7 Hadamardovy matice a kódy, a něco odhadů.

V kapitole 3 jsme konstruovali $2{-}(11,5,2)$ design. Pro $2=\lambda-1$ bude $3=\lambda$, $5=2\lambda-1$ a $11=4\lambda-1$, takže $2{-}(11,5,2)$ design je příkladem $2{-}(4\lambda-1,2\lambda-1,\lambda-1)$ designu. Takovým designům se říká *Hadamardovy*. Otázka je, zda existují i pro jiné hodnoty λ. Pro $\lambda=2$ dostáváme parametry $(7,3,1)$, čemuž vyhovuje Fanova rovina. Další příklady uvedeme později. Nejprve se budeme zabývat obecnými vlastnostmi takových designů.

Standardní rovnost $r(k-1)=(v-1)\lambda$ má v našem případě tvar $r(2\lambda-2)=(4\lambda-2)(\lambda-1)$, odkud $r=2\lambda-1$, takže rovnost $kb=vr$ implikuje $v=b=4\lambda-1$. Vidíme, že Hadamardovy designy jsou čtvercové. Každé dva různé bloky se protínají právě v $\lambda-1$ bodech.

Uvažme incidenční matici M nějakého $2{-}(4\lambda{-}1,2\lambda{-}1,\lambda{-}1)$ designu. Dva její různé řádky mají společných $\lambda-1$ jedniček a $(4\lambda-1)-2(2\lambda-1)+(\lambda-1)=\lambda$ nul. Vytvořme novou matici H tak, že k M přidáme řádek a sloupec složený ze samých jedniček a současně všechny nuly změníme na minus jedničky. Ve vzniklé matici se dva různé řádky u a v shodují právě na 2λ místech. Uvážíme-li jejich bodový součin $u\cdot v$, vidíme, že shody dávají v jednotlivých pozicích $+1$ a neshody -1, takže $u\cdot v=0$. Jinými slovy, $HH^{\mathsf{T}}=nI$, kde $n=4\lambda$.

Každá matice H řádu n, která splňuje $HH^{\mathsf{T}}=nI$ a obsahuje pouze hodnoty $+1$ a -1, se nazývá *Hadamardova*. Jsou-li její prvý řádek a prvý sloupec složeny toliko z hodnot $+1$, hovoříme o Hadamardově matici v *normalizovaném* tvaru. Hadamardovy designy indukují, jak jsme nahlédli, právě takové Hadamardovy matice.

Rovnost $HH^{\mathsf{T}}=nI$ implikuje, že každé dva různé řádky mají stejný počet shod a neshod. Číslo n tedy musí být sudé, pokud $n>1$. Vynásobíme-li libovolný sloupec hodnotou -1, počet neshod se nemění. Rovnost $HH^{\mathsf{T}}=nI$ rovněž zjevně zůstává v platnosti, pokud vynásobíme řádek hodnotou -1. Každou Hadamardovu matici proto lze převést do normalizovaného tvaru.

Ať H je taková matice řádu $2h\geq 4$. Ať u a v jsou dva její různé řádky, přičemž žádný z nich ať není prvý řádek matice. Každý z nich v bodovém součinu s prvým řádkem dává nulu. Protože prvý řádek je složen ze samých jedniček, tak u i v musí obsahovat h hodnot $+1$ a h hodnot -1. Ať se shodují v λ společných hodnotách $+1$. Potom je přesně $h-\lambda$ sloupců, ve kterých je v u hodnota $+1$ a ve v hodnota -1. Stejně je i sloupců, kde v má $+1$ a u má -1. Proto se u a v neshodují právě v $2(h-\lambda)$ pozicích. Počet těchto pozic musí být ale také roven h, neboť $u\cdot v=0$. Vidíme, že $h=2\lambda$ je číslo sudé, a že počet společných $+1$ (a podobně i -1) je přesně λ.

Pro Hadamardovu matici H (ne nutně normalizovanou) položme $H_1=\frac{1}{\sqrt{n}}H$. Pak $H_1H_1^{\mathsf{T}}=I$, takže $H_1^{\mathsf{T}}=H_1^{-1}$, odkud $H_1^{\mathsf{T}}H_1=I$ a $H^{\mathsf{T}}H=nI$. Vidíme, že transpozicí vznikne z Hadamardovy matice opět matice Hadamardova. V každém sloupci (kromě prvního) normalizované Hadamardovy matice řádu $2h>4$ je tedy právě h hodnot $+1$.

Matice (1) a $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ jsou Hadamardovy. Hadamardovy matice vyšších řádů lze odvodit, jak dokazuje následující tvrzení, z Hadamardových designů. Odvozením přitom rozumíme výše popsaný postup, kdy se z incidenční matice M vytváří matice H, kterou lze dále upravovat násobením řádků a sloupců hodnotou -1.

Tvrzení 7.1. *Každou Hadamardovu matici řádu $n \geq 3$ lze odvodit z nějakého $2{-}(4\lambda-1, 2\lambda-1, \lambda-1)$ designu, kde $4\lambda = n$.*

Důkaz. Ať H je normalizovaná Hadamardova matice řádu $n \geq 3$. Výše jsme již ukázali, že $n = 4\lambda$, přičemž každý řádek kromě prvého obsahuje 2λ hodnot $+1$ a 2λ hodnot -1. Dva takové různé řádky mají hodnotu $+1$ právě na λ společných pozicích.

Odstraňme nyní prvý řádek a prvý sloupec a nahraďme všechny výskyty hodnoty -1 hodnotou 0. Získanou matici označme M. Je to incidenční matice designu s bloky délky $2\lambda - 1$. Dva různé bloky mají společných $\lambda - 1$ bodů, protože odpovídající řádky mají společných λ jedniček, a každý bod leží v $2\lambda - 1$ blocích, protože odpovídající sloupec obsahuje právě 2λ jedniček. Podle Věty 3.5 proto jde o $2{-}(4\lambda-1, 2\lambda-1, \lambda-1)$ design. □

Je-li H Hadamardova matice, tak lze snadno nahlédnout, že $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ je rovněž Hadamardova matice. Maticím takto postupně odvozovaným z matice $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ se říká *Sylvestrovy H-matice*. Mají řád 2^m, $m \geq 1$. Lze je snadno vyjádřit i přímo. Pokud řádky i sloupce číslujeme od 0 do $2^k - 1$, tak pro $j = \sum \varepsilon_i 2^i$ a $j' = \sum \varepsilon'_i 2^i$ v buňce (j, j') leží hodnota $(-1)^{\sum \varepsilon_i \varepsilon_{i'}}$. Sylvestrova H-matice řádu 2^k se tak vlastně dá chápat jako multiplikační tabulka operace bodového součinu vektorů délky k, kde se místo 0 píše $+1$ a místo 1 se píše -1.

Konstrukcí Hadamardových matic existuje celá řada. Přesto není dosud známo, zda takovou matici lze sestrojit pro každý řád dělitelný čtyřmi.

Z každé Hadamardovy matice H řádu $n \geq 2$ se odvozuje binární kód $C(H)$ délky n tak, že každému řádku H se přiřadí dvě kódová slova: v jednom se hodnoty $+1, -1$ nahradí po řadě hodnotami $1, 0$, a v druhém se $+1, -1$ nahradí hodnotami $0, 1$. Protože počet shod i neshod dvou různých řádků je přesně $n/2$, je i Hammingova vzdálenost dvou kódových slov odvozených z dvou různých řádků přesně $n/2$ (kódová slova odvozená z téhož řádku mají Hammingovu vzdálenost maximální možnou, tj. n.) Kódům $C(H)$ se říká *Hadamardovy*. Mají parametry $(n, 2n, n/2)$.

Tvrzení 7.2. *Ať H je Sylvestrova H-matice řádu 2^m. Pak se $C(H)$ shoduje s Reed-Mullerovým kódem $\mathcal{R}(m, 1)$.*

Důkaz. Připomeňme, že pro booleovský polynom $a \in \mathbb{F}_2[x_1, \ldots, x_m]$ značí v_a binární vektor délky 2^m, který má v pozici $\sum \varepsilon_i 2^{m-i}$ hodnotu $a(\varepsilon_1, \ldots, \varepsilon_m)$.

Označme $s : \mathbb{F}_2[x_1, \ldots, x_m] \to \mathbb{F}_2[x_1, \ldots, x_{m+1}]$ zobrazení, které v každém polynomu nahradí proměnnou x_i proměnnou x_{i+1}. Vyjádřit polynom $b \in \mathbb{F}_2[x_1, \ldots, x_{m+1}]$ ve tvaru $s(a)$ tudíž lze právě když x_1 nefiguruje v žádném monomu polynomu b. Pro dosazování platí vztah $s(a)(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m+1}) = a(\varepsilon_2, \ldots, \varepsilon_{m+1})$. Hodnota $v_{s(a)}$ v pozici $j = \sum_{i=1}^{m+1} \varepsilon_i 2^{m+1-i}$ je proto rovna hodnotě v_a v pozici $j' = \sum_{i=1}^{m} \varepsilon_{i+1} 2^{m-i} = \sum_{i=2}^{m+1} \varepsilon_i 2^{m+1-i}$. Je-li $\varepsilon_1 = 0$, tak $j = j'$. Je-li $\varepsilon_1 = 1$, tak $j = 2^m + j'$. Pro $j < 2^m$ má tedy $v_{s(a)}$ v pozicích j a $2^m + j$ hodnotu stejnou jako v_a v pozici j, takže $v_{s(a)} = (v_a, v_a)$. Podobně $v_{x_1+s(a)} = (v_a, 1 + v_a)$.

Ať H_2 označuje Sylvestrovu H-matici řádu 2. Pro $m = 1$ tvrzení plyne z toho, že $\mathcal{R}(1, 1) = C(H_2) = \mathbb{F}_2^2$. Indukční přechod dostáváme z toho, že zdvojení $H \to (H \ H)$ souhlasí se zdvojením $v_a \to (v_a, v_a)$, zatímco $H \to (H \ -H)$ odpovídá $v_a \to (v_a, 1 + v_a)$. □

Ukážeme, že není možné konstruovat $(n, 2n, d)$ kódy tak, aby bylo $d > n/2$. Podobně ukážeme, že neexistují $(n, k, n/2)$ kódy, pro které by bylo $k > 2n$. Hadamardovy kódy jsou proto optimální pro volby parametrů $d \geq n/2$ a $k \geq 2n$.

Tvrzení 7.3. *Ať C je (n, k, d) kód takový, že $d > n/2$. Potom $k \leq 2d/(2d - n) \leq n + 1$.*

Důkaz. Představme si orientovaný graf s ohodnocenými hranami, které mohou být vícenásobné, jehož vrcholy jsou kódová slova C a kde mezi $u, v \in C$, $u \neq v$, vede hrana ohodnocená dvojicí $(i, \alpha) \in \{1, \ldots, n\} \times \{0, 1\}$ právě když pro $u = (u_1, \ldots, u_n)$ a $v = (v_1, \ldots, v_n)$ máme $\alpha = u_i \neq v_i$. Celkový počet hran je alespoň $k(k - 1)d$, neboť mezi u a v vede právě $d(u, v) \geq d$ hran.

Označme $k(i, \alpha)$ počet $u \in C$, pro které je $\alpha = u_i$. V grafu se nachází právě $k(i, \alpha) \cdot (k - k(i, \alpha)) \leq k^2/4$ hran ohodnocených dvojicí (i, α). Proto je počet hran nejvýše $(2n)(k^2/4) = nk^2/2$. Dostáváme nerovnost $nk/2 \geq (k - 1)d$, ze které plyne $(2d - n)k \leq 2d$. Druhá nerovnost je patrná z $(n+1)(2d-n) - 2d = n(2d - n - 1) \geq 0$. □

Obdobný odhad lze získat i pro případ q-árních kódů, kde $q > 2$. Vychází se ze stejného grafu, úpravy jsou však o něco málo výpočtově náročnější. V binárním i obecném případě se mluví o *Plotkinově* odhadu.

Tvrzení 7.4. *Ať je n sudé. Pro každý $(n, k, n/2)$ kód C platí $k \leq 2n$.*

Důkaz. Pro $\alpha \in \{0, 1\}$ položme $C_\alpha = \{u \in C;\ u_1 = \alpha\}$ a označme D_α kód vzniklý propíchnutím C_α v pozici 1. Pak D_α (pokud $D_\alpha \neq \emptyset$) je $(n - 1, k_\alpha, d_\alpha)$ kód, kde $k_0 + k_1 = k$ a $d_\alpha \geq d$. Podle Tvrzení 7.3 máme $k_0 + k_1 \leq 2((n-1)+1) = 2n$. □

Kapitolu zakončíme tvrzením o existenci lineárních kódů, které je známo jako *Gilbert-Varšamovova nerovnost.*

Tvrzení 7.5. *Ať n, k a d jsou celá kladná čísla, $d \leq n$. Je-li $V_q(n, d-1) < q^{n-k+1}$, pak existuje q-ární $[n, k, d]$ kód.*

Důkaz. Předpokládejme, že jsme nalezli maximální lineární q-ární kód délky n s minimální vzdáleností d. Označme h jeho dimenzi. Zvolme celé $k > 0$ největší takové, že $V_q(n, d-1) < q^{n-k+1}$. Dokazované tvrzení je možno vyjádřit jako $h \geq k$. Nerovnost $h < k$ je možné zapsat jako $h + 1 \leq k$, a tedy jako $V_q(n, d-1) < q^{n-(h+1)+1} = q^{n-h}$. Pro důkaz sporem tedy stačí ověřit, že tato nerovnost vede ke sporu s maximalitou C.

Přepišme nejprve $V_q(n, d-1) < q^{n-h}$ jako $q^h V_q(n, d-1) < q^n$. Z nerovnosti plyne existence $u \in \mathbb{F}_2^n$, jež splňuje $d(u, x) \geq d$ pro každé $x \in C$. Položme $C' = \{\lambda u + x;\ \lambda \in \mathbb{F}_q \text{ a } x \in C\}$. Váha $\lambda u + x$ je pro $\lambda \neq 0$ stejná jako váha $u + \lambda^{-1} x$, a ta je rovna $d(u, -\lambda^{-1} x) \geq d$. Proto má C' minimální váhu alespoň d. □