CV 3. Kódy z kombinatorických designů

- **Balanced block design** ~ Balancovaný (vyvážený) blokový design.

  (b, v, r, k, λ) - design

  v - body, prvky, variety
  b - počet bloků
  k - počet prvků v bloku
  r - počet výskytů prvku v blocích
  každý prvek je v r blocích (replication #)
  λ - počet výskytů dvojice prvků v blocích

  Příklad: Fanova rovina $(7, 7, 3, 3, 1)$ - design

  (Cyklický rozklad $\mathbb{Z}_7$ na Δ, $\{1, e, 4\}$)

- Incidenční matice designu

  $A = [a_{ij}]$ A je $v \times b$ matice $a_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j \end{cases}$, x_i pro $i = 1 \dots v$ jsou prvky.

  Příklad: $(7, 16, 3)$- kód z Fanovy roviny ← Je perfektní!

- Vlastnosti designů

  Lemma 3.1.
  (i) $b \cdot k = v \cdot r$ ← počet prvků v multimnožině
  (ii) $r(k-1) = \lambda(v-1)$ ← počet výskytů dvojice

  symetrický design $\Leftrightarrow$ $v = b$ $\Rightarrow$ $k = r$ a (v, k, λ) - design

  - projektivní rovina řádu n je $(n^2+n+1, n+1, 1)$ - design
  - Hadamard design je - $(4t-1, 2t-1, t-1)$ - design
  - Vždy $v \leq b$ (Fisherovo lemma)

3.1.1. Mějme přirozené číslo n. Sestavme systém všech k-prvkových podmnožin množiny V, kde $V = [1, n]$. Jedná se o kombinatorický design? Pokud ano, jaké jsou jeho parametry?

Jaké parametry by takový design měl?

Počet variet $r = n$

Počet bloků $b = \binom{n}{k} = \frac{n!}{(n-k)!\,k!}$

replication # $r = \binom{n-1}{k-1}$

velikost bloků $k = k$

počet výskytů páru $\lambda = \binom{n-2}{k-2}$

$\left(\binom{n}{k}, n, \binom{n-1}{k-1}, k, \binom{n-2}{k-2}\right)$ - design

Ověříme rovnosti: (i) $b \cdot k = r \cdot r$

$\binom{n}{k} \cdot k = n \cdot \binom{n-1}{k-1}$

$\frac{n! \cdot k}{(n-k)!\,k!} = \frac{n \cdot (n-1)!}{(n-1-(k-1))!\,(k-1)!}$

$\frac{n!}{(n-k)!\,(k-1)!} = \frac{n!}{(n-k)!\,(k-1)!}$

(ii) - podobně

Jaké rozměry má incidenční matice tohoto designu?

$A = r \times b \Rightarrow A = n \times \binom{n}{k}$

v řádku: $\lambda = \binom{n-1}{k-1}$ jedniček

ve sloupci: $k = k$ jedniček

Jaký kód bychom dostali z řádků matice A?

$\left(\binom{n}{k}, n, d\right)$ - kód (binární), $dist(C) = ?$

$dist(a_i, a_j) = w(\bar{a}_i) + w(\bar{a}_j) - 2(\bar{a}_i \wedge \bar{a}_j) = 2 \cdot \binom{n-1}{k-1} - 2\binom{n-2}{k-2} =$

$= 2\left[\binom{n-1}{k-1} - \binom{n-2}{k-2}\right] = 2 \cdot \binom{n-2}{k-1}$

proto

Platí kombinator. identita

$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ odtud $\binom{n}{k} - \binom{n-1}{k-1} = \binom{n-1}{k}$

Příklad designu $\binom{n}{k}$ pro

$n = 5, \quad k = 3$ $\qquad \left(\binom{5}{3}, 5, \binom{4}{2}, 3, \binom{3}{1}\right)$ - design

$b = \binom{5}{3} = 10$

1. {1 2 3}
2. {1 2 4}
3. {1 2 5}
4. {1 3 4}
5. {1 3 5}
6. {1 4 5}
7. {2 3 4}
8. {2 3 5}
9. {2 4 5}
10. {3 4 5}

← bloky designu

Incidenční matice

$M =$

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
1	1	1	1	1	1	1	0	0	0	0
2	1	1	1	0	0	0	1	1	1	0
3	1	0	0	1	1	0	1	1	0	1
4	0	1	0	1	0	1	1	0	1	1
5	0	0	1	0	1	1	0	1	1	1

$dist = 2\binom{4}{2} - 2\binom{3}{1} =$

$= 2 \cdot 6 - 2 \cdot 3 = 12 - 6 = \underline{\underline{6}}$

každé dva řádky se shodují ve 3 jedničkách. Tj každá dvojice prvků je ve 3 blocích.

dostaneme $\left(\binom{n}{k}, n, d\right) = (10, 5, 6)$

můžeme přidat $\bar{0} = 00\ldots0 = (10, 6, 6)$ - kód

Př ① Použijte bloky $(11, 5, 2)$ - designu k sestavení $(11, 24, 5)$ - kódu.

1. {1, 3, 4, 5, 9}
2. {2, 4, 5, 6, 10}
3. {3, 5, 6, 7, 11}
4. {1, 4, 6, 7, 8}
5. {2, 5, 7, 8, 9}
6. {3, 6, 8, 9, 10}
7. {4, 7, 9, 10, 11}
8. {1, 5, 8, 10, 11}
9. {1, 2, 6, 9, 11}
10. {1, 2, 3, 7, 10}
11. {2, 3, 4, 8, 11}

$M =$

	1	2	3	4	5	6	7	8	9	10	11
1	1	0	0	1	0	0	0	1	1	1	0
2	0	1	0	0	1	0	0	0	1	1	1
3	1	0	1	0	0	1	0	0	0	1	1
4	1	1	0	1	0	0	1	0	0	0	1
5	1	1	1	0	1	0	0	1	0	0	0
6	0	1	1	1	0	1	0	0	1	0	0
7	0	0	1	1	1	0	1	0	0	1	0
8	0	0	0	1	1	1	0	1	0	0	1
9	1	0	0	0	1	1	1	0	1	0	0
10	0	1	0	0	0	1	1	1	0	1	0
11	0	0	1	0	0	0	1	1	1	0	1

Incidenční matice z Hadamardova $(11, 5, 2)$ - designu

$(4t-1, 2t-1, t-1)$ - design

kód, který sestavíme nebude perfektní.
Hammingova hranice pro $(11, M, 5)$-kód dává $M \leq 30$ Ověřte sami.
Je ale známo $A_2(11,5) = 24$ a kód sestavený z tohoto designu bude mít $M = 24$. Je tedy nejlepší možný vzhledem k velikosti.

Sestavíme C - $(11, 24, 5)$-kód

Incidenční matice designu A - 11×11
prohodíme $0 \leftrightarrow 1$ a dostaneme B - 11×11

kód C bude tvořen řádky A a řádky B

tj. pro $i = 1, 2 \dots 11$ $\bar{a}_i \in C$ a $\bar{b}_i \in C$

a také nulovým slovem $\bar{0} = 0,0 \dots 0$ a jedničkovým $\bar{1} = 1,1, \dots, 1$

Tj. celkem 24 slov délky 11.

- Ukážeme, že $dist(C) = 5$
  - V každém řádku A je pět 1 a každé dva řádky se shodují ve dvou 1 (protože $\lambda = 2$)
    $d(\bar{a}_i, \bar{a}_j) = w(\bar{a}_i) + w(\bar{a}_j) - 2w(\bar{a}_i \wedge \bar{a}_j) = 5 + 5 - 4 = \underline{6}$
  - Pro řádky B to dopadne stejně $d(\bar{b}_i, \bar{b}_j) = 6$
    $d(\bar{b}_i, \bar{b}_j) = w(b_i) + w(b_j) - 2w(b_i b_j) = 6 + 6 - 2 \cdot 3 = 12 - 6 = \underline{6}$
  - Od $\bar{0}, \bar{1}$ slova se všechna $\bar{a}_i$ a $\bar{b}_i$ liší alespoň na 5-ti pozicích.
  - Zbývá $d(a_i, b_j)$ pro $i \neq j$ (pro $i = j$ je $d(\bar{a}_i, \bar{b}_j) = 11$)
    $\bar{a}_i$ a $\bar{b}_j$ se liší na pozicích, kde se $\bar{a}_i$ a $\bar{a}_j$ shodují.
    počet pozic, kde se $\bar{a}_i$ a $\bar{a}_j$ shodují $= 2\lambda + 1$
    tj. $d(a_i, b_j) = \overbrace{11 - d(a_i, a_j)} = 11 - 6 = \underline{5}$ ■

Pozn. Jedná se o Hadamardův $(4t-1, 2t-1, t-1)$-design pro $t = 3$
tj: $(11, 5, 2)$-design

Př. (2.) Ukažte, že pro parametry (b, v, k, r, λ)-dicesjna platí (i) $b \cdot k = v \cdot r$ Bylo na přednášce

(ii) $r(k-1) = \lambda(v-1)$

(prvků)

od (i) - Počet výskytů všech symbolů v designu můžeme spočítat dvěma způsoby $x = ?$

- pro symbol máme v-možností (variant) a v blocích se opakuje r krát, tedy $x = r \cdot v$
- symboly se vyskytují v b blocích a každý blok jich obsahuje k, tedy $x = b \cdot k$

Celkem $r \cdot v = b \cdot k$

od (ii) Počet výskytů párů v designu spočítáme dvěma způsoby (vzhledem k jednomu lib. pevnému prvku)

- pro pevný prvek y vytvoříme $v-1$ párů a každý z nich je v λ blocích

počet párů s y $= (v-1) \cdot \lambda$

- pevný prvek y se v blocích nachází r krát a v každém z r bloků tvoří $k-1$ párů.

počet párů s y $= r \cdot (k-1)$

Celkem $r \cdot (k-1) = (v-1) \cdot \lambda$

Př. (3) Ukažte, že neexistují (b, v, r, k, λ)-designy s parametry

(i) $(12, 8, 6, 4, 3)$ a (ii) $(22, 22, 7, 7, 2)$

od (i) musí být $r \cdot v = k \cdot b$ a taky $r(k-1) = (v-1)\cdot\lambda$

$6 \cdot 8 \overset{?}{=} 12 \cdot 4$ $\quad$ $6(4-1) \overset{?}{=} (8-1)\cdot 3$

$48 = 48$ ✓ $\quad$ $18 \neq 21$

nelze sestrojit

od (ii) musí být $r \cdot v = k \cdot b$ a taky $r(k-1) = (v-1)\cdot\lambda$

$7 \cdot 22 = 7 \cdot 22$ ✓ $\quad$ $7(7-1) = (22-1)\cdot 2$

Pro symetrický design vždy $\quad$ $7 \cdot 6 = 21 \cdot 2$

$42 = 42$ ✓

a také pro (v, k, λ)-design, kde v je sudé

musí být $k - \lambda$ rovno druhé mocnině Důkaz ?

$(22, 22, 7, 7, 2) \sim (22, 7, 2)$-dizajn

protože $k - \lambda = 7 - 2 = 5 \neq n^2$ pro jakékoli n sudé, tak design pokud ~~✓~~ ✗

Př. (4) Ukažte, že existuje-li Hadamard $(4t-1, 2t-1, t-1)$-dizajn pak $A_2(4t-1, 2t-1) \geq 8t$

Zobecněním argumentů pro kód z FANO PLANE a příkladu 2.12.

Konstruovaný kód by měl slova délky $n = 4t-1$

Počet slov by byl $2 \cdot n + 2 = 8t$

Pro min vzdálenost $dist(C) = 2\lambda + 1 = 2(t-1) + 1 = 2t-1$

Odtud $A_2(4t-1, 2t-1) \geq 8t$

3.1.3.♡ Vezměte incidenční matici A designu Fanovy roviny a vypočítejte AA^T.

konečná projektivní rovina n-tého řádu je

$(n^2+n+1, n+1, 1)$-design pro $n=2$ $(7,3,1)$-design

$$M = \begin{bmatrix} 1&0&0&0&1&0&1\\ 1&1&0&0&0&1&0\\ 0&1&1&0&0&0&1\\ 1&0&1&1&0&0&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1&1&0&1&0&0&0\\ 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1\\ 1&0&1&0&0&0&1 \end{bmatrix} = \begin{bmatrix} 3&1&1&1&1&1&1\\ 1&3&1&1&1&1&1\\ 1&1&3&1&1&1&1\\ 1&1&1&3&1&1&1\\ 1&1&1&1&3&1&1\\ 1&1&1&1&1&3&1\\ 1&1&1&1&1&1&3 \end{bmatrix}$$

Fanova rovina

Další vztahy mezi parametry designu

Fischerovo lemma (Důkaz)

V každém (b, v, r, k, λ)-designu, kde $k < v$ platí, že $b \geq v$

Důkaz: Označím A incidenční matici designu. Ta je řádu $v \times b$.

Dále označíme M matici $A \cdot A^T$. $(M = A \cdot A^T)$

Pak $M = [m_{ij}]$ je čtvercová matice řádu v, pro kterou platí

$$m_{ij} = \begin{cases} r & \text{pro } i = j \\ \lambda & \text{pro } i \neq j \end{cases}$$

Pro $i=j$ je $m_{ii} = r$, protože m_{ii} je vlastně skalární součin řádku i matice A samotného se sebou. Každý řádek matice A obsahuje r-jedniček a zbytek jsou 0. Tedy $m_{ii} = \vec{r}_i^{\,A} \cdot \vec{r}_i^{\,A} = r$

Pro $i \neq j$ je $m_{ij} = \lambda$, protože m_{ij} je skal. součin dvou různých řádků matice A. Ty se shodují v 1-ičkách na λ pozicích. Tedy $m_{ij} = \lambda$.

Pro $r \neq \lambda$ jsou všechny řádky matice M lin. nezávislé a tedy hodnost matice M je v. $(h(M) = v)$. Z vlastností maticového součinu plyne také násl. rovnost (nerovnost)

$$v = h(M) = h(A \cdot A^T) \leq \min\{h(A), h(A^T)\} = h(A) \leq b$$

$v \times v$ $\qquad$ $v \times b$

odtud $v \leq b$. ∎