3 Designy a konstrukce lineárního Golayova kódu

Fanovu rovinu lze chápat jako systém trojbodových podmnožin, který má tu vlastnost, že každá dvojbodová pomnožina leží právě v jedné trojbodové množině tohoto systému. Každý takový systém se nazývá **Steinerův systém trojic**. (Steiner triple system, STS). Fanova rovina je STS na sedmi bodech. Není obtížné dokázat, že STS na v bodech existuje právě když $v \equiv 1 \bmod 6$ nebo $v \equiv 3 \bmod 6$. STS na 9 bodech snadno zkonstruujeme z matice 3×3, kde 6 trojic je tvořeno řádky a sloupci a dalších 6 trojic získáme jako $\{(i, \sigma(i)); 1 \leq i \leq 3\}$, kde σ probíhá S_3. Tyto trojice tvoří známé schéma počítání determinantu matice řádu 3.

Počet trojic v STS velikosti v lze snadno odvodit. Máme $\binom{v}{2}$ dvojic a každá z nich určuje jednoznačně některou z b trojic. Každá trojice je určena právě třemi dvojicemi, takže musí platit $\binom{v}{2} = 3b$.

Zvolíme-li pevně nějaký bod A nosné množiny, tak ten leží ve $v-1$ dvojicích. Označíme-li r počet trojic, které obsahují daný bod, tak dostaneme $2r = v-1$, neboť každá z r trojic je určena dvěma různými body odlišnými od bodu A.

Podmínka $v \equiv 1, 3 \bmod 6$ je vyjádřením podmínky, aby $v-1$ bylo dělitelné 2 a $\binom{v}{2}$ bylo dělitelné třemi. Dokázali jsme, že každý STS musí tuto podmínku splňovat.

Obecnější pojem než STS jsou designy. Řekneme, že systém bloků $\mathcal{B}$ na množině X je $t{-}(v, k, \lambda)$ **design**, jestliže

- $|X| = v$
- $k = |B|$ pro každé $B \in \mathcal{B}$
- každá t-bodová podmnožina X je obsazena v právě λ blocích $\mathcal{B}$.

STS na v bodech je $2{-}(v, 3, 1)$ design. V teorii designů se připouští, aby se některé bloky $\mathcal{B}$ mohly opakovat (čili taková podmnožina může figurovat v $\mathcal{B}$ vícekrát). Designům bez opakování se říká **jednoduché**. Zde se budeme zabývat pouze jednoduchými designy a v dalším se tedy pod slovem design myslí jednoduchý design. Zaměříme se zejména na $2-(v, k, \lambda)$ designy.

Následující tvrzení zobecňuje úvahy, které jsme již učinili v případě Steinerova systému trojic.

Tvrzení 3.1. *Ať $\mathcal{B}$ je $2{-}(v, k, \lambda)$ design. Označme b počet bloků. Potom*

$$\lambda v(v-1) = bk(k-1).$$

Pro $k \geq 2$ navíc platí, že existuje číslo r, které pro každý bod nosné množiny určuje počet bloků, jež tento bod obsahuje, a které splňuje $\lambda(v-1) = r(k-1)$.

Důkaz. Počítejme velikost w množiny

$$W = \{(A, B);\ B \in \mathcal{B}, A \subseteq B \text{ a } |A| = 2\}.$$

Máme $\binom{v}{2}$ možností pro A, takže $w = \lambda\binom{v}{2}$. Současně pro daný blok B můžeme zvolit $\binom{k}{2}$ dvojic A obsažených v B, odkud $w = b\binom{k}{2}$.

Druhou rovnost pak obdržíme podobnou úvahou, když místo W uvažujme její podmnožinu složenou ze všech (A, B), kde A obsahuje daný vybraný bod. □

Význam písmen v, k, λ, b a r se v dalším výkladu o designech nebude měnit.

Důsledek 3.2. *V každém* $2{-}(v, k, \lambda)$ *designu, kde* $k \geq 2$*, platí* $rv = bk$*.*

□

Ať $\mathcal{B}$ je $t{-}(v, k, \lambda)$ design a ať $B_1, \ldots, B_b$ a $x_1, \ldots, x_v$ jsou nějaká lineární uspořádání bloků $\mathcal{B}$ a bodové nosné množiny. V našich úvahách bude značnou roli hrát *incidenční matice* M, jejíž j-tý řádek je roven incidenčnímu vektoru i_{B_j}.

Následující lemma má charakter pozorování, a proto je uvedeno bez důkazu.

Lemma 3.3. *Ať* M *je incidenční matice* $2{-}(v, k, \lambda)$ *designu. Položme* $U = MM^T$ *a* $V = M^TM$*. Potom*

- $U = (u_{ij})$ *a* $V = (v_{ij})$ *jsou symetrické čvtercové matice řádů* b *a* v*.*
- $u_{ii} = k$ *pro každé* $i \in \{1, \ldots, b\}$
- $v_{jj} = r$ *pro každé* $j \in \{1, \ldots, v\}$
- *Je-li* $1 \leq i < j \leq b$*, tak* $u_{ij} = |B_i \cap B_j|$
- *Je-li* $1 \leq i < j \leq v$*, tak* $v_{ij} = \lambda$*.*

□

Matici $V = M^TM$ můžeme zapsat jako $(r - \lambda)I + \lambda J$, kde I je jednotková matice a J je matice jedničková (tedy matice, která má hodnotu 1 v každé pozici). Z kontextu je zřejmé, že I i J jsou čtvercové matice řádu v. Pro další úvahy bude důležité, že matice V je invertibilní:

Lemma 3.4. *Pro každé* $n \geq 1$ *platí, že* $\det(sI + tJ) = (s + nt)s^{n-1}$*.*

Důkaz. Odečteme nejprve poslední sloupec matice ode všech předchozích a pak přičteme součet všech předchozích řádků k poslednímu. Získáme matici, která má na hlavní diagonále hodnotu s ve všech řádcích mimo posledního, v dolním pravém rohu má hodnotu $s + nt$, a všude pod diagonálou má nuly. □

Věta 3.5. *Ať* $k \geq 2$*. Ať* $\mathcal{B}$ *je systém* k*-bodových podmnožin* v*-bodové množiny* X *a ať* $v = |\mathcal{B}|$*. Předpokládejme, že každý bod množiny* X *leží ve stejném počtu bloků. Potom je tento počet roven* k *a platí, že* $\mathcal{B}$ *je* $2 - (v, k, \lambda)$ *design právě když pro každé dva různé bloky* B *a* C *je* $|B \cap C| = \lambda$*.*

Důkaz. Označme M incidenční matici designu $\mathcal{B}$ a použijme stejné označení jako v Lemmatu 3.3. Matice U a V jsou čtvercové řádu v. Protože předem nepředpokládáme, že $\mathcal{B}$ je nutně 2-design, tak o V pouze víme, že je symetrickou maticí, kde v_{ij} udává počet bloků, které obsahují prvky x_i a x_j.

Součet hodnot na diagonále je jak pro U tak pro V roven velikosti množiny $\{(x, B);\ x \in B \text{ a } B \in \mathcal{B}\}$. Podle předpokladů věty jsou hodnoty u_{ii} (velikost i-tého bloku) a v_{ii} (počet bloků obsahujících bod x_i) na volbě i nezávislé. Proto $k = v_{ii} = u_{ii}$ pro každé i, $1 \leq i \leq k$.

Tvrzení věty lze tedy vyjádřit vztahem

$$MM^{\mathsf{T}} = (k-\lambda)I + \lambda J \ \Leftrightarrow\ M^{\mathsf{T}}M = (k-\lambda)I + \lambda J.$$

Determinant matice $(k-\lambda)I+\lambda J$ je podle Lemmatu 3.4 roven $(k-\lambda)^{n-1}(k+(v-1)\lambda)$. Případ $k = \lambda$ lze opominout, neboť ten, jak lze nahlédnout například s použitím Tvrzení 3.1, v obou případech znamená, že $\mathcal{B}$ obsahuje jediný blok, odkud $v = 1 = k$. Ať tedy je $k > \lambda$. Potom $\det M \neq 0$, neboť $\det MM^{\mathsf{T}} = \det M^{\mathsf{T}}M = (\det M)^2$. Vztah $MM^{\mathsf{T}} = M^{\mathsf{T}}M$ lze pak vyjádřit jedank jako $M^{-1}(MM^{\mathsf{T}})M = MM^{\mathsf{T}}$, jednak jako $M(M^{\mathsf{T}}M)M^{-1} = M^{\mathsf{T}}M$. Protože předpokládáme, že známe vyjádření MM^{T} nebo vyjádření $M^{\mathsf{T}}M$, tak pro dokončení důkazu stačí ověřit, že M komutuje s maticí $(k-\lambda)I+\lambda J$. Protože M jistě komutuje s I, jde o to, zda komutuje s J. Matice MJ má v každé buňce hodnotu k, neboť všechny bloky $\mathcal{B}$ jsou velikosti k. Matice JM má ovšem v každé buňce také hodnotu k, neboť každý bod leží přesně v k blocích. □

Systémy, které vyhovují větě 3.5, se nazývají **čtvercové (kvadratické) designy**, někdy též **symetrické designy**. Jsou to 2–(v, k, λ) designy, které mají právě v bloků. Rovnosti z Tvrzení 3.1 se redukují na $r = k$ a $\lambda(v-1) = k(k-1)$. V těchto desginech je role bodu a bloku záměnná, neboť transponováním incidenční matice vznikne matice, která je rovněž incidenční maticí 2-designu.

Pro další výklad jsou důležité 2$-(11, 5, 2)$ designy. Z rovnosti $\lambda v(v-1) = bk(k-1)$ uvedené v Tvrzení 3.1 plyne, že $220 = 20b$, tedy $b = v = 11$. Takže tyto designy jsou čvercové.

Položme $Y = \{1, 2, 3, 4, 5\}$ a ať X je množina všech dvouprvkových podmnožin Y. Grafem na Y rozumíme nějakou podmnožinu X. Je-li dán graf na Y takový, že z každého vrcholu vycházejí právě dvě hrany, vidíme, že takový graf propojuje všechny vrcholy Y. Tedy tvoří pěticyklus. Každý pěticyklus lze orientovat dvěma způsoby, a každá z těchto orientací poskytuje permutaci $\varphi \in S_5$ řádu 5. Opačná orientace samozřejmě dává inverzní permutaci φ^{-1}. Položme $P = \{\varphi \in S_5, |\varphi| = 5\}$. Pro každé $\varphi \in P$ ať $P_\varphi = \{\{i, \varphi(i)\}, i \in Y\}$. Vidíme, že P_φ je pěticyklus a že každý pěticyklus lze vyjádřit tímto způsobem. Pro φ, $\psi \in P$ máme $P_\varphi = P_\psi$ právě když $\varphi = \psi^{\pm 1}$. Na Y tedy existuje $12 = |P|/2$ pěticyklů.

Pro φ, $\psi \in P$ ať $t(\varphi, \psi) = |\{i \in Y;\ \psi(i) = \varphi^{\pm 1}(i)\}|$. Zjevně $t(\varphi, \psi) = |P_\varphi \cap P_\psi|$. Jelikož $P_{\varphi^2} \cup P_\varphi = X$, tak $t(\varphi, \psi) + t(\varphi^2, \psi) = 5$. Dva pěticykly na Y, které

se shodují ve čtyřech hranách se již shodují zcela, takže $t(\varphi,\psi) \notin \{1,4\}$. Zřejmě $t(\varphi,\psi) = 5 \Leftrightarrow \psi = \varphi^{\pm 1}$ a $t(\varphi,\psi) = 0 \Leftrightarrow \psi = \varphi^{\pm 2}$. Pro zbylých 20 permutací ψ platí buď $t(\varphi,\psi) = 2$ a $t(\varphi^2,\psi) = 3$, nebo $t(\varphi,\psi) = 3$ a $t(\varphi^2,\psi) = 2$. Obě skupiny jsou zjevně stejně velké.

Lemma 3.6. *Definujme na P relaci ρ tak, že $(\varphi,\psi) \in \rho \Leftrightarrow t(\varphi,\psi) \in \{0,2\}$. Tato relace je ekvivalence a každá její ekvivalenční třída má 12 prvků.*

Důkaz. Potřebujeme dokázat, že ρ je tranzitivní relace. Ať $(\varphi,\psi) \in \rho$ a $(\varphi,\psi') \in \rho$. Případy $\psi = \varphi^{\pm 1}$, $\psi' = \varphi^{\pm 1}$ a $\psi' = \psi^{\pm 1}$ jsou triviální, takže předpokládáme, že žádný z nich nenastává. Cílem je tedy ukázat, že

$$t(\varphi,\psi) = t(\varphi,\psi') = 2 \text{ a } \psi' \neq \psi^{\pm 1} \Rightarrow t(\psi,\psi') = 2.$$

Prvky Y můžeme případně přejmenovat, tak aby cyklický zápis permutace φ byl roven (1 2 3 4 5). Definujme φ_i jako permutaci ($i{+}1$ $i{+}2$ i $i{-}2$ $i{-}1$). Ta se shoduje s φ v bodech $i+1$ a $i-2$, a s φ^{-1} v žádném bodě. Pro všechna $i \in Y$ tedy máme $t(\varphi,\varphi_i^{\pm 1}) = 2$. Z Lemmatu 3.8 plyne, že neexistuje žádné jiné $\psi \in P$, $\psi \neq \varphi_i^{\pm 1}$, které by splňovalo $t(\varphi,\psi) = 2$. Je tedy třeba ukázat, že $t(\varphi_j,\varphi_k) = 2$ pro všechna $j,k \in Y$, $j \neq k$. Dvojici $\{j,k\}$ lze vyjádřit jako $\{i,i+1\}$ nebo jako $\{i,i+2\}$, kde $i \in Y$. Máme

$$\varphi_{i+1} = (i{+}2\ i{-}2\ i{+}1\ i{-}1\ i) \text{ a } \varphi_{i+2} = (i{-}2\ i{-}1\ i{+}2\ i\ i{+}1).$$

Permutace φ_i se cs φ_{i+1} nikdy neshoduje a s φ_{i+2} se shoduje v bodech $i+2$ a $i-2$. Permutace φ_i^{-1} se s φ_{i+2} neshoduje nikde a s φ_{i+1} se shoduje v bodech $i+1$ a i. Tvrzení je dokázáno. □

Pro každé $i \in Y$ položme $F_i = \{\{a,b\} \in X;\ i \in \{a,b\}, a \neq b\}$. Dále ať $X' = X \cup \{\infty\}$ a $F_i' = F_i \cup \{\infty\}$, $1 \leq i \leq 5$.

Zvolme $\varphi \in P$ a položme

$$\Phi = \{\psi \in P; (\varphi,\psi) \in \rho\} \quad \text{a} \quad B_\varphi = \{P_\varphi; \varphi \in \Phi\} \cup \left\{F_i';\ i \in Y\right\}.$$

Množinu B_φ chápeme jako design na X', tedy jako množinu 11 bloků velikosti 5.

Lemma 3.7. *Systém B_φ je $2{-}(11,5,2)$ design pro každé $\varphi \in S_5$, $|\varphi| = 5$.*

Důkaz. Je-li $i \leq i < j \leq 5$, tak $F_i' \cap F_j' = \{\infty,\{i,j\}\}$. Je-li $\psi,\psi' \in \Phi$ a $P_\psi \neq P_{\psi'}$, tak $|P_\psi \cap P_{\psi'}| = t(\psi,\psi') = 2$. Je-li $i \in Y$ a $\psi \in \Phi$, tak $F_i' \cap P_\psi = \{\{(i,\psi(i)\},\{i,\psi^{-1}(i)\}\}$. Lemma tudíž plyne z Věty 3.5. □

Dva designy se nazývají **izomorfní**, jestliže existuje bijekce jejich nosných množin, která převádí bloky jednoho designu na bloky druhého designu.

Jsou-li $\varphi,\psi \in P$ a $(\varphi,\psi) \in \rho$, tak z definice B_φ plyne, že se shoduje s B_ψ. Pokud neplatí $(\varphi,\psi) \in \rho$, tak jsou B_φ a B_ψ různé designy. Jsou však izomorfní, neboť pokud přejmenujeme prvky Y tak, aby cyklický zápis φ či ψ byl roven (1 2 3 4 5), tak vždy dostaneme stejný design.

Lemma 3.8. *Až na izomorfismus existuje jediný* $2{-}(11,5,2)$ *design.*

Důkaz. Ať $\mathcal{B}$ je takový design na množině X', kde $\infty \in X'$. Označme F_i', $1 \leq i \leq 5$, bloky $\mathcal{B}$, které obsahují bod ∞ a položme $F_i = F_i' \setminus \{\infty\}$.

Podle Věty 3.5 je $|F_i \cap F_j| = 1$ kdykoliv $1 \leq i < j \leq 5$. Takových dvojic (i,j) je právě $10 = |X|$. Protože žádné $a \in X$ neleží ve třech různých množinách F_k, $k \in Y$, je každé $a \in X$ možné jednoznačně vyjádřit jako $\{a\} = F_i \cap F_j$. Tím dostáváme ztotožnění X s dvoubodovými podmnožinami množiny Y. Každý blok $B \in \mathcal{B}$, který neobsahuje ∞, poskytuje nějaký graf na Y. Pro $i \in Y$ je $|B \cap Y_i| = 2$, takže z každého vrcholu vycházejí právě dvě hrany. To ale znamená, že B je pěticyklus a že ho lze vyjádřit jako P_φ, kde $\varphi \in P$. Je-li P_ψ nějaký jiný blok $\mathcal{B}$, tak z $|P_\varphi \cap P_\psi| = 2$ plyne $t(\varphi,\psi) = 2$, a proto $\mathcal{B} = B_\varphi$. □

Důsledek 3.9. *Až na izomorfismus existuje jediný* $2{-}(11,6,3)$ *design.*

Důkaz. Pro $2{-}(11,5,2)$ design $\mathcal{B}$ na X položme $\mathcal{B}' = \{X \setminus B;\, B \in \mathcal{B}\}$. Pokud B_1 a B_2 jsou dva různé bloky $\mathcal{B}$, tak $|B_1 \cap B_2| = 2$, a proto $(X \setminus B_1) \cap (X \setminus B_2) = X \setminus (B_1 \cup B_2)$ má $11-(5+5-2) = 3$ bodů. $2{-}(11,6,3)$ designy jsou čtvercové, jelikož $3 \cdot 11 \cdot 10 = 11 \cdot 6 \cdot 5$. Podle Věty 3.5 je $\mathcal{B}'$ tedy $2{-}(11,6,3)$ designem. Z každého $2{-}(11,5,2)$ designu lze opačným postupem získat $2{-}(11,6,3)$ design, takže tvrzení je skutečně přímý důsledek Tvrzení 3.10. □

Ať F je komutativní těleso a ať $1 \leq i_1 < \ldots < i_k \leq n$ jsou celá čísla. Zobrazení $F^n \to F^{n-k}$, které z vektoru $(u_1,\ldots,u_n)$ vynechá pozice $i_1,\ldots,i_k$, je jistě homomorfismem vektorových prostorů. Jádro homomorfismu tvoří vektory $(u_1,\ldots,u_n)$ takové, že $u_j = 0$, kdykoliv $1 \leq j < i_1$ nebo $i_k < j \leq n$ nebo $i_s < j < i_{s+1}$ pro nějaké s, $1 \leq s < k$. Jinými slovy, v jádru jsou všechny vektory, kde nenulové hodnoty jsou pouze na pozicích $i_1,\ldots,i_k$.

Uvedenému lineárnímu zobrazení budeme říkat **propíchnutí** v pozicích $i_1,\ldots,i_k$.

Je-li C nějaký $[n,k,d]_q$ kód, tak jeho obrazem bude **propíchnutý kód** $C_{i_1,\ldots,i_k}$. Propíchnutý kód je $[n,k-h]_q$ kód, kde h je dimenze prostoru všech kódových slov C, které jsou nulové mimo pozice $i_1,\ldots,i_k$.

Lemma 3.10. *Ať C je $[n,k,d]_q$ kód, kde $d > 1$. Pak pro každé i, $1 \leq i \leq n$, je propíchnutý kód C_i délky $n-1$ a dimenze k. Jeho minimální váha je $d-1$ nebo d, přičemž první případ nastane, pokud existuje $u \in C$ takové, že $|u| = d$ a $u_i = 0$.*

Důkaz. Z $d > 1$ plyne, že žádné kódové slovo nemá váhu 1. Proto se propíchnutím dimenze nezmění. Ať $u \in C$ a ať u' je propíchnuté slovo vzniklé z u. Pak $|u'|$ je rovno $|u|$ nebo $|u|-1$. Slovo váhy $d-1$ může v C_i tedy vzniknout jen v popsané situaci. □

Lemma 3.11. *Označme N symetrickou matici, která je incidenční maticí* $2{-}(11,6,3)$ *designu. Ať C je samoduální dvojnásobně sudý* $[24,12,8]$ *kód, který*

obsahuje kódová slova vah 24 *a* 12. *Každý propíchnutý kód* C_i, $1 \leq i \leq 24$, *je permutačně ekvivalentní kódu*

$$\begin{pmatrix} I & \begin{matrix} 1 & \cdots & 1 \end{matrix} \\ & N \end{pmatrix}$$

přičemž

$$\begin{pmatrix} & \begin{matrix} 0 & 1 \cdots 1 \end{matrix} \\ I & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \quad N \end{pmatrix}$$

je kód permutačně ekvivalentní kódu C.

Důkaz. Ať w je binární slovo délky 24, které obsahuje samé jedničky. Podle předpokladu existují slova w' a w'' váhy 12 taková, že $w = w' + w''$, přičemž $w' \cap w'' = 0$. Můžeme předpokládat, že pozice i, ve které propíchneme C, splňuje $w'_i = 0$. Zpermutujme pozice tak, aby $w'_1 = w'_2 = \cdots = w'_{12} = 0$ a $w'_{13} = w'_{14} = \cdots = w'_{24} = 1$. Bez újmy na obecnosti nyní můžeme dokonce předpokládat, že $i = 1$. Uvažme všechna $v \in C$ taková, že $v_j = 0$ pokud $1 \leq j \leq 12$. Z $12 = |v| + |w' + v|$ plyne $v \in \{0, w'\}$, neboť C je minimální váhy 8. Propíchnutím C na pozicích 13 až 24 tedy získáme kód délky 12 a dimenze 11. Pokud by prověrková matice tohoto kódu obsahovala alespoň jednu nulu, tak by tento kód obsahoval slovo váhy 1. Pak by bylo možné nalézt $u \in C$ tak, že $|u \cap w''| \equiv 1 \bmod 2$, což je ve sporu s předpokladem $|u \cap w''| \equiv u \cdot w'' = 0 \bmod 2$. Uvažovaná prověrková matice má tedy samé jedničky, takže vzniklý kód je paritní. Je proto možné vytvořit matici, jejíž řádky jsou složeny z kódových slov, která má následující tvar (nuly ve sloupci 13 lze získat odečítáním prvého řádku od všech ostatních).

$$\begin{pmatrix} 0 & \begin{matrix} 0 \cdots 0 \end{matrix} & 1 & \begin{matrix} 1 \cdots 1 \end{matrix} \\ 1 & & 0 & \\ \vdots & I & \vdots & M \\ 1 & & 0 & \end{pmatrix}$$

Tato matice se skládá z řádků lineárně nezávislých, a proto je generující maticí kódu C. Vyměníme-li sloupec 1 se sloupcem 13, dostaneme tvar

$$\begin{pmatrix} & \begin{matrix} 0 & 1 \cdots 1 \end{matrix} \\ I & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \quad M \end{pmatrix}$$

Buďte $u_1, \ldots, u_{11}$ řádky matice M. Kód C je dvojnásobně sudý, a proto u_j musí mít váhu 2, 6 nebo 10. Současně mají ale váhu alespoň 6. V případě váhy 10 bychom dostali váhu 4 součtem s w'. Čili $|u_j| = 6$, kde $1 \leq j \leq 11$. Pro $1 \leq r < s \leq 11$ je ze stejných důvodů $u_r + u_s$ také váhy 6, takže $2|u_r \cap u_s| = |u_r| + |u_s| - |u_r + u_s| = 6$. Vidíme, že M je podle Věty 3.5 incideční maticí $2{-}(11, 6, 3)$ designu. Podle Tvrzení 3.10 lze přehazováním řádků a sloupců převést M na N. Pokud výměnu řádků r a s doprovodíme výměnou sloupců r a s, získáme generující matici v požadovaném tvaru. □

Uvažme znovu matici $G = (I\ S)$, kde

$$S = \begin{pmatrix} 0 & 1 \cdots 1 \\ 1 & \\ \vdots & N \\ 1 & \end{pmatrix}$$

.

Jde o generující matici nějakého kódu C. Každé dva řádky G mají sudý počet společných jedniček, a proto je C kód samoduální. Z Lemmatu 2.10 vyplývá, že je to kód dvojnásobně sudý. Protože matice S je symetrická a $C = C^{\perp}$, je $G' = (S\ I)$ také generující maticí.

Dále dokazujeme, že $d = 8$. Pro spor předpokládejme, že existuje $v \in C$ váhy 4. Ať $A \subseteq \{1, \ldots, 24\}$ jsou ty indexy, že $v_i = 1$ právě pro $i \in A$. Položme $a = |A \cap \{1, \ldots, 12\}|$. Vidíme, že v je součtem a řádků matice G a $4 - a$ řádků matice G'. Případ $a \neq 2$ lze zjevně okamžitě vyloučit. Ať $v = u_i + u_j$, kde $u_1, \ldots, u_{12}$ jsou řádky G a $1 \leq i < j \leq 12$. Je-li $i = 1$, je $|v| = 3 + (11 - 6) = 8$ a pro $i \geq 2$ je obdobně $|v| = 2 + 6 = 8$. Minimální váha kódu C je tedy 8.

Tvrzení 3.12. *Až na permutační ekvivalenci existuje jediný* $[24, 12, 8]$ *kód, který je dvojnásobně sudý, samoduální a obsahuje kódová slova vah* 12 *a* 24. *Všechny kódy z něj odvozené propíchnutím v jedné pozici jsou vzájemně permutačně ekvivalentní.*

Důkaz. Důkaz plyne z úvah předchozího odstavce. □

Kód délky 24 popsaný v Tvrzení 3.14 se nazývá **rozšířený Golayův kód**. Perfektním **binárním Golayovým kódem** se pak nazývá kód délky 23, který z něj získáme propíchnutím.