus laipsnis. Tada žodžių aibė \mathbb{F}_q^n yra tiesinė erdvė.

Apibrėžimas. Tiesinį erdvės \mathbb{F}_q^n poerdvį $\mathbf{L} \subset \mathbb{F}_q^n$ vadinsime tiesiniu kodu. Jeigu šio poerdvio dimensija yra k , o minimalus atstumas – d , sakysime, kad tai $[n, k, d]$ kodas.

Tiesinio $[n, k]$ arba $[n, k, d]$ kodo \mathbf{L} dydis $|\mathbf{L}| = q^k$, o jo koeficientas

$$R(\mathbf{L}) = \frac{\log_q |\mathbf{L}|}{n} = \frac{k}{n}.$$

Tiesinio kodo generuojanti matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Tegu $\mathbf{L} \subset \mathbb{F}_q^n$ yra tiesinis $[n, k]$ kodas. Kūno \mathbb{F}_q elementų matricą $G = (g_{ij})_{k \times n}$ vadinsime generuojančia kodo \mathbf{L} matrica, jei n ilgio žodžiai

$$\mathbf{g}_i = g_{i1}g_{i2}\dots g_{in}, \quad i = 1, 2, \dots, k,$$

sudaro kodo \mathbf{L} bazę.

Kadangi

$$\{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\} = \mathcal{L}(\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k) = \mathbf{L},$$

tai abipus vienareikšmis atvaizdis

$$\mathbf{x} \leftrightarrow \mathbf{x}G$$

nusako erdvės \mathbb{F}_q^k žodžiais pateikiamos informacijos kodavimą kodo \mathbf{L} žodžiais.

Ekvivalentaus kodo generuojanti matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Elementarieji matricos G pertvarkiai:

dviejų eilučių (arba stulpelių) keitimas vietomis;

eilutės daugyba iš $\alpha \in \mathbf{F}_q$, $\alpha \neq 0$;

eilutės keitimas jos bei kitos eilutės suma;

stulpelio daugyba iš $\alpha \in \mathbf{F}_q$, $\alpha \neq 0$.

Teorema. Tegu G yra tiesinio kodo \mathbf{L} generuojanti matrica, o G' yra matrica, gauta iš G , atlikus elementariųjų jos pertvarkių seką. Tada G' yra kodo, ekvivalentaus \mathbf{L} , generuojanti matrica.

Galime nagrinėti tiesinius kodus, turinčius specialaus pavidalo ("patogias") generuojančias matricas.

Standartinio pavidalo generuojanti matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Jei G yra $[n, k]$ kodo generuojanti matrica, tai elementariaisiais pertvarkiais galima gauti

$$G' = \begin{pmatrix} 1 & 0 & \dots & 0 & a_{1,1} & \dots & a_{1,n-k} \\ 0 & 1 & \dots & 0 & a_{2,1} & \dots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & a_{k,1} & \dots & a_{k,n-k} \end{pmatrix} = (I_k, A);$$

čia: I_k yra vienetinė $k \times k$ matrica, A – kūno \mathbf{F}_q elementų $k \times (n - k)$ matrica. Gautoji matrica vadinama *standartinio pavidalo* generuojančia matrica.

Kai $G = (I_k, A)$, kodavimo procedūra atrodo šitaip:

$$\mathbf{x} \rightarrow \mathbf{xy}, \quad \mathbf{y} = \mathbf{x}A.$$

Koduojami žodžiai tiesiog pailginami, pridedant $n - k$ kontrolinių simbolių.

Kodo žodžio svoris

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Žodžio $\mathbf{x} \in \mathbf{F}_q^n$, $\mathbf{x} = x_1 \dots x_n$, svoriu vadinsime skaičių

$$w(\mathbf{x}) = \sum_{x_i \neq 0} 1.$$

Teorema. Tegu d yra tiesinio kodo \mathbf{L} minimalus atstumas. Tada

$$d = \min\{w(\mathbf{x}) : \mathbf{x} \in \mathbf{L}, \mathbf{x} \neq 00 \dots 0\}.$$

Irodymas. Pažymėkime $d' = \min\{w(\mathbf{z}) : \mathbf{z} \in \mathbf{L}, \mathbf{z} \neq 00 \dots 0\}.$

Kodo žodžio svoris

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Žodžio $\mathbf{x} \in \mathbf{F}_q^n$, $\mathbf{x} = x_1 \dots x_n$, svoriu vadinsime skaičių

$$w(\mathbf{x}) = \sum_{x_i \neq 0} 1.$$

Teorema. Tegu d yra tiesinio kodo \mathbf{L} minimalus atstumas. Tada

$$d = \min\{w(\mathbf{x}) : \mathbf{x} \in \mathbf{L}, \mathbf{x} \neq 00 \dots 0\}.$$

Irodymas. Pažymėkime $d' = \min\{w(\mathbf{z}) : \mathbf{z} \in \mathbf{L}, \mathbf{z} \neq 00 \dots 0\}.$

- $\mathbf{0} \neq \mathbf{x} \in \mathbf{L} \Rightarrow d \leq h(\mathbf{x}, \mathbf{0}) = w(\mathbf{x}) \Rightarrow d \leq d'.$

Kodo žodžio svoris

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Žodžio $\mathbf{x} \in \mathbf{F}_q^n$, $\mathbf{x} = x_1 \dots x_n$, svoriu vadinsime skaičių

$$w(\mathbf{x}) = \sum_{x_i \neq 0} 1.$$

Teorema. Tegu d yra tiesinio kodo \mathbf{L} minimalus atstumas. Tada

$$d = \min\{w(\mathbf{x}) : \mathbf{x} \in \mathbf{L}, \mathbf{x} \neq 00 \dots 0\}.$$

Irodymas. Pažymėkime $d' = \min\{w(\mathbf{z}) : \mathbf{z} \in \mathbf{L}, \mathbf{z} \neq 00 \dots 0\}$.

- $0 \neq \mathbf{x} \in \mathbf{L} \Rightarrow d \leq h(\mathbf{x}, 0) = w(\mathbf{x}) \Rightarrow d \leq d'$.
- Tegu $\mathbf{x}, \mathbf{y} \in \mathbf{L}$ yra artimiausi kodo žodžiai. Tada $d = h(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y}) \Rightarrow d \geq d'$.

□

Kodo kontrolinė matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Tegu \mathbf{L} yra tiesinis $[n, k]$ kodas. $(n - k) \times n$ matricą H , kuri tenkina sąlygą

$$\mathbf{L} = \{\mathbf{x} : \mathbf{x}H^T = \mathbf{0}_{1,n-k}\},$$

vadinsime kodo \mathbf{L} kontroline matrica.

Tarkime, kad G yra $[n, k]$ kodo \mathbf{L} generuojanti matrica.

- I. Bet kuri $(n - k) \times n$ matrica H , sudaryta iš tiesiškai nepriklausomų eilučių ir tenkinanti sąlygą

$$GH^T = \mathbf{0}_{k,n-k},$$

bus \mathbf{L} kontrolinė matrica.

- II. Jei $G = (I_k, A)$, tai matrica

$$H = (-A^T, I_{n-k})$$

yra \mathbf{L} kontrolinė matrica.

Kodo kontrolinė matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Teorema. Tegu H yra tiesinio kodo \mathbf{L} kontrolinė matrica. Jeigu egzistuoja d tiesiškai priklausomų H stulpelių, o bet kuri $d - 1$ šios matricos stulpelių sistema yra tiesiškai nepriklausoma, tai kodo \mathbf{L} minimalus atstumas lygus d .

Pavyzdys. (Kodas su kontroliniu simboliu) Matrica iš vienos eilutės

$$H = (h_1 h_2 \dots h_n), \quad h_j \in \mathbb{F}_q, \quad h_j \neq 0,$$

yra kontrolinė $[n, n - 1, 2]$ kodo \mathbf{K} matrica.

$\mathbf{x} \in \mathbf{K}$, $\mathbf{x} = x_1 x_2 \dots x_n$, tada ir tik tada, kai

$$\mathbf{x}H^T = h_1 x_1 + h_2 x_2 + \dots + h_n x_n = 0.$$

Kontrolinis simbolis

$$x_n = -(h_1 x_1 + h_2 x_2 + \dots + h_{n-1} x_{n-1}) h_n^{-1}.$$

Dekodavimas

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

$\mathbf{L} \subset \mathbb{F}_q^n$ yra tiesinis $[n, k]$ kodas. Suskaidysime erdvę \mathbb{F}_q^n sluoksniais

$$\mathbf{L}_{\mathbf{x}} = \mathbf{x} + \mathbf{L} = \{\mathbf{x} + \mathbf{c} : \mathbf{c} \in \mathbf{L}\}, \quad \mathbf{x} \in \mathbb{F}_q^n.$$

Aibės $\mathbf{L}_{\mathbf{x}}, \mathbf{L}_{\mathbf{y}}$ arba nesikerta, arba sutampa; čia $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. Todėl sluoksnių aibės dydis yra $|\mathbb{F}_q^n / \mathbf{L}| = q^{n-k}$.

Gautas žodis \mathbf{x} . Taikydami minimalaus atstumo taisyklę, šį žodį dekoduosime kodo žodžiu \mathbf{c} , kuris tenkina sąlygą

$$h(\mathbf{c}, \mathbf{x}) = w(\mathbf{x} - \mathbf{c}) = \min_{\mathbf{c}' \in \mathbf{L}} w(\mathbf{x} - \mathbf{c}').$$

Tačiau žodis $\mathbf{a} = \mathbf{x} - \mathbf{c}$ yra tame pat sluoksnyje kaip \mathbf{x} . Vadinasi, dekoduojant reikia peržiūrėti sluoksnį kuriame atsidūrė \mathbf{x} , rasti jame mažiausią svorį turintį elementą \mathbf{a} ir dekoduoti taip:

$$\mathbf{x} \rightarrow f(\mathbf{x}) = \mathbf{x} - \mathbf{a}.$$

Standartinė kodo lentelė

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

[Kodo lentelė](#)

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

$$\mathbf{L} = \{\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_N\}, \mathbf{c}_0 = \mathbf{0}, N = q^k - 1.$$

Standartinė kodo \mathbf{L} lentelė

$$\begin{pmatrix} \mathbf{a}_0 & \mathbf{c}_1 & \mathbf{c}_2 & \dots & \mathbf{c}_N \\ \mathbf{a}_1 & \mathbf{a}_1 + \mathbf{c}_1 & \mathbf{a}_1 + \mathbf{c}_2 & \dots & \mathbf{a}_1 + \mathbf{c}_N \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_m & \mathbf{a}_m + \mathbf{c}_1 & \mathbf{a}_m + \mathbf{c}_2 & \dots & \mathbf{a}_m + \mathbf{c}_N \end{pmatrix}$$

Pirmo stulpelio žodžius \mathbf{a}_i parenkame taip, kad būtų patenkinamos sąlygos:

$$\mathbf{a}_0 = \mathbf{0}, w(\mathbf{a}_i) = \min\{w(\mathbf{a}) : \mathbf{a} \in \mathbb{F}_q^n, \mathbf{a} \notin \bigcup_{j < i} \mathbf{L}_{\mathbf{a}_j}\}, i \geq 1.$$

Kiekvienoje eilutėje išrašyti atitinkamo sluoksnio $\mathbf{L}_{\mathbf{a}}$ elementai, o pirmasis iš jų (lyderis) turi mažiausią svorį.

Sindromai

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

[Sindromai](#)

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Tegu H yra kodo \mathbf{L} kontrolinė matrica, $\mathbf{x} \in \mathbb{F}_q^n$.
Žodžio \mathbf{x} sindromu vadinsime \mathbb{F}_q^{n-k} elementą $s(\mathbf{x}) = \mathbf{x}H^T$.

Jei $\mathbf{c} \in \mathbf{L}$ ir $\mathbf{x} = \mathbf{a}_i + \mathbf{c}$, tai $s(\mathbf{x}) = s(\mathbf{a}_i)$.

Skirtingoms klasėms priklausančius žodžius atitinka skirtingi sindromai:

Sindromai	\mathbf{s}_1	\mathbf{s}_2	\dots	\mathbf{s}_m
Lyderiai	\mathbf{a}_1	\mathbf{a}_2	\dots	\mathbf{a}_m .

Dekodavimo algoritmas:

- randame gautojo žodžio \mathbf{x} sindromą $s(\mathbf{x})$;
- randame $s(\mathbf{x})$ atitinkantį lyderį \mathbf{a} ir dekoduojuame \mathbf{x} žodžiu $\mathbf{f}(\mathbf{x}) = \mathbf{x} - \mathbf{a}$.

Kontrolinė $r \times n$ matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Ieškosime kuo didesnių tiesinių kodų, kurių minimalus atstumas $d = 3$, o kontrolinės matricos H eilučių skaičių r . Bet kurie du H stulpeliai turi būti tiesiškai nepriklausomi.

Kontrolinė $r \times n$ matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Ieškosime kuo didesnių tiesinių kodų, kurių minimalus atstumas $d = 3$, o kontrolinės matricos H eilučių skaičių r . Bet kurie du H stulpeliai turi būti tiesiškai nepriklausomi.

- Pasirinkime iš aibės $V_1 = \mathbb{F}_q^r$ nenulinį žodį s_1 ir sudarykime iš jo elementų pirmąjį H stulpelį.

Kontrolinė $r \times n$ matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Ieškosime kuo didesnių tiesinių kodų, kurių minimalus atstumas $d = 3$, o kontrolinės matricos H eilučių skaičių r . Bet kurie du H stulpeliai turi būti tiesiškai nepriklausomi.

- Pasirinkime iš aibės $V_1 = \mathbb{F}_q^r$ nenulinį žodį s_1 ir sudarykime iš jo elementų pirmąjį H stulpelį.
- Jeigu m -asis matricos H stulpelis sudarytas iš žodžio $s_m \in V_m$ komponentų, tai $m + 1$ -asis stulpelis bus $s_{m+1} \in V_{m+1} = V_m \setminus \{\alpha s_m : \alpha \in \mathbb{F}_q\}$. Jeigu $V_{m+1} = \emptyset$, matricos H sudarymą užbaikime.

Kontrolinė $r \times n$ matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Ieškosime kuo didesnių tiesinių kodų, kurių minimalus atstumas $d = 3$, o kontrolinės matricos H eilučių skaičių r . Bet kurie du H stulpeliai turi būti tiesiškai nepriklausomi.

- Pasirinkime iš aibės $V_1 = \mathbb{F}_q^r$ nenulinį žodį \mathbf{s}_1 ir sudarykime iš jo elementų pirmąjį H stulpelį.
- Jeigu m -asis matricos H stulpelis sudarytas iš žodžio $\mathbf{s}_m \in V_m$ komponentų, tai $m + 1$ -asis stulpelis bus $\mathbf{s}_{m+1} \in V_{m+1} = V_m \setminus \{\alpha \mathbf{s}_m : \alpha \in \mathbb{F}_q\}$. Jeigu $V_{m+1} = \emptyset$, matricos H sudarymą užbaikime.
- Kadangi $\text{rang}(H) = r$ ir $|V_m| = q^r - 1 - (m - 1)(q - 1)$, $m \geq 2$, tai H turės $n = (q^r - 1)/(q - 1)$ stulpelių.

Kontrolinė $r \times n$ matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Ieškosime kuo didesnių tiesinių kodų, kurių minimalus atstumas $d = 3$, o kontrolinės matricos H eilučių skaičių r . Bet kurie du H stulpeliai turi būti tiesiškai nepriklausomi.

- Pasirinkime iš aibės $V_1 = \mathbb{F}_q^r$ nenulinį žodį s_1 ir sudarykime iš jo elementų pirmąjį H stulpelį.
- Jeigu m -asis matricos H stulpelis sudarytas iš žodžio $s_m \in V_m$ komponentų, tai $m + 1$ -asis stulpelis bus $s_{m+1} \in V_{m+1} = V_m \setminus \{\alpha s_m : \alpha \in \mathbb{F}_q\}$. Jeigu $V_{m+1} = \emptyset$, matricos H sudarymą užbaikime.
- Kadangi $\text{rang}(H) = r$ ir $|V_m| = q^r - 1 - (m - 1)(q - 1)$, $m \geq 2$, tai H turės $n = (q^r - 1)/(q - 1)$ stulpelių.
- Matrica H yra kontrolinė tiesinio $[n, n - r, 3]$ kodo matrica.

Hamingo kodai $\mathbf{H}_q(r)$

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Apibrėžimas. Tegu $r \geq 1$, $n = (q^r - 1)/(q - 1)$. Tiesinius $[n, n - r, 3]$ kodus iš \mathbb{F}_q abėcėlės žodžių vadinsime Hamingo kodais ir žymėsime $\mathbf{H}_q(r)$.

Teorema. Hamingo kodai yra tobuli.

Irodymas. (n, N, d) kodas yra tobulas tada ir tik tada, kai

$$NV_q(n, t) = q^n, \quad t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Kodui $\mathbf{H}_q(r)$ gausime $NV_q(n, t) = q^{n-r}(1 + n(q-1)) = q^n$. \square

$[n, n - r, 3]$ kodo žodis sudarytas iš $n - r$ reikšminių ir r kontrolinių bitų. Tinkamai pasirinkus jo kontrolinę ir generuojančią matricas, kodavimas ir dekodavimas yra labai paprastas.

Hamingo kodai $\mathbf{H}_2(r)$

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Surašome pirmųjų $2^r - 1$ natūraliųjų skaičių skleidinių dvejetainėje sistemoje elementus į matricos stulpelius. Gautoji $r \times (2^r - 1)$ matrica yra kontrolinė kodo $\mathbf{H}_2(r)$ matrica.

- Jeigu kodo žodis $\mathbf{c} \in \mathbf{H}_2(r)$ siuntimo metu buvo i -oje pozicijoje iškraipytas, tai gautasis žodis yra

$$\mathbf{x} = \mathbf{c} + \varepsilon_i;$$

čia ε_i yra žodis, kurio visos komponentės, išskyrus i -ąją, lygios nuliui. Tada sindromas

$$\mathbf{x}H^T = \varepsilon_i H^T$$

sudarytas iš tų pačių simbolių kaip ir matricos H i -asis stulpelis, t.y. dvejetainis neteisingai perduotos žodžio komponentės numeris.

- Tokiu būdu gavėjas gali atstatyti tą kodo žodį, kuris buvo siųstas. Tačiau norėdamas atkurti pradinį šaltinio žodį, gavėjas turi žinoti kokią generuojančią matricą koduodamas naudojo siuntėjas.

Hamingo kodai $H_2(3)$

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $H_q(r)$

Hamingo kodai $H_2(r)$

Hamingo kodai $H_2(3)$

Golay kodai

G_{24} kontrolinė
matrica

G_{24} dekodavimas

$H_2(3)$ yra tiesinis $[7, 4, 3]$ kodas. Jo kontrolinė ir generuojanti matricos gali būti

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Kodavimo – dekodavimo procedūros pavyzdžiai:

- (be klaidų)

$$1011 \xrightarrow{G} 0110011 \xrightarrow{H^T} 000$$

- (viena klaida)

$$1011 \xrightarrow{G} 0110011 \xrightarrow{\text{klaida}} 01\textcolor{red}{0}0011 \xrightarrow{H^T} 011$$

Golay kodai (1949)

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

[Golay kodai](#)

\mathbf{G}_{24} kontrolinė
matrica

\mathbf{G}_{24} dekodavimas

Tegu $\mathbf{c}_1 = 110001110101000000000000 \in \mathbb{F}_2^{23}$.

Cikliškai perstūmę simbolius, sudarome dar 11 žodžių

$\mathbf{c}_2 = 011000111010100000000000$,

.....

$\mathbf{c}_{12} = 000000000000110001110101$.

Visi jie tiesiškai nepriklausomi. Tegu $\mathbf{c}_i^* = \mathbf{c}_i 1 \in \mathbb{F}_2^{24}$.

Apibrėžimas. *Tiesinius kodus*

$$\mathbf{G}_{23} = \mathcal{L}(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{12}), \quad \mathbf{G}_{24} = \mathcal{L}(\mathbf{c}_1^*, \mathbf{c}_2^*, \dots, \mathbf{c}_{12}^*)$$

vadinsime dvejetainiais Golay kodais.

Teorema. *Kodo \mathbf{G}_{23} parametrai yra $[23, 12, 7]$, o kodo \mathbf{G}_{24} – $[24, 12, 8]$. Be to, kodas \mathbf{G}_{23} yra tobulas.*

G_{24} kontrolinė matrica

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo
generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $H_q(r)$

Hamingo kodai $H_2(r)$

Hamingo kodai $H_2(3)$

Golay kodai

G_{24} kontrolinė
matrica

G_{24} dekodavimas

G_{24} turi standartinio pavidalo generuojančią matricą $G = (I_{12}, A)$,

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Tada kontrolinė matrica $H = (-A^T, I_{12}) = (A, I_{12})$.

Be to, G ir H abi yra ir generuojančios ir kontrolinės kodo G_{24} matricos.

G_{24} dekodavimas

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

G_{24} kontrolinė
matrica

G_{24} dekodavimas

Tegu $G = (I_{12}, A)$, $H = (A, I_{12})$. Gautas žodis

$$\mathbf{x} = \mathbf{x}_1 \mathbf{x}_2, \quad \mathbf{x}_i \in \mathbb{F}_2^{12},$$

kuriame padaryta ≤ 3 klaidų.

$\varepsilon_i \in \mathbb{F}_2^{12}$ žymime žodį, kuriame tik i -tasis simbolis yra 1, kiti - nuliai,

$$\varepsilon_0 = 000000000000.$$

Dekodavimo algoritmas

1. Randame sindromus

$$\mathbf{s}_1 = \mathbf{x}G^T = \mathbf{x}_1 + \mathbf{x}_2A, \quad \mathbf{s}_2 = \mathbf{x}H^T = \mathbf{x}_1A + \mathbf{x}_2$$

ir jų svorius $w(\mathbf{s}_1)$, $w(\mathbf{s}_2)$.

2. Jei $w(\mathbf{s}_1) \leq 3$, $w(\mathbf{s}_2) \geq 5$, tai $\mathbf{x} \mapsto \mathbf{x} - \mathbf{s}_1\varepsilon_0$.

3. Jei $w(\mathbf{s}_2) \leq 3$, $w(\mathbf{s}_1) \geq 5$, tai $\mathbf{x} \mapsto \mathbf{x} - \varepsilon_0\mathbf{s}_2$.

G_{24} dekodavimas

Baigtinio kūno sąvoka

Tiesinė erdvė

Tiesinis poerdvis

Poerdvio dimensija

Tiesiniai kodai

Generuojanti matrica

Ekvivalentaus kodo

generuojanti matrica

Standartinė matrica

Kodo žodžio svoris

Kontrolinė matrica

Dekodavimas

Kodo lentelė

Sindromai

Kontrolinė $r \times n$
matrica

Hamingo kodai $\mathbf{H}_q(r)$

Hamingo kodai $\mathbf{H}_2(r)$

Hamingo kodai $\mathbf{H}_2(3)$

Golay kodai

G_{24} kontrolinė
matrica

G_{24} dekodavimas

4. Jei $w(\mathbf{s}_2) \geq 5$, $w(\mathbf{s}_1) \geq 5$, tai sudarome naujus sindromus

$$\mathbf{s}_{1i} = \mathbf{s}_1 + \varepsilon_i A, \quad i = 1, 2, \dots, 12.$$

Jei kuriam nors j , $w(\mathbf{s}_{1j}) \leq 2$, o likusieji $w(\mathbf{s}_{1i}) \geq 4$, tai

$$\mathbf{x}' = \mathbf{x} - \varepsilon_0 \varepsilon_j$$

ir žodžiui \mathbf{x}' kartojame 1-3 žingsnius.

Esant kitokiai svorių $w(\mathbf{s}_{1i})$ sekai, analogiškai nagrinėjami sindromų

$$\mathbf{s}_{2i} = \mathbf{s}_2 + \varepsilon_i A, \quad i = 1, 2, \dots, 12.$$

svoriai. Sėkmės atveju

$$\mathbf{x}' = \mathbf{x} - \varepsilon_j \varepsilon_0.$$

Jei abi svorių sekos netenkina minėtų sąlygų, dekoduoti negalima dėl pernelyg didelių iškraipymų.