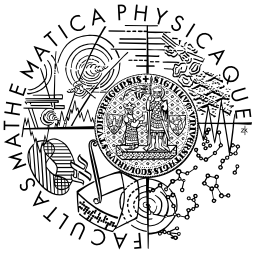


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Tomáš Janovský

Binární kódy indukované hranovým grafem n-dimenzionální krychle

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.

Studijní program: Matematika pro informační technologie

Praha 2024

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Za veškerou ochotu, trpělivost, čas a mnoho cenných rad při psaní bakalářské práce bych rád poděkoval svému školiteli doc. Mgr. et Mgr. Janu Žemličkovi Ph.D. Dále bych rád poděkoval kamarádovi Janu Frnkovi za přečtení mé práce a dodání svých poznatků. Nakonec bych rád poděkoval své rodině za podporu během celého mého studia.

Název práce: Binární kódy indukované hranovým grafem n-dimenzionální krychle

Autor: Tomáš Janovský

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: Tato práce se zabývá binárními kódy indukovanými hranovým grafem n-dimenzionální krychle, dále kódy designu definovaného pomocí vrcholového grafu n-dimenzionální krychle a nakonec duály těchto kódů. První kapitola je věnována uvedením do tématu a jsou zde definovány potřebné pojmy z teorie lineárních kódů, grafů a designů. Druhá kapitola se věnuje konstrukci výše zmíněných kódů, popisu jejich základních parametrů jako jsou dimenze a Hammingova vzdálenost kódu a nakonec také popisu generujících matic těchto kódů. Na závěr se poslední kapitola zabývá duály kódů zkonstruovaných v druhé kapitole především pak opět popisu Hammingovy vzdálenosti.

Klíčová slova: kód indukovaný grafem, n-dimenzionální krychle, hranový graf

Title: Binary codes induced by the line graph of an n-dimensional cube

Author: Tomáš Janovský

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This paper deals with the binary codes from the line graph of the n-cube, then the codes of the design, which is defined by the vertex graph of the n-cube, and finally the dual codes of these codes. The first chapter is devoted to an introduction to the topic and the necessary concepts from the theory of linear codes, graphs and designs are defined there. The second chapter is devoted to the construction of the aforementioned codes, the description of their basic parameters such as the dimension and the Hamming distance of the code, and finally the description of the generating matrices of these codes. Finally, the last chapter deals with the dual codes of the codes constructed in the second chapter especially again the description of the Hamming distance.

Keywords: code induced by graph, n-dimensional cube, line graph

Obsah

Úvod

V digitální éře, kde se informace stávají nedílnou součástí našich životů, je spolehlivost přenosu a uchování dat nezbytná. Žádný přenos nebo digitální záznam informace však nemusí být bezchybný, například kvůli elektromagnetickému šumu, či nedokonalému přenosovému kanálu. Tím se dostáváme k důležitosti konceptu samoopravných kódů. Jak už z názvu vyplývá, studium samoopravných kódů má za cíl tvorbu kódů s dobrou opravou chyb. Pro to, aby kód byl schopen dobré opravy chyb, musí mít kódová slova dostatečnou takzvanou Hammingovu vzdálenost. Hammingovou vzdáleností slov zde myslíme počet písmen (složek), ve kterých se kódová slova liší a Hammingovou vzdáleností kódu myslíme minimum z těchto vzdáleností pro jeden daný kód. Protože chceme posílat zprávu co nejlevněji, ale zároveň s malou pravděpodobností chyby, hledáme takové kódy, které mají dostatečnou Hammingovu vzdálenost, obsahují dostatečný počet slov a kódová slova tohoto kódu nejsou příliš dlouhá.

Jednou z mnoha konstrukcí samoopravných kódů jsou kódy indukované grafy. Tyto kódy jsou tvořeny pomocí matic sousednosti a incidence grafů, přičemž za množinu kódových slov daného kódu uvažujeme lineární obal řádků těchto matic. Jednou skupinou takových kódů jsou kódy indukované grafy n-dimenzionální krychle. Kódy indukovanými grafy n-dimenzionální krychle se zabývali matematici Washiela Fish, Jennifer D. Key a Eric C. Mwambene v článcích Fish et al., 2009a, Fish et al., 2009b a Fish et al., 2010, přičemž první dva zmíněné články se zabývají kódy indukovanými vrcholovým grafem n-dimenzionální krychle, a podobnými kódy těmto kódům, a třetí se zabývá kódy indukovanými hranovým grafem n-dimenzionální krychle. Jak už z názvu práce a z výše napsaného plyne, v této práci se zabýváme kódy indukovanými hranovým grafem n-dimenzionální krychle a vycházíme z třetího zmíněného článku Fish et al., 2010. Tyto kódy jsou zkoumány hlavně v souvislosti s permutačním kódováním a dekódováním, ale tím se v této práci zabývat nebudeme.

Hlavním cílem této práce je ukázat konstrukci a vlastnosti kódu designu definovaného pomocí vrcholového grafu n-dimenzionální krychle, dále, a to především, kódu indukovaného hranovým grafem n-dimenzionální krychle a nakonec popsat vlastnosti duálů těchto kódů. U těchto kódů ukážeme jejich základní parametry, tedy jejich dimenzi a Hammingovu vzdálenost.

První kapitola obsahuje základní definice potřebné pro pochopení tématu. Nejprve jsou uvedeny definice zabývající se kódy, poté definice z teorie grafů a nakonec definice struktury incidence a designu. V druhé kapitole se věnujeme dimenzi a Hammingově váze kódu definovaného pomocí matice incidence vrcholového grafu n-dimenzionální krychle a kódu indukovaného hranovým grafem n-dimenzionální krychle. Je zde dokázáno, že dimenze prvního z výše zmíněných kódů je $2^n - 1$ a druhého $2^n - 2$. Dále zde ukazujeme, že minimální vzdálenost prvního jmenovaného kódu je n a druhého $2(n - 1)$. Na závěr této kapitoly také popisujeme, jak mohou vypadat generující matice těchto kódů. Poslední kapitola je pak věnována duálům výše zmíněných kódů, neboli ortogonálním doplňkům prostorů kódů. U nich dokazujeme, že minimální vzdálenost je pro $n \geq 3$ rovna 4.

1 Základní teorie

V celém textu budeme pracovat převážně s vektorovými prostory $\mathbb{F}^n$ nad konečným tělesem $\mathbb{F}$, ve většině případů dokonce pouze nad binárním tělesem $\mathbb{F}_2$. Kódovým slovem myslíme řádkový vektor $\boldsymbol{u} \in \mathbb{F}^n$, tedy $\boldsymbol{u} = u_1 \dots u_n$. Bodovým součinem dvou slov $\boldsymbol{u} = u_1 \dots u_n$ a $\boldsymbol{v} = v_1 \dots v_n$ rozumíme $\boldsymbol{u} \cdot \boldsymbol{v} = \sum_{i=1}^{n} u_i \cdot v_i$. V celém textu také uvažujeme pouze netriviální kódy, tedy kódy $\mathcal{C}$ takové, že $|\mathcal{C}| > 1$. Dále v celém textu bude $\boldsymbol{e}_i$ značit i-tý vektor kanonické báze a $\mathbf{1}$ bude značit řádkový jedničkový vektor, tedy $\mathbf{1} = \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}$.

Základní definice v této kapitole vycházejí převážně z Žemlička, 2024, pro definice z teorie samoopravných kódů, Matoušek; Nešetřil, 2000, pro teorii grafů, a Beth, 1985, pro definici struktury incidence a designu.

1.1 Lineární kódy

Začneme s definicemi lineárního kódu, Hammingovy vzdálenosti a definicemi generující a kontrolní matice.

Definice 1 (Lineární kód)**.** *Množina $\mathcal{C} \subseteq \mathbb{F}^n$ je lineární kód, jde-li o podprostor aritmetického vektorového prostoru $\mathbb{F}^n$.*

Definice 2 (Hammingova vzdálenost slov, vzdálenost kódu a Hammingova váha)**.** *Nechť $\boldsymbol{u}$, $\boldsymbol{v} \in \mathbb{F}^n$ jsou slova kódu $\mathcal{C}$, kde $\mathcal{C} \subseteq \mathbb{F}^n$, $\mathcal{C} \neq \emptyset$. Pak*

- $\mathrm{d}(\boldsymbol{u},\boldsymbol{v}) = |\{i | u_i \neq v_i\}|$ *se nazývá Hammingova vzdálenost slov $\boldsymbol{u}$ a $\boldsymbol{v}$*
- $\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(\boldsymbol{u},\boldsymbol{v}) | \boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}, \boldsymbol{u} \neq \boldsymbol{v}\}$ *se nazývá Hammingova vzdálenost kódu*
- $\mathrm{w}(\boldsymbol{u}) = \mathrm{d}(\boldsymbol{u}, \mathbf{0})$ *se nazývá Hammingova váha slova $\boldsymbol{u}$*

Hammingově vzdálenosti kódu také říkáme minimální vzdálenost kódu, či pouze vzdálenost kódu. Pro lineární kódy $\mathcal{C} \subseteq \mathbb{F}_q^n$, kde $k = dim_{\mathbb{F}_q^n}(\mathcal{C})$ a $d = \mathrm{d}(\mathcal{C})$ se obvykle používá značení $[n, k]$-kódy, $[n, k]_q$-kódy, či $[n, k, d]_q$-kódy.

Lze snadno nahlédnout, že pro lineární kódy platí

$$\mathrm{d}(\mathcal{C}) = \min(\{\boldsymbol{w}(\boldsymbol{c}) | \boldsymbol{c} \in \mathcal{C} \setminus \{\mathbf{0}\}\}),$$

proto se také někdy $\mathrm{d}(\mathcal{C})$ říká minimální váha kódu. Slova kódu $\mathcal{C}$ s minimální vahou budeme nazývat minimální slova kódu $\mathcal{C}$.

Pro práci s lineárními kódy a často i pro jejich definování se využívají generující a kontrolní matice.

Definice 3 (Generující a kontrolní matice)**.** *Nechť $\mathcal{C}$ je $[n, k]$-kód, kde dimenze $k \in \{0,1,\dots,n\}$, $G \in \mathbb{F}^{k \times n}$ a $H \in \mathbb{F}^{(n-k) \times n}$. Řekneme, že G je generující matice kódu $\mathcal{C}$, jestliže $\mathcal{C} = \mathrm{Im}(G^T)$. Dále řekneme, že matice H je kontrolní matice kódu $\mathcal{C}$, pokud $\mathcal{C} = \mathrm{Ker}(H)$.*

Kódy v této práci jsou definovány maticemi, jejichž řádky generují dané kódy, ale nejsou lineárně nezávislé. Pokud bychom matice upravili elementárními řádkovými úpravami do odstupňovaného tvaru a vynechali nulové řádky z konce matice, dostali bychom právě generující matice. Pro naši práci s kódy, ale budou lepší matice v původním tvaru.

Jak už je výše napsáno, lineární kód je takový kód, který tvoří podprostor vektorového prostoru $\mathbb{F}^n$. Ortogonální doplněk (vzhledem k bodovému součinu) tohoto podprostoru tvoří také podprostor a mluvíme o něm jako o duálu kódu.

Definice 4 (Duál kódu)**.** *Nechť $\mathcal{C}$ je lineární kód, pak duál kódu $\mathcal{C}$ je takový kód $\mathcal{C}^\perp$, který tvoří ortogonální doplněk $\mathcal{C}$ (uvažujeme-li bodový součin), neboli*

$$\mathcal{C}^\perp = \{\boldsymbol{v} \in \mathbb{F}^n | \boldsymbol{v} \cdot \boldsymbol{u} = 0, \forall \boldsymbol{u} \in \mathcal{C}\}.$$

Pomocí duálu kódu definujeme dvě speciální třídy lineárních kódů, samoduální a samoortogonální kódy.

Definice 5 (Samoduální a samoortogonální kód)**.** *Mějme lineární kód $\mathcal{C}$ a jeho duál $\mathcal{C}^\perp$. Pak $\mathcal{C}$ je samoortogonální kód, pokud platí $\mathcal{C} \subseteq \mathcal{C}^\perp$ a samoduální, pokud $\mathcal{C} = \mathcal{C}^\perp$.*

Definice 6 (Permutačně ekvivalentní kódy)**.** *Mějme kódy $\mathcal{C}_1, \mathcal{C}_2 \in \mathbb{F}^n$, $\sigma \in S_n$ (permutaci na množině $\{1, \ldots, n\}$), označíme $\mathcal{C}_1 \sim_\sigma \mathcal{C}_2$ pokud*

$$c_1 \ldots c_n \in \mathcal{C}_1 \equiv c_{\sigma(1)} \ldots c_{\sigma(n)} \in \mathcal{C}_2.$$

O kódech $\mathcal{C}_1, \mathcal{C}_2 \in \mathbb{F}^n$ řekneme, že jsou permutačně ekvivalentní (prostřednictvím permutace $\sigma \in S_n$), jestliže existuje $\sigma \in S_n$ taková, že $\mathcal{C}_1 \sim_\sigma \mathcal{C}_2$.

Definice 7 (Standardní tvar generující matice)**.** *O generující matici lineárního $[n, k]$-kódu řekneme, že je ve standardním tvaru, má-li formu $\left(I_k \;\middle|\; A\right) \in \mathbb{F}^{k \times n}$.*

1.2 Grafy

Definice 8 (Graf)**.** *Graf G je uspořádaná dvojice (V, E), kde V je neprázdná množina a E je množina dvouprvkových podmnožin množiny V. Prvky množiny V se nazývají vrcholy grafu G a prvky množiny E hrany grafu G.*

Definice 9 (Podgraf)**.** *Graf $H = (\widetilde{V}, \widetilde{E})$, je podgrafem grafu $G = (V, E)$, pokud $\widetilde{V} \subseteq V$, $\widetilde{E} \subseteq E$ a zároveň každá hrana z $\widetilde{E}$ má oba vrcholy ve $\widetilde{V}$.*

Definice 10 (Stupeň vrcholu a regulární graf)**.** *Stupeň vrcholu v_i udává počet hran grafu G obsahující v_i. Graf G je regulární, pokud mají každé dva jeho vrcholy stejný stupeň.*

Jak už z naší definice grafu vyplývá v této práci uvažujeme pouze neorientované grafy bez smyček, protože hrany uvažujeme jako dvouprvkové množiny.

Definice 11 (Matice sousednosti grafu)**.** *Mějme graf $G = (V, E)$ s n vrcholy. Označme vrcholy $v_1, \ldots, v_n$. Matice sousednosti grafu G je pak čtvercová matice $A = (a_{i,j})_{n \times n}$ definovaná předpisem*

$$a_{i,j} = \begin{cases} 1 & \text{pro } \{v_i, v_j\} \in E \\ 0 & \text{jinak} \end{cases}$$

Definice 12 (Matice incidence grafu)**.** *Ať $G = (V, E)$ je graf, kde $|V| = n$ a $|E| = m$. Označme vrcholy $V = \{v_1, \ldots, v_n\}$ a hrany $E = \{e_1, \ldots, e_m\}$. Pak matice incidence grafu G je matice $B = (b_{i,j})_{n \times m}$ typu $n \times m$ definovaná předpisem*

$$b_{i,j} = \begin{cases} 1 & \textit{jestliže } v_i \in e_j \\ 0 & \textit{jinak} \end{cases}$$

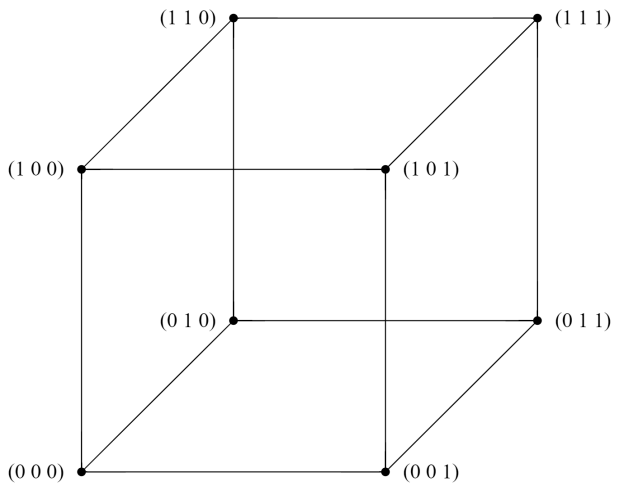
Z definic jasně vyplývá, že podoba matic sousednosti i incidence závisí na tom v jakém pořadí vrcholy (respektive hrany) označíme. Matice sousednosti grafu G jsou pak shodné až na permutaci řádků a sloupců a to samé platí i pro matice incidence grafu G.

Při vytváření kódu budeme pracovat pouze s jednou specifickou skupinou grafů, které se nazývají Hammingovy grafy.

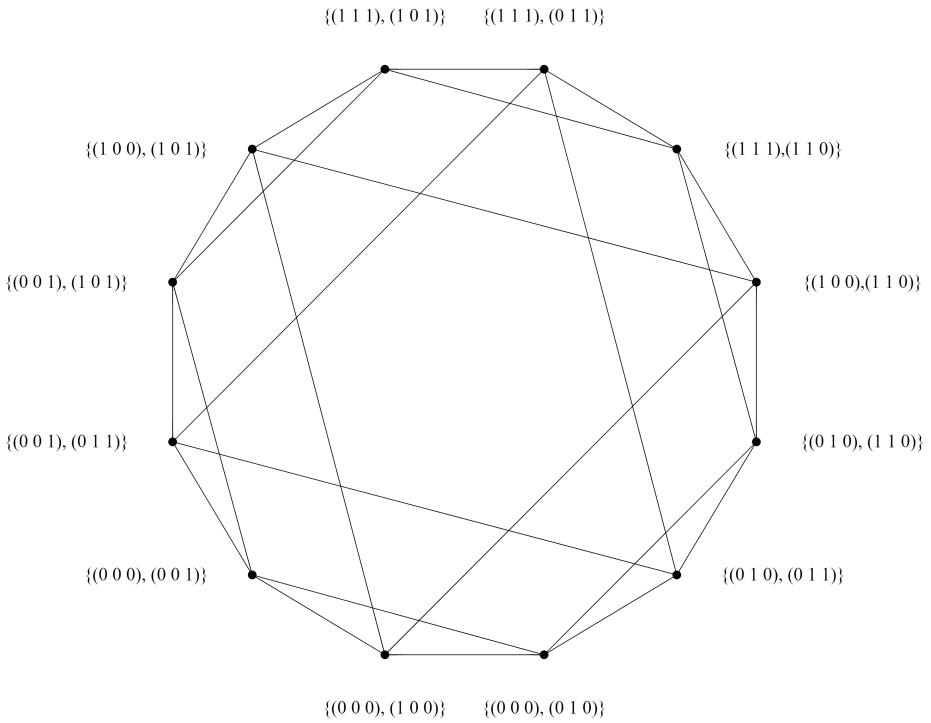
Definice 13 (Hammingův graf a grafy n-dimenzionální krychle)**.** *Mějme dáno $n, m \in \mathbb{N}$ a množinu R velikosti m. Graf $H(n, m) = (V_H, E_H)$ s m^n vrcholy, které označíme n-ticemi z R^n, a hranami, které spojují dva vrcholy právě tehdy, když se n-tice označující vrchol liší v jedné složce, nazýváme Hammingův graf.*

Vrcholovým grafem n-dimenzionální krychle myslíme Hammingův graf, kde $m = 2$, a značíme jej Q_n. Tedy $Q_n = (V_n, E_n)$, kde pro vrcholy a hrany platí, že $V_n = \mathbb{F}_2^n$ a $E_n = \{\{\boldsymbol{u}, \boldsymbol{v}\} | , \boldsymbol{u}, \boldsymbol{v} \in V_n, d(\boldsymbol{u}, \boldsymbol{v}) = 1\}$.

Hranovým grafem n-dimenzionální krychle, myslíme graf $L(Q_n) = (E_n, H_n)$, kde $H_n = \left\{\{h_1, h_2\} \subseteq E_n \middle| \, |h_1 \cap h_2| = 1\right\}$.



Obrázek 1.1 Vrcholový graf 3-dimenzionální krychle



Obrázek 1.2 Hranový graf 3-dimenzionální krychle

Definice 14 (Kódy indukované grafem)**.** *Mějme graf G a jeho matici sousednosti A. O kódu $\mathcal{C}$ řekneme, že je indukovaný grafem G, jestliže je lineární obal řádkových vektorů matice A roven množině všech slov kódu $\mathcal{C}$.*

1.3 Struktura incidence a designy

Definice 15 (Struktura incidence a design)**.** *Trojici $\mathcal{D} = (\mathcal{P},\mathcal{B},\mathcal{I})$, kde $\mathcal{P}$ je množina bodů, $\mathcal{B}$ je množina bloků a $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ je binární relace, zvaná incidence, nazýváme struktura incidence.*
Konečnou strukturu incidence $\mathcal{D} = (\mathcal{P},\mathcal{B},\mathcal{I})$ nazve blokový $t-(v,k,\lambda)$ design $(t,v,k,\lambda \in \mathbb{N})$, pokud $|\mathcal{P}| = v$, každý blok $B \in \mathcal{B}$ je incidentní právě s k body z $\mathcal{P}_n$, tedy $\forall B \in \mathcal{B} : \left|\{p \in \mathcal{P} | (p,B) \in \mathcal{I}\right| = k$ a právě t bodů je incidentních právě s λ bloky, tedy $\forall M \subseteq \mathcal{P}$, že $|M| = t$, platí $|\{B \in \mathcal{B} | (p,B) \in \mathcal{I}; \forall p \in M\}| = \lambda$.
Design nazýváme symetrický, pokud platí $|\mathcal{P}| = |\mathcal{B}|$.

Definice 16 (Matice incidence designu $\mathcal{D}$)**.** *Mějme design $\mathcal{D} = (\mathcal{P},\mathcal{B},\mathcal{I})$, kde $b = |\mathcal{B}|$ a $v = |\mathcal{P}|$. Matici $M = (m_{i,j})_{b \times v}$, kde řádky reprezentují bloky a sloupce body designu $\mathcal{D}$, pro níž platí $m_{i,j} = 1$, pokud je i-tý blok incidentní s j-tým bodem, a $m_{i,j} = 0$ v opačném případě, nazýváme maticí incidence designu $\mathcal{D}$.*

Definice 17 (Kód designu $\mathcal{D}$)**.** *Mějme design $\mathcal{D}$ a jeho matici incidence G. O kódu $\mathcal{C}$ řekneme, že je kódem designu $\mathcal{D}$, jestliže je lineární obal řádkových vektorů matice G roven množině všech slov kódu $\mathcal{C}$.*

2 Kódy indukované grafy n-dimenzionální krychle

2.1 Hranový graf n-dimenzionální krychle

V této sekci uvažujeme vrcholový graf n-dimenzionální krychle Q_n a hranový graf n-dimenzionální krychle $L(Q_n)$ dle definic výše. Nejprve v jednoduchém lemmatu ukážeme počet hran grafu Q_n a poté pomocí grafu $L(Q_n)$ zadefinujeme strukturu incidence $\mathcal{D}(L(Q_n))$.

Lemma 1. *Vrcholový graf n-dimenzionální krychle má $2^{n-1}n$ hran.*

Důkaz. Podle definice hran n-dimenzionální krychle je jasné, že z každého vrcholu vede právě n hran, neboli graf je regulární a každý vrchol je stupně n. Vrcholů je opět dle definice 2^n. Dále každá hrana spojuje dva vrcholy, tedy všech hran je právě $\frac{2^n n}{2} = 2^{n-1}n$.

□

Definice 18 (Struktura incidence $\mathcal{D}(L(Q_n))$)**.** *Mějme hranový graf $L(Q_n) = (E_n, H_n)$. Pak definujeme strukturu incidence grafu $L(Q_n)$ jako $\mathcal{D}(L(Q_n)) = (E_n, \mathcal{B}, \mathcal{I})$, s body E_n, bloky $\mathcal{B} = \left\{\overline{\{\boldsymbol{u}, \boldsymbol{v}\}} | \{\boldsymbol{u}, \boldsymbol{v}\} \in E_n\right\}$, pro bloky dané vztahem $\overline{\{\boldsymbol{u}, \boldsymbol{v}\}} = \left\{\{\boldsymbol{x}, \boldsymbol{y}\} \in E_n \middle| |\{\boldsymbol{u}, \boldsymbol{v}\} \cap \{\boldsymbol{x}, \boldsymbol{y}\}| = 1\right\}$, a incidencí $\mathcal{I}$ takovou, že pro $h \in E_n$ a $B \in \mathcal{B}$ platí $(h, B) \in \mathcal{I} \iff h \in B$.*

Lemma 2. *Struktura incidence $\mathcal{D}(L(Q_n))$ je $1-(2^{n-1}n, 2(n-1), 2(n-1))$ design.*

Důkaz. Počet bodů tohoto designu je roven počtu hran vrcholového grafu Q_n, tedy $2^{n-1}n$. Z každého vrcholu grafu Q_n jde právě n hran, tedy vypustíme-li v každém vrcholu tu jednu hranu určující daný blok, dostaneme, že každý blok je incidentní s právě $2(n-1)$ body z E_n. Tedy tak i právě každý jeden bod z E_n je incidentní s $2(n-1)$ bloky. Tedy $\mathcal{D}(L(Q_n))$ je $1-(2^{n-1}n, 2(n-1), 2(n-1))$ design.

□

Tento design budeme značit $\mathcal{D}_n$.

Dále zkonstruujeme matici incidence grafu Q_n. Vrcholy grafu Q_n budeme značit binární reprezentací čísel a ztotožňovat toto značení binárními čísly s danými čísly $0, \ldots, 2^n - 1$. Maticí incidence grafu Q_n, rozumíme matici $G_n \in \mathbb{F}^{2^n \times 2^{n-1}n}$ s řádky reprezentujícími vrcholy, přičemž vrcholy jsou řazeny postupně dle jejich binární reprezentace, a sloupci reprezentujícími hrany grafu Q_n. Nejprve nahlédneme na to, jak z grafu Q_{n-1} vzniká graf Q_n. Předpokládejme tedy, že máme graf Q_{n-1} s vrcholy označenými čísly $0, \ldots, 2^{n-1} - 1$, kde u binární reprezentace čísel přidáme každému binárnímu číslu na začátek jeden nulový bit. Dále mějme graf $\widetilde{Q_{n-1}}$ isomorfní grafu Q_{n-1} tak, že vrcholy jsou označeny binárními čísly, které se liší od Q_{n-1} pouze v přidaném prvním bitu, kde bude nyní jednička. Nakonec spojíme vždy vrchol Q_{n-1} s vrcholem $\widetilde{Q_{n-1}}$ pokud se jejich označení liší právě pouze v prvním, přidaném, bitu. Tak dostaneme graf Q_n.

Matice G_n zkonstruujeme induktivně podobným způsobem jako jsme konstruovali graf Q_n výše. Nejprve nahlédneme, že jediná možná matice incidence

grafu Q_1 je $G_1 = \begin{pmatrix}1\\1\end{pmatrix}$. Nyní uvažujme, že už máme sestrojenou matici G_{n-1} a chceme sestrojit matici G_n. Řádky opět reprezentují vrcholy grafu Q_n, ty jsou uspořádány dle své binární reprezentace vzestupně, tedy dle konstrukce grafu Q_n jsou nejprve vrcholy grafu Q_{n-1} a poté vrcholy grafu $\widetilde{Q_{n-1}}$. Sloupce matice reprezentují hrany, které jsou seřazeny následujícím způsobem. Prvních $2^{n-2}(n-1)$ sloupců reprezentují hrany grafu Q_{n-1} seřazené jako u matice G_{n-1}, tedy hrany $\{0,1\},\{0,2\},\{1,3\},\{2,3\},\cdots,\{2^{n-1}-2,2^{n-1}-1\}$. Dalších 2^{n-1} sloupců reprezentuje hrany propojující podgrafy Q_{n-1} a $\widetilde{Q_{n-1}}$ a jsou seřazeny v tomto pořadí: $\{0,2^{n-1}\},\{1,2^{n-1}+1\},\cdots,\{2^{n-1}-1,2^n-1\}$. Posledních $2^{n-2}(n-1)$ sloupců reprezentuje hrany grafu $\widetilde{Q_{n-1}}$ a seřazeny jsou opět stejně jako u matice G_{n-1}, akorát u každé hrany vrcholu přičteme 2^{n-1}, tedy $\{2^{n-1},2^{n-1}+1\}$, $\{2^{n-1},2^{n-1}+2\},\{2^{n-1}+1,2^{n-1}+3\},\{2^{n-1}+2,2^{n-1}+3\},\cdots,\{2^n-2,2^n-1\}$.

Takováto konstrukce nám dává následující lemma.

Lemma 3. *Matici incidence G_n grafu Q_n lze sestrojit správným uspořádáním sloupců tak, že platí*

$$G_n = \begin{pmatrix} G_{n-1} & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & G_{n-1} \end{pmatrix}.$$

Důkaz. Horní blok G_{n-1} je zřejmý, protože znázorňuje prvních 2^{n-1} vrcholů propojených příslušnými hranami. Nulový blok pod tímto blokem je jasný z toho, že každá hrana obsahuje pouze dva vrcholy, tedy v jednom sloupci jsou právě dvě jedničky, které už jsou obsaženy v horním bloku. Pro spodní blok G_{n-1} si stačí uvědomit, že řádky reprezentují druhých 2^{n-1} vrcholů a hrany mezi nimi. Nulový blok nad tímto blokem opět plyne z toho, že každý sloupec obsahuje právě dvě jedničky. Bloky jednotkových matic pak plynou z toho, že se jedná o hrany propojující podgrafy Q_{n-1} a $\widetilde{Q_{n-1}}$.

□

Nyní definujeme k této matici příslušnou strukturu incidence a ukážeme, že se jedná o $1-(2^{n-1}n,n,2)$ design.

Definice 19. *Mějme vrcholový graf $Q_n=(V_n,E_n)$. Pak definujeme strukturu incidence grafu Q_n jako $\mathcal{D}(Q_n)=(E_n,\mathcal{V},\mathcal{I})$, s body E_n, bloky $\mathcal{V}=\{\overline{\boldsymbol{u}}|\boldsymbol{u}\in V_n\}$, pro $\overline{\boldsymbol{u}}=\left\{\{\boldsymbol{u},\boldsymbol{u}+\boldsymbol{e}_i\}\middle| i\in\{1,\ldots,n\}\right\}$, a incidencí $\mathcal{I}$ takovou, že $\forall\{\boldsymbol{u},\boldsymbol{v}\}\in E_n$ a $\forall\overline{\boldsymbol{u}}\in\mathcal{V}$ platí $(\{\boldsymbol{u},\boldsymbol{v}\},\overline{\boldsymbol{u}})\in\mathcal{I}\iff\{\boldsymbol{u},\boldsymbol{v}\}\in\overline{\boldsymbol{u}}$.*

Lemma 4. *Struktura incidence $\mathcal{D}(Q_n)$ je $1-(2^{n-1}n,n,2)$ design, který budeme značit $\mathcal{G}_n$. Maticí incidence tohoto designu je pak matice G_n.*

Důkaz. Počet bodů designu je podle definice $\mathcal{D}(Q_n)$ roven počtu hran grafu Q_n, tedy $2^{n-1}n$. Z definice bloků, kde každý blok obsahuje n hran (bodů) a toho, že blok je incidentní s bodem, pokud daný bod v tomto bloku leží, dostáváme, že každý blok je incidentní právě s n body. Nakonec zbývá dokázat, že každý jeden bod je incidentní právě s dvěma bloky. Z definice bodů lze vidět, že pro $\{\boldsymbol{u},\boldsymbol{v}\}\in E_n$ platí, $\{\boldsymbol{u},\boldsymbol{v}\}=\{\boldsymbol{u},\boldsymbol{u}+\boldsymbol{e}_j\}=\{\boldsymbol{v},\boldsymbol{v}+\boldsymbol{e}_j\}$, pro nějaké $j\in\{1,\cdots,n\}$. Tak dostáváme, že $\{\boldsymbol{u},\boldsymbol{v}\}$ leží právě blocích $\overline{\boldsymbol{u}}$ a $\overline{\boldsymbol{v}}$, tedy každý bod je incidentní s právě dvěma bloky. Také dostáváme, že G_n je maticí incidence tohoto designu.

□

Pomocí matic incidence grafu Q_n rekurentně sestrojíme matici sousednosti grafu $L(Q_n)$, kterou budeme značit M_n.

Lemma 5. *Matice sousednosti $M_n \in \mathbb{Z}^{(2^{n-1}n)\times(2^{n-1}n)}$, grafu $L(Q_n)$, je tvaru*

$$M_n = {G_n}^T G_n - 2I_{2^{n-1}n} = \begin{pmatrix} M_{n-1} & {G_{n-1}}^T & 0 \\ G_{n-1} & 0 & G_{n-1} \\ 0 & {G_{n-1}}^T & M_{n-1} \end{pmatrix},$$

kde G_n je matice incidence grafu Q_n.

Důkaz. Nejdříve dokážeme, že $M_n = {G_n}^T G_n - 2I_{2^{n-1}n}$. Pro zjednodušení označme $m = 2^n$ a $l = 2^{n-1}n$. Víme, že $G_n \in \{0,1\}^{m\times l}$, tedy ${G_n}^T G_n \in \mathbb{N}^{l\times l}$. Dále z maticového součinu platí, že $({G_n}^T G_n)_{i,j} = \boldsymbol{g}_i \cdot \boldsymbol{g}_j$, kde $\boldsymbol{g}_i$, $\boldsymbol{g}_j$ jsou i-tý a j-tý sloupec matice G_n.

Pokud $i = j$, pak $\boldsymbol{g}_i = \boldsymbol{g}_j$. Dále $\boldsymbol{g}_i$ má z definice matice incidence dvě složky rovny 1 (protože hrana obsahuje pouze dva vrcholy). Tedy z definice bodového součinu vyplývá, že $({G_n}^T G_n)_{i,j} = 2$.

Naopak pokud $i \neq j$, pak bereme dvě různé hrany. Ty mají společný buď jeden nebo žádný vrchol, tedy $\boldsymbol{g}_i \cdot \boldsymbol{g}_j \in \{0, 1\}$ (1 pokud mají společný jeden vrchol, 0 pokud žádný).

Pro M_n podle naší definice sousednosti hranového grafu platí, že $(M_n)_{i,j} = 1$ právě tehdy, když i-tý a j-tý vrchol grafu $L(Q_n)$ jsou sousedné, což je, když mají i-tá a j-tá hrana grafu Q_n společný vrchol a zároveň nejde o stejnou hranu. V opačném případě $(M_n)_{i,j} = 0$. Tedy pro $i \neq j$ dostáváme $(M_n)_{i,j} = ({G_n}^T G_n)_{i,j}$ a pro $i = j$ dostáváme $(M_n)_{i,j} = ({G_n}^T G_n)_{i,j} - 2$. Zbytek dokážeme z předchozího lemmatu a této rovnosti pomocí maticového násobení po blocích.

Máme tedy

$$M_n = {G_n}^T G_n - 2I_{2^{n-1}n} = \begin{pmatrix} {G_{n-1}}^T & 0 \\ I_{2^{n-1}} & I_{2^{n-1}} \\ 0 & {G_{n-1}}^T \end{pmatrix} \begin{pmatrix} G_{n-1} & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & G_{n-1} \end{pmatrix} - 2I_{2^{n-1}n} =$$

$$= \begin{pmatrix} {G_{n-1}}^T G_{n-1} & {G_{n-1}}^T & 0 \\ G_{n-1} & 2I_{2^{n-1}} & G_{n-1} \\ 0 & {G_{n-1}}^T & {G_{n-1}}^T G_{n-1} \end{pmatrix} - 2I_{2^{n-1}n} = \begin{pmatrix} M_{n-1} & {G_{n-1}}^T & 0 \\ G_{n-1} & 0 & G_{n-1} \\ 0 & {G_{n-1}}^T & M_{n-1} \end{pmatrix}.$$

□

2.2 Binární kódy

V této kapitole budeme konstruovat binární kódy pomocí grafů Q_n a $L(Q_n)$ a matic G_n a M_n z předchozí kapitoly. Nyní budeme uvažovat matice M_n a G_n jako matice s řádky generujícími binární kódy, tedy pouze nad $\mathbb{F}_2$, a tedy platí, že $M_n = {G_n}^T G_n$. Binární kód generovaný řádky matice M_n, tedy kód indukovaný grafem $L(Q_n)$, budeme značit $\mathcal{C}(M_n)$. Binární kód generovaný řádky matice G_n, tedy kód designu $\mathcal{G}_n$, budeme značit $\mathcal{C}(G_n)$.

Lemma 6. *Pro hodnost matice G_n, kde $n \geq 1$, platí, že* $\operatorname{rank}(G_n) = 2^n - 1$.

Důkaz. První rovnost dokážeme indukcí podle n. Pro $n = 1$ máme $G_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ tedy $\text{rank}(G_1) = 1$. Dále uvažujme, že rovnost platí pro $n-1$, a dokážeme, že platí i pro n. Vezmeme podobu matice dle lemmatu 3 a provedeme prohození bloků pomocí prohazování sloupců a následné vynulování pomocí ekvivalentní řádkové úpravy, přičítání řádků. Tedy

$$\begin{aligned}
&\text{rank}\left(\begin{pmatrix} G_{n-1} & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & G_{n-1} \end{pmatrix}\right) = \text{rank}\left(\begin{pmatrix} I_{2^{n-1}} & G_{n-1} & 0 \\ I_{2^{n-1}} & 0 & G_{n-1} \end{pmatrix}\right) = \\
&= \text{rank}\left(\begin{pmatrix} I_{2^{n-1}} & G_{n-1} & 0 \\ 0 & G_{n-1} & G_{n-1} \end{pmatrix}\right) = 2^{n-1} + \text{rank}\left(\begin{pmatrix} G_{n-1} & G_{n-1} \end{pmatrix}\right) = \\
&= 2^{n-1} + \text{rank}(G_{n-1}).
\end{aligned}$$

Dostáváme tedy, že $\text{rank}(G_n) = 2^{n-1} + \text{rank}(G_{n-1})$. z indukčního předpokladu pak dostáváme, že $\text{rank}(G_n) = 2^{n-1} + 2^{n-1} - 1 = 2^n - 1$.

□

Lemma 7. *Pro matici G_n a libovolný vektor $\boldsymbol{u} \in \mathbb{F}_2^{2^n}$ platí, že $\boldsymbol{u}G_n = \mathbf{0}$ právě tehdy, když $\boldsymbol{u} = \mathbf{0}$ nebo $\boldsymbol{u} = \mathbf{1}$.*

Důkaz. Matice G_n má dle předchozího lemmatu 6 hodnost $2^n - 1$, tedy platí, že $\dim(\text{Ker}(G_n)) = 1$. Navíc, protože je maticí incidence vrcholového grafu, jsou v každém sloupci právě dvě jedničky a zbytek jsou nuly a žádný řádek není nulový. Nulový vektor tedy dostaneme právě lineární kombinací všech jejích řádků nebo žádného řádku, proto $\boldsymbol{u}G_n = \mathbf{0}$ právě tehdy, když $\boldsymbol{u} = \mathbf{0}$ nebo $\boldsymbol{u} = \mathbf{1}$.

□

Lemma 8. *Matice M_n, kde $n \geq 2$, má hodnost* $\text{rank}(M_n) = 2^n - 2$. *Navíc platí, že $\mathcal{C}(M_n) \subseteq \mathcal{C}(G_n)$.*

Důkaz. Pro důkaz tohoto lemmatu nejprve zadefinujeme kód $\mathcal{C}({G_n}^T)$ generovaný řádky matice ${G_n}^T$ a také lineární zobrazení $\tau_n : \mathcal{C}({G_n}^T) \to \mathcal{C}(M_n)$, že pro každé $\boldsymbol{w} \in \mathcal{C}({G_n}^T)$ platí $\tau_n(\boldsymbol{w}) = \boldsymbol{w}G_n$. Z předchozího lemmatu 7 máme, že $\mathbf{1}G_n = \mathbf{0}$. Navíc G_n má 2^n řádků a $\text{rank}(G_n) = 2^n - 1$. Tedy pro τ_n pak platí, že $\text{Ker}(\tau_n) = \text{LO}\{\mathbf{1}\}$.

Dále si všimneme, že všechny řádky matice M_n jsou lineární kombinací řádků matice G_n, protože $M_n = {G_n}^T G_n$. Tedy $\text{rank}(M_n) \leq \text{rank}(G_n) = 2^n - 1$ a také $\mathcal{C}(M_n) \subseteq \mathcal{C}(G_n)$. Dále z toho vidíme, že $\text{Im}(\tau_n) = \mathcal{C}(M_n)$ neboli, že τ_n je surjektivní zobrazení.

Sečteme-li 2^{n-1} prostředních řádků matice ${G_n}^T$ dostaneme $\mathbf{1}$, tedy $\mathbf{1} \in \mathcal{C}({G_n}^T)$. Navíc $\dim(\mathcal{C}({G_n}^T)) = 2^n - 1$, protože $\text{rank}({G_n}^T) = \text{rank}(G_n) = 2^n - 1$. Tedy z $\text{Ker}(\tau_n) = \text{LO}\{\mathbf{1}\}$, $\mathbf{1} \in \mathcal{C}({G_n}^T)$ a $\text{Im}(\tau_n) = \mathcal{C}(M_n)$ dostáváme, že pro dimenzi kódu $\mathcal{C}(M_n)$ platí $\dim(\mathcal{C}(M_n)) = 2^n - 2$, tedy i $\text{rank}(M_n) = 2^n - 2$.

□

Lemma 9. *Kód $\mathcal{C}({G_n}^T)$ je kód sudé váhy.*

Důkaz. Toto tvrzení plyne přímo z toho, že G_n je maticí incidence grafu, tedy v každém sloupci jsou právě dvě jedničky a zbytek nuly. Proto každý řádek matice

${G_n}^T$ má váhu 2, tedy je sudé váhy. Každé slovo kódu $\mathcal{C}({G_n}^T)$ je tedy lineární kombinací slov sudé váhy a tedy opět slovo sudé váhy.

□

Nyní ukážeme, jaká je minimální váha nejprve kódu $\mathcal{C}(G_n)$ a poté kódu $\mathcal{C}(M_n)$. Na příkladu ukážeme princip důkazu následující věty a zároveň dokážeme větu pro $n = 1$, $n = 2$ a $n = 3$.

Příklad. Začneme od $n = 1$ s maticí G_1 a budeme postupně konstruovat matici G_2, kód $\mathcal{C}(G_2)$ a dále matici G_3 a kód $\mathcal{C}(G_3)$. Tedy pro $n = 1$ máme vrcholový graf:

Obrázek 2.1 Vrcholový graf 1-dimenzionální krychle

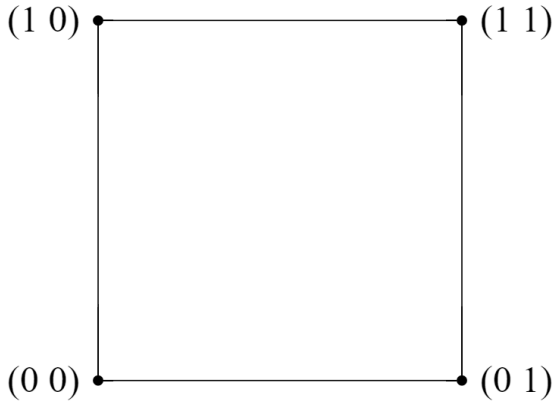
Není těžké nahlédnout, že:

$$G_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

a

$$\mathcal{C}(G_1) = \left\{ \begin{pmatrix} 1 \end{pmatrix}, \begin{pmatrix} 0 \end{pmatrix} \right\}.$$

Pro $n = 2$ máme vrcholový graf:



Obrázek 2.2 Vrcholový graf 2-dimenzionální krychle

Z něj pak dostáváme:

$$G_2 = \left(\begin{array}{c|cc|c} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Na matici můžeme vidět platnost lemmatu 3. Zde ještě můžeme lehce vypsat všechny kódová slova a nahlédnout, že minimální vzdálenost kódu je opravdu 2, tedy n.

$$\mathcal{C}(G_2) = \left\{ \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \right\}$$

Nakonec pro $n = 3$ napíšeme matici pomocí lemmatu 3, nebo opět můžeme zkonstruovat z definice pomocí grafu z obrázku 1.1.

$$G_3 = \begin{pmatrix} G_2 & I_4 & \mathrm{o} \\ \mathrm{o} & I_4 & G_2 \end{pmatrix} = \left(\begin{array}{cccc|cccc|cccc} 1&1&0&0 & 1&0&0&0 & 0&0&0&0 \\ 1&0&1&0 & 0&1&0&0 & 0&0&0&0 \\ 0&1&0&1 & 0&0&1&0 & 0&0&0&0 \\ 0&0&1&1 & 0&0&0&1 & 0&0&0&0 \\ \hline 0&0&0&0 & 1&0&0&0 & 1&1&0&0 \\ 0&0&0&0 & 0&1&0&0 & 1&0&1&0 \\ 0&0&0&0 & 0&0&1&0 & 0&1&0&1 \\ 0&0&0&0 & 0&0&0&1 & 0&0&1&1 \end{array}\right).$$

U tohoto případu už vidíme, že by bylo nepraktické vypsat všechna kódová slova, protože bychom jich měli 128.

Ukážeme, že minimální váha kódových slov kódu $\mathcal{C}(G_3)$ je 3, a že slova s minimální vahou jsou právě řádky matice G_3. Slovo $\boldsymbol{v} \in \mathcal{C}(G_3)$ budeme brát jako konkatenaci vektorů $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ a $\boldsymbol{v}_3$, tedy $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$, kde $\boldsymbol{v}_1$ jsou první čtyři souřadnice vektoru $\boldsymbol{v}$, $\boldsymbol{v}_2$ druhé čtyři a $\boldsymbol{v}_3$ poslední čtyři souřadnice.

1) Nejprve uvažujeme, že $\boldsymbol{v}$ je lineární kombinací $k \in \{1, 2, 3, 4\}$ řádků z prvních čtyř řádků matice G_3. Pak $\boldsymbol{v}_1 \in \mathcal{C}(G_2)$, tedy $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ nebo $\boldsymbol{v}_1 = \boldsymbol{0}$. Z matice dále vidíme, že $\mathrm{w}(\boldsymbol{v}_2) \geq 1$ a $\boldsymbol{v}_3 = \boldsymbol{0}$. Pokud $\boldsymbol{v}_1 = \boldsymbol{0}$, pak je vidět, že jsme udělali lineární kombinaci všech čtyř řádků, $\boldsymbol{v}_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$, tedy $\mathrm{w}(\boldsymbol{v}) = 4$. Naopak pokud $\boldsymbol{v}_1 \neq \boldsymbol{0}$, pak $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ a tedy $\mathrm{w}(\boldsymbol{v}) \geq 3$. Navíc pokud chceme, aby $\mathrm{w}(\boldsymbol{v}) = 3$, pak musí být $\mathrm{w}(\boldsymbol{v}_1) = 2$ a hlavně $\mathrm{w}(\boldsymbol{v}_2) = 1$, tedy je jasné, že to musí být řádek G_3.

2) Pokud $\boldsymbol{v}$ je lineární kombinací $k \in \{1, 2, 3, 4\}$ řádků z posledních čtyř řádků matice G_3, pak můžeme postupovat stejně, akorát nyní je $\boldsymbol{v}_3 \in \mathcal{C}(G_2)$ a $\boldsymbol{v}_1 = \boldsymbol{0}$.

3) Nakonec předpokládejme, že $\boldsymbol{v}$ je lineární kombinací $k \in \{1, 2, 3, 4\}$ řádků z prvních čtyř řádků matice G_3 a $l \in \{1, 2, 3, 4\}$ řádků z druhých čtyř řádků této matice. Pak platí $\boldsymbol{v}_1 \in \mathcal{C}(G_2)$ i $\boldsymbol{v}_3 \in \mathcal{C}(G_2)$.

Pokud $\boldsymbol{v}_1 \neq \boldsymbol{0}$ a zároveň $\boldsymbol{v}_3 \neq 0$, pak $\mathrm{w}(\boldsymbol{v}) \geq 4$, protože $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ i $\mathrm{w}(\boldsymbol{v}_3) \geq 2$. Naopak pokud $\boldsymbol{v}_1 = \boldsymbol{0}$ a zároveň $\boldsymbol{v}_3 = 0$, pak $\boldsymbol{v}_2 = \boldsymbol{1} + \boldsymbol{1} = \boldsymbol{0}$.

Nakonec jestliže $\boldsymbol{v}_1 = \boldsymbol{0}$ a $\boldsymbol{v}_3 \neq 0$ (respektive $\boldsymbol{v}_1 \neq \boldsymbol{0}$ a $\boldsymbol{v}_3 = 0$), pak $\boldsymbol{v}_2 \neq \boldsymbol{0}$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 3$. Pokud $\mathrm{w}(\boldsymbol{v}) = 3$, pak musí být $\mathrm{w}(\boldsymbol{v}_2) = 1$ a $\mathrm{w}(\boldsymbol{v}_2) = 2$, a protože $\boldsymbol{v}_1 = \boldsymbol{0}$, je $\boldsymbol{v}$ lineární kombinací určitě prvních čtyř řádků, tedy abychom dostali $\mathrm{w}(\boldsymbol{v}_2) = 1$ musíme do lineární kombinace přidat ještě další tři řádky z druhé poloviny matice. Ale $\boldsymbol{v}_3$ je pak lineární kombinací tří řádků z G_2, což je ovšem ten zbylý řádek této matice (protože hodnost matice je 3). Navíc $\boldsymbol{v}_2$ je jednotkový vektor s jedničkou na pozici i, kde i je řádek vynechaný pro lineární kombinaci. Tedy opět dostáváme, že $\boldsymbol{v}$ je řádkem matice G_3.

Věta 10. *Pro minimální vzdálenost kódu $\mathcal{C}(G_n)$, kde $n \geq 1$, platí, že $d(\mathcal{C}(G_n)) = n$. Tedy $\mathcal{C}(G_n)$ je $[2^{n-1}n, 2^n - 1, n]_2$ kód. Navíc pro $n \geq 3$ jsou minimální slova kódu $\mathcal{C}(G_n)$ právě řádky matice G_n.*

Důkaz. Dimenzi kódu $\mathcal{C}(G_n)$ máme dokázanou v předchozím lemmatu 6. Stačí tedy dokázat minimální vzdálenost, kterou dokážeme indukcí podle n.

Pro $n = 1$, $n = 2$ tvrzení o minimální váze kódu platí (dle předchozího příkladu), navíc vidíme, že řádky matic mají minimální váhu. Pro $n = 3$ navíc platí i to, že v řádky G_3 jsou slova s minimální vahou kódu $\mathcal{C}(G_3)$ (opět viz

příklad výše). Předpokládejme, že tvrzení platí pro $n-1$. Pomocí lemmatu 3 dokážeme, že tvrzení pak platí i pro n. Označíme řádky matice G_{n-1} jako vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{2^{n-1}}$. Dále budeme brát každé slovo $\boldsymbol{v} \in (\mathcal{C}(G_n)$ jako konkatenaci vektorů $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$, kde $\boldsymbol{v}_1$ je tvořen prvními $2^{n-2}(n-1)$ souřadnicemi vektoru $\boldsymbol{v}$, $\boldsymbol{v}_2$ je tvořen dalšími 2^{n-1} souřadnicemi $\boldsymbol{v}$ a $\boldsymbol{v}_3$ je tvořen zbylými $2^{n-2}(n-1)$ souřadnicemi $\boldsymbol{v}$.

Z podoby matice G_n vidíme, že její řádky mají váhu o jedna větší než řádky matice G_{n-1}, tedy dle indukčního předpokladu mají váhu n. Pokud uvažujeme, že minimální váha kódu $\mathcal{C}(G_n)$ je n, pak mají řádky matice G_n minimální váhu. Následujícím způsobem ukážeme zbytek tvrzení.

1) Nejprve uvažujme, že $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ vektorů z množiny prvních 2^{n-1} řádků matice G_n. Označme $I \subseteq \{1, \ldots, 2^{n-1}\}$ množinu indexů řádků matice G_n tvořících vektor $\boldsymbol{v}$, tedy $|I| = k \geq 1$. Pak z lemmatu 3 o podobě matice G_n máme $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{u}_i$, $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{e}_i$ a $\boldsymbol{v}_3 = \boldsymbol{0}$. Mohou nastat dvě možnosti. Pokud $\boldsymbol{v}_1 \neq \boldsymbol{0}$, pak z indukčního předpokladu $\mathrm{w}(\boldsymbol{v}_1) \geq n-1$, dále $\mathrm{w}(\boldsymbol{v}_2) = k$, a tedy $\mathrm{w}(\boldsymbol{v}) \geq n-1+k \geq n$. Navíc $\mathrm{w}(\boldsymbol{v}) = n$ právě tehdy, když $k = 1$, tedy když $\boldsymbol{v}$ je právě řádek G_n. Naopak pokud $\boldsymbol{v}_1 = \boldsymbol{0}$, pak dle lemmatu 7 $\boldsymbol{v}_1 = \sum_{i=1}^{2^{n-1}} \boldsymbol{u}_i$. Proto $k = 2^{n-1}$, a tedy $\boldsymbol{v}_2 = \boldsymbol{1}$. Dostáváme tak, že $\mathrm{w}(\boldsymbol{v}) = 2^{n-1} > n$ pro $n \geq 3$.

2) Pokud je $\boldsymbol{v}$ lineární kombinací $k \geq 1$ vektorů z množiny zbylých 2^{n-1} řádků matice G_n, pak pro $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$ platí, že $\boldsymbol{v}_1 = \boldsymbol{0}$, $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{e}_i$ a $\boldsymbol{v}_3 = \sum_{i \in I} \boldsymbol{u}_i$. Tedy můžeme použít stejné argumenty jako u předchozí části důkazu.

3) Nyní uvažujme, že je $\boldsymbol{v}$ lineární kombinací $k \geq 1$ vektorů z množiny prvních 2^{n-1} řádků matice G_n a $l \geq 1$ vektorů z množiny zbylých 2^{n-1} řádků matice G_n. Tady označme množiny indexů $I \subseteq \{1, \ldots, 2^{n-1}\}$ a $J \subseteq \{1, \ldots, 2^{n-1}\}$, že $|I| = k \geq 1$ a $|J| = l \geq 1$. Pak opět z lemmatu 3 dostáváme, že $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{u}_i$, $\boldsymbol{v}_3 = \sum_{j \in J} \boldsymbol{u}_j$ a $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{e}_i + \sum_{j \in J} \boldsymbol{e}_j$. Opět rozebereme jednotlivé možnosti.

Nejdříve uvažujme, že $\boldsymbol{v}_1 = \boldsymbol{0}$ a $\boldsymbol{v}_3 = \boldsymbol{0}$, tedy $k = 2^{n-1}$ a $l = 2^{n-1}$. Pak ale i $\boldsymbol{v}_2 = \boldsymbol{0}$, tedy $\boldsymbol{v} = \boldsymbol{0}$. Dále uvažujme, že $\boldsymbol{v}_1 \neq \boldsymbol{0}$ a $\boldsymbol{v}_3 \neq \boldsymbol{0}$. Pak z indukčního předpokladu máme, že $\mathrm{w}(\boldsymbol{v}_1) \geq n-1$ a zároveň $\mathrm{w}(\boldsymbol{v}_3) \geq n-1$, tedy platí $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1)$. Tedy pro $n \geq 3$ platí, že $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1) > n$.

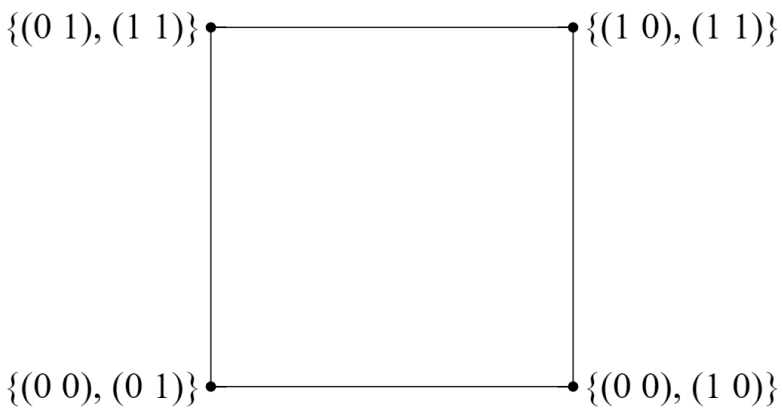
Nakonec uvažujme, že $\boldsymbol{v}_1 = \boldsymbol{0}$ a $\boldsymbol{v}_3 \neq \boldsymbol{0}$. Pak $k = 2^{n-1}$ a $l < 2^{n-1}$. Dále $\boldsymbol{v}_2 = \boldsymbol{1} + \sum_{j \in J} \boldsymbol{e}_j$, a protože $l < 2^{n-1}$, pak $\boldsymbol{v}_2 \neq \boldsymbol{0}$. Tedy platí, že $\mathrm{w}(\boldsymbol{v}_2) \geq 1$. Dále z indukčního předpokladu pro $\boldsymbol{v}_3$ platí, že $\mathrm{w}(\boldsymbol{v}_3) \geq n-1$, tedy dostáváme, že $\mathrm{w}(\boldsymbol{v}) \geq n$. Z předchozího také dostáváme, že $\mathrm{w}(\boldsymbol{v}) = n$ právě tehdy, když $\mathrm{w}(\boldsymbol{v}_3) = n-1$ a zároveň $\mathrm{w}(\boldsymbol{v}_2) = 1$. Víme, že $\mathrm{w}(\boldsymbol{v}_2) = 1$, když $l = 2^{n-1} - 1$. Tedy $\boldsymbol{v}$ je lineární kombinací $2^n - 1$ řádků matice G_n, z lemmatu 7 tedy plyne, že $\boldsymbol{v}$ je řádek matice G_n (ten řádek, který nebyl zahrnut do lineární kombinace). Pro $\boldsymbol{v}_1 \neq \boldsymbol{0}$ a $\boldsymbol{v}_3 = \boldsymbol{0}$ provedeme důkaz identicky.

Dostáváme tedy, že minimální vzdálenost kódu $\mathcal{C}(G_n)$ je $d(\mathcal{C}(G_n)) = n$ (pro $n \geq 1$). Máme tedy, že $\mathcal{C}(G_n)$ je $[2^{n-1}n, 2^{n-1}, n]_2$ kód a pro $n \geq 3$ jsou minimální slova v řádcích matice G_n.

□

Nyní ukážeme minimální vzdálenost kódu $\mathcal{C}(M_n)$, ale před tím opět předvedeme princip důkazu na příkladu pro $n = 2$ a $n = 3$.

Příklad. Nejprve najdeme minimální váhu kódu $\mathcal{C}(M_n)$ pro $n = 2$. Pro $n = 2$ máme graf $L(Q_2)$:



Obrázek 2.3 Hranový graf 2-dimenzionální krychle

A jeho matici sousednosti M_2:

$$M_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Pomocí této matice najdeme celý kód :

$$\mathcal{C}(M_2) = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \right\}.$$

Z toho vidíme, že minimální váha kódu $\mathcal{C}(M_2)$ je 2, tedy $2(n-1)$. Zde dokonce platí, že minimální slova jsou v řádcích matice M_2. Zajímavostí pro $n = 2$ je, že $G_2 = G_2^T$, tedy i $\mathcal{C}(G_2) = \mathcal{C}(G_2)^T$. To využijeme pro $n = 3$.

Pro $n = 3$ máme graf $L(Q_3)$ na obrázku 1.2 a jeho matice sousednosti vypadá následovně:

$$M_3 = \begin{pmatrix} M_2 & {G_2}^T & 0 \\ G_2 & 0 & G_2 \\ 0 & {G_2}^T & M_2 \end{pmatrix} = \left(\begin{array}{cccc|cccc|cccc} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right).$$

Opět bychom mohli vypsat všechna kódová slova, kterých je ovšem 64. Místo toho rozebereme jednotlivé možnosti podobně jako v důkazu následující věty.

Označíme množinu prvních 4 řádků matice M_3 jako R_1, druhých 4 jako R_2 a posledních 4 jako R_3. Slovo $\boldsymbol{v} \in \mathcal{C}(M_3)$ je tedy lineární kombinací řádků matice M_3 a budeme ho zapisovat jako konkatenaci vektorů $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ a $\boldsymbol{v}_3$, kde $\boldsymbol{v}_1$ jsou první 4 složky vektoru $\boldsymbol{v}$, $\boldsymbol{v}_2$ druhé 4 a $\boldsymbol{v}_3$ poslední 4 složky. Máme tedy $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$.

1) Uvažujme, že $\boldsymbol{v}$ je lineární kombinací řádků z R_1. Pak z matice vidíme, že pokud $\boldsymbol{v}_1 = \mathbf{0}$, pak $\boldsymbol{v}_2 = \mathbf{0}$ nebo $\boldsymbol{v}_2 = \mathbf{1}$. Pokud $\boldsymbol{v}_2 = \mathbf{0}$, pak i $\boldsymbol{v} = \mathbf{0}$. Naopak pokud $\boldsymbol{v}_2 = \mathbf{1}$, pak $\mathrm{w}(\boldsymbol{v}) = 4 = 2(n-1)$. Navíc vidíme, že je to minimální slovo, které není v řádku matice M_3, tedy zde neplatí, že by byla minimální slova řádky matice M_3. Pokud $\boldsymbol{v}_1 \neq \mathbf{0}$ z toho, že známe $\mathcal{C}(M_2)$ a $\mathcal{C}(G_2)$, vidíme, že $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_2) \geq 2$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$.

2) Pokud je $\boldsymbol{v}$ lineární kombinací řádků z R_3, pak můžeme brát stejný postup jako u kroku 1) akorát máme prohozeny vektory $\boldsymbol{v}_1$ a $\boldsymbol{v}_3$.

3) Uvažujeme-li, že je $\boldsymbol{v}$ je lineární kombinací řádků z R_2, pak vidíme, že platí $\boldsymbol{v}_1 = \boldsymbol{v}_3$. Tedy $\boldsymbol{v}_1 = \mathbf{0}$ právě, když $\boldsymbol{v}_3 = \mathbf{0}$. Pak ale i $\boldsymbol{v} = \mathbf{0}$. Pokud $\boldsymbol{v}_1 = \boldsymbol{v}_3 \neq \mathbf{0}$, pak opět ze znalosti $\mathcal{C}(G_2)$, $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$.

4) Je-li $\boldsymbol{v}$ je lineární kombinací řádků z R_1 a R_2, pak pokud $\boldsymbol{v}_3 = \mathbf{0}$ dostáváme případ 1) a pokud $\boldsymbol{v}_2 = \mathbf{0}$ dostáváme případ 3). Pokud ovšem $\boldsymbol{v}_2 \neq \mathbf{0}$ a $\boldsymbol{v}_3 \neq \mathbf{0}$, pak $\mathrm{w}(\boldsymbol{v}_2) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$.

5) Je-li $\boldsymbol{v}$ je lineární kombinací řádků z R_2 a R_3, pak můžeme použít stejné argumenty jako u případu 4).

6) Uvažujme nyní, že $\boldsymbol{v}$ je lineární kombinací řádků z R_1 a R_3. Pokud $\boldsymbol{v}_1 = \mathbf{0}$ a $\boldsymbol{v}_3 = \mathbf{0}$, pak i $\boldsymbol{v}_2 = \mathbf{0}$. Pokud $\boldsymbol{v}_1 = \mathbf{0}$ a $\boldsymbol{v}_3 \neq \mathbf{0}$, pak $\boldsymbol{v}_2 \neq \mathbf{0}$ a ze znalosti $\mathcal{C}(M_2)$ a $\mathcal{C}(G_2)$ máme, že $\mathrm{w}(\boldsymbol{v}_2) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$. Pro $\boldsymbol{v}_3 = \mathbf{0}$ a $\boldsymbol{v}_1 \neq \mathbf{0}$ platí to samé. Nakonec pokud $\boldsymbol{v}_1 \neq \mathbf{0}$ a $\boldsymbol{v}_3 \neq \mathbf{0}$, pak opět $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$.

7) Nakonec předpokládejme, že je $\boldsymbol{v}$ lineární kombinací řádků z R_1, R_2 i R_3. Pokud $\boldsymbol{v}_1 \neq \mathbf{0}$ a $\boldsymbol{v}_3 \neq \mathbf{0}$, pak $\mathrm{w}(\boldsymbol{v}_1) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$. To platí, protože $\mathcal{C}(M_2) \subset \mathcal{C}(G_2)$ (vidíme, že řádky M_2 jsou lineární kombinací řádků G_2). Pokud $\boldsymbol{v}_1 = \mathbf{0}$ a $\boldsymbol{v}_3 = \mathbf{0}$, pak $\boldsymbol{v}_2 = \mathbf{0}$ nebo $\boldsymbol{v}_2 = \mathbf{1}$, tedy $\boldsymbol{v} = \mathbf{0}$, nebo $\mathrm{w}(\boldsymbol{v}_2) \geq 4$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 4$. Pokud $\boldsymbol{v}_1 = \mathbf{0}$ a $\boldsymbol{v}_3 \neq \mathbf{0}$, pak i $\boldsymbol{v}_2 \neq \mathbf{0}$, tedy $\mathrm{w}(\boldsymbol{v}_2) \geq 2$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2$, a proto $\mathrm{w}(\boldsymbol{v}) \geq 4$. Obdobně pokud $\boldsymbol{v}_1 \neq \mathbf{0}$ a $\boldsymbol{v}_3 = \mathbf{0}$. Tedy minimální váha $\mathcal{C}(M_3)$ je 4.

Věta 11. *Pro $n \geq 2$ je minimální vzdálenost kódu $\mathcal{C}(M_n)$ rovna $2(n-1)$, neboli $d(\mathcal{C}(M_n)) = 2(n-1)$. Tedy $\mathcal{C}(M_n)$ je $[2^{n-1}n, 2^n - 2, 2(n-1)]_2$ kód. Navíc pro $n \geq 4$ jsou minimální slova $\mathcal{C}(M_n)$ právě řádky matice M_n.*

Důkaz. Větu dokážeme opět indukcí podle n. Pro $n = 2$ a $n = 3$ máme větu dokázanou v příkladu výše. Pro $n = 4$ dokážeme tvrzení o minimálních slovech pomocí Programu 1, který hrubou silou najde všechna kódová slova minimální váhy.

Už pro $n = 2$ na příkladu vidíme, že řádky matice mají minimální váhu. Uvažujeme, že řádky matice M_{n-1} mají minimální váhu, tedy $2(n-2)$, a uvažujme, že minimální váha kódu $\mathcal{C}(M_n)$ je $2(n-2)$. Pak z podoby matice M_n vidíme, že řádky této matice mají hodnost $2(n-2)+2$ nebo $(n-1)+(n-1)$, tedy $2(n-1)$, neboli řádky mají minimální váhu.

Nyní předpokládejme, že tvrzení platí pro $n-1$ a dokážeme ho pro n. Tedy minimální slova kódu $\mathcal{C}(M_{n-1})$ jsou řádky matice M_{n-1} a $d(\mathcal{C}(M_{n-1})) = 2(n-2)$. Libovolné slovo $\boldsymbol{v} \in \mathcal{C}(M_{n-1})$ je lineární kombinací řádků matice M_{n-1} a zapíšeme ho jako konkatenaci vektorů $\boldsymbol{v}_1, \boldsymbol{v}_2$ a $\boldsymbol{v}_3$, tedy $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$. Řádky matice M_{n-1} rozdělíme také na tři bloky (do tří podmnožin) R_1, R_2 a R_3, kde R_1 je prvních $2^{n-2}(n-1)$ řádků, R_2 je dalších 2^{n-1} řádků a R_3 je zbylých $2^{n-2}(n-1)$ řádků matice M_n. Dále označíme i-tý řádek matice G_{n-1}^T jako $\boldsymbol{q}_i$, i-tý řádek matice

G_{n-1} jako $\boldsymbol{g}_i$ a i-tý řádek matice M_{n-1} jako $\boldsymbol{m}_i$. Navíc $\boldsymbol{m}_i = \boldsymbol{q}_i G_{n-1}$, protože $M_{n-1} = {G_{n-1}}^T G_{n-1}$. Nyní opět rozebereme všechny možné případy.

1) Nejdříve uvažujme, že $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ řádků z R_1, a označme $I \subseteq \{1, \cdots, 2^{n-2}(n-1)\}$ množinu indexů těchto řádků, pak $|I| = k$. Pro $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$, pak platí $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{m}_i$, $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{q}_i$ a $\boldsymbol{v}_3 = \boldsymbol{0}$. Navíc platí, že $\boldsymbol{v}_1 = (\sum_{i \in I} \boldsymbol{q}_i) G_{n-1} = \boldsymbol{v}_2 G_{n-1}$, protože $\boldsymbol{m}_i = \boldsymbol{q}_i G_{n-1}$. Nejprve, ať $\boldsymbol{v}_1 \neq \boldsymbol{0}$, pak i $\boldsymbol{v}_2 \neq \boldsymbol{0}$. Z indukčního předpokladu máme, že $\mathrm{w}(\boldsymbol{v}_1) \geq 2(n-2)$ a z lemmatu 9 plyne, že $\mathrm{w}(\boldsymbol{v}_2) \geq 2$. Dostáváme tak $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1)$. Navíc uvažujme, že $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, pak $\mathrm{w}(\boldsymbol{v}_1) = 2(n-2)$ a $\mathrm{w}(\boldsymbol{v}_2) = 2$. Z indukčního předpokladu platí, že $\boldsymbol{v}_1 = \boldsymbol{m}_n$ pro nějaké $n \in \{1, \cdots, 2^{n-2}(n-1)\}$, tedy $\boldsymbol{v}_2 G_{n-1} = \boldsymbol{v}_1 = \boldsymbol{m}_n$. Zároveň platí, že $\boldsymbol{m}_n = \boldsymbol{q}_n G_{n-1}$, tedy $(\boldsymbol{v}_2 + \boldsymbol{q}_n) G_{n-1} = \boldsymbol{0}$. Z lemmatu 7 dostáváme, že $\boldsymbol{v}_2 + \boldsymbol{q}_n = \boldsymbol{0}$ nebo $\boldsymbol{v}_2 + \boldsymbol{q}_n = \boldsymbol{1}$. Ale víme, že $\boldsymbol{v}_2$ i $\boldsymbol{q}_n$ mají mít váhu 2, tedy $\boldsymbol{v}_2 + \boldsymbol{q}_n = \boldsymbol{0}$, neboli $\boldsymbol{v}_2 = \boldsymbol{q}_n$. Z toho dostáváme, že $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$ právě, když $\boldsymbol{v}$ je řádek M_n. Dále pokud $\boldsymbol{v}_1 = \boldsymbol{0}$, pak z rovnosti $\boldsymbol{v}_2 G_{n-1} = \boldsymbol{v}_1$ dostaneme $\boldsymbol{v}_2 G_{n-1} = \boldsymbol{0}$. Tedy dle lemmatu 7 $\boldsymbol{v}_2 = \boldsymbol{0}$ nebo $\boldsymbol{v}_2 = \boldsymbol{1}$. Jestliže $\boldsymbol{v}_2 = \boldsymbol{0}$, pak $\boldsymbol{v} = \boldsymbol{0}$, jestliže $\boldsymbol{v}_2 = \boldsymbol{1}$, pak $\mathrm{w}(\boldsymbol{v}) = 2^{n-1} > 2(n-1)$, pro $n \geq 4$.

2) Pokud uvažujeme, že $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ řádků z R_3, pak pro $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$ platí, že $\boldsymbol{v}_1 = \boldsymbol{0}$, $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{q}_i$ a $\boldsymbol{v}_3 = \sum_{i \in I} \boldsymbol{m}_i$. Tedy můžeme použít stejné argumenty jako u předchozího případu, tedy v části 1).

3) Dále uvažujme, že $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ řádků z R_2. Pak pro $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$ platí, že $\boldsymbol{v}_1 = \boldsymbol{v}_3 = \sum_{i \in I} \boldsymbol{g}_i$, $\boldsymbol{v}_2 = \boldsymbol{0}$. Z věty 10 pak dostáváme, že $\mathrm{w}(\boldsymbol{v}_1) = \mathrm{w}(\boldsymbol{v}_2) \geq n-1$ a zároveň $\mathrm{w}(\boldsymbol{v}_1) = \mathrm{w}(\boldsymbol{v}_2) = n-1$ právě tehdy, když $\boldsymbol{v}_1 = \boldsymbol{v}_3 = \boldsymbol{g}_m$. Z toho dostáváme, že $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1)$ a $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$ právě, když $\boldsymbol{v}$ je řádek matice M_n.

4) Dále předpokládejme, že $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ řádků z R_1 a $l \geq 1$ řádků z R_2. Pro $I \subseteq \{1, \cdots, 2^{n-2}(n-1)\}$, $|I| = k$, a $J \subseteq \{1, \cdots, 2^{n-1}\}$, $|J| = l$, pak $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{m}_i + \sum_{j \in J} \boldsymbol{g}_j$, $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{q}_i$ a $\boldsymbol{v}_3 = \sum_{j \in J} \boldsymbol{g}_j$. Pokud $\sum_{j \in J} \boldsymbol{g}_j = \boldsymbol{0}$ dostaneme $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{m}_i$, $\boldsymbol{v}_3 = \boldsymbol{0}$ a tedy první případ. Tedy dále uvažujme, že $\sum_{j \in J} \boldsymbol{g}_j \neq \boldsymbol{0}$. Nyní pokud $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{q}_i = \boldsymbol{0}$, pak i $\sum_{i \in I} \boldsymbol{m}_i = \boldsymbol{0}$, protože $\sum_{i \in I} \boldsymbol{m}_i = \sum_{i \in I} \boldsymbol{q}_i G_{n-1}$ a tím dostáváme třetí možnost. Uvažujme tedy, že $\boldsymbol{v}_3 = \sum_{j \in J} \boldsymbol{g}_j \neq \boldsymbol{0}$ a $\boldsymbol{v}_2 \neq \boldsymbol{0}$. Pak platí $\mathrm{w}(\boldsymbol{v}_2) \geq 2$. Jestliže $\boldsymbol{v}_1 \neq \boldsymbol{0}$, pak z věty 10 $\mathrm{w}(\boldsymbol{v}_1) \geq n-1$, protože $\mathcal{C}(M_n) \subseteq \mathcal{C}(G_n)$, tedy $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{m}_i + \sum_{j \in J} \boldsymbol{g}_j \in \mathcal{C}(G_n)$. Dostáváme tak $\mathrm{w}(\boldsymbol{v}) \geq n-1+2+n-1 = 2n > 2(n-1)$. Na druhou stranu, pokud $\boldsymbol{v}_1 = \boldsymbol{0}$, pak $\sum_{i \in I} \boldsymbol{m}_i = \sum_{j \in J} \boldsymbol{g}_j \in \mathcal{C}(M_{n-1})$, tedy $\mathrm{w}(\boldsymbol{v}_3) \geq 2(n-2)$. Protože $\mathrm{w}(\boldsymbol{v}_2) \geq 2$, dostáváme, že $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1)$. Navíc pokud by $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, pak musí být $\mathrm{w}(\boldsymbol{v}_3) = 2(n-2)$ a $\mathrm{w}(\boldsymbol{v}_2) = 2$, tedy platí $\boldsymbol{v}_3 = \sum_{j \in J} \boldsymbol{g}_j = \sum_{i \in I} \boldsymbol{m}_i = \boldsymbol{m}_n$ pro nějaké $n \in I$ dle indukčního předpokladu. Navíc $\sum_{i \in I} \boldsymbol{q}_i G_{n-1} = \sum_{i \in I} \boldsymbol{m}_i = \boldsymbol{m}_n = \boldsymbol{q}_n G_{n-1}$, tedy $(\sum_{i \in I} \boldsymbol{q}_i + \boldsymbol{q}_n) G_{n-1} = \boldsymbol{0}$. Ale my chceme, aby $\mathrm{w}(\boldsymbol{v}_3) = 2$, tedy $\sum_{i \in I} \boldsymbol{q}_i + \boldsymbol{q}_n = \boldsymbol{0}$ a tedy $\boldsymbol{v}_3 = \boldsymbol{q}_n$. To nám tedy opět dává, že pokud $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, pak $\boldsymbol{v}$ je řádkem matice M_n.

5)Pokud $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ řádků z R_3 a $l \geq 1$ řádků z R_2, můžeme použít stejné argumenty jako u předchozí části důkazu.

6) Předpokládejme, že $\boldsymbol{v}$ je lineární kombinací $k \geq 1$ řádků z R_1 a $l \geq 1$ řádků z R_3. Pro $I \subseteq \{1, \cdots, 2^{n-2}(n-1)\}$, $|I| = k$, a $J \subseteq \{1, \cdots, 2^{n-2}(n-1)\}$, $|J| = l$, pak $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{m}_i$, $\boldsymbol{v}_2 = \sum_{i \in I} \boldsymbol{q}_i + \sum_{j \in J} \boldsymbol{q}_j$ a $\boldsymbol{v}_3 = \sum_{j \in J} \boldsymbol{m}_j$. Nejprve uvažujeme, že $\boldsymbol{v}_1 \neq \boldsymbol{0}$ a $\boldsymbol{v}_3 \neq \boldsymbol{0}$, pak z indukčního předpokladu dostáváme $\mathrm{w}(\boldsymbol{v}_1) \geq 2(n-2)$ a $\mathrm{w}(\boldsymbol{v}_3) \geq 2(n-2)$, a tedy $\mathrm{w}(\boldsymbol{v}) \geq 4(n-2) > 2(n-1)$ pro $n \geq 4$. Dále uvažujme, že $\boldsymbol{v}_1 = \boldsymbol{0}$. Dostáváme z lemmatu 7, že $\sum_{i \in I} \boldsymbol{q}_i = \boldsymbol{1}$, protože $\boldsymbol{v}_1 = \sum_{i \in I} \boldsymbol{q}_i G_{n-1}$

a kdyby $\sum_{i\in I} \boldsymbol{q}_i = \boldsymbol{0}$, dostáváme třetí případ. Pokud by $\boldsymbol{v}_2 = \boldsymbol{0}$, pak $\sum_{j\in J} \boldsymbol{q}_j = \boldsymbol{1}$ a tedy i $\boldsymbol{v}_3 = \boldsymbol{0}$. Také pokud $\boldsymbol{v}_1 = \boldsymbol{0}$ a $\boldsymbol{v}_3 = \boldsymbol{0}$, pak $\boldsymbol{v}_2 = \boldsymbol{0}$. Tedy ať $\boldsymbol{v}_3 \neq \boldsymbol{0}$, potom $\boldsymbol{v}_2 \neq \boldsymbol{0}$. Pak tedy z indukčního předpokladu a lemmatu 9 platí, že $\mathrm{w}(\boldsymbol{v}) \geq 2(n-2)+2 = 2(n-1)$. Pokud $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, pak musí být $\mathrm{w}(\boldsymbol{v}_3) = 2(n-2)$, tedy z indukčního předpokladu $\boldsymbol{v}_3 = \boldsymbol{m}_t = \boldsymbol{q}_t G_{n-1} = \sum_{j\in J} \boldsymbol{q}_j G_{n-1}$ pro nějaké $t \in \{1, \cdots, 2^{n-2}(n-1)\}$. Opět díky tomu a lemmatu 7 dostáváme $\sum_{j\in J} \boldsymbol{q}_j + \boldsymbol{q}_t = \boldsymbol{0}$ nebo $\sum_{j\in J} \boldsymbol{q}_j + \boldsymbol{q}_t = \boldsymbol{1}$. Ale chceme, že $\mathrm{w}(\boldsymbol{v}_2) = 2$, a $\boldsymbol{v}_2 = \boldsymbol{1} + \sum_{j\in J} \boldsymbol{q}_j$, tedy lze jen $\sum_{j\in J} \boldsymbol{q}_j + \boldsymbol{q}_t = \boldsymbol{1}$, a tak $\boldsymbol{v}_2 = \boldsymbol{q}_t$. Z toho dostáváme, že $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, když $\boldsymbol{v}_3 = \boldsymbol{m}_t$ a $\boldsymbol{v}_2 = \boldsymbol{q}_t$, tedy když $\boldsymbol{v}$ je řádek M_n. Pro $\boldsymbol{v}_3 = \boldsymbol{0}$ provedeme důkaz obdobně.

7) Nakonec předpokládejme, že $\boldsymbol{v}$ je lineární kombinací $r \geq 1$ řádků z R_1, $s \geq 1$ řádků z R_2 a $t \geq 1$ řádků z R_3. Pak pro $I \subseteq \{1, \cdots, 2^{n-2}(n-1)\}$, $|I| = r$, $J \subseteq \{1, \cdots, 2^{n-1}\}$, $|J| = s$, a $K \subseteq \{1, \cdots, 2^{n-2}(n-1)\}$, $|K| = t$ a pro $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 \end{pmatrix}$ platí $\boldsymbol{v}_1 = \sum_{i\in I} \boldsymbol{m}_i + \sum_{j\in J} \boldsymbol{g}_j$, $\boldsymbol{v}_2 = \sum_{i\in I} \boldsymbol{q}_i + \sum_{k\in K} \boldsymbol{q}_k$ a $\boldsymbol{v}_3 = \sum_{k\in K} \boldsymbol{m}_k + \sum_{j\in J} \boldsymbol{g}_j$. Nejprve uvažujme, že $\boldsymbol{v}_1 \neq \boldsymbol{0}$ a $\boldsymbol{v}_3 \neq \boldsymbol{0}$. Protože $\mathcal{C}(M_n) \subseteq \mathcal{C}(G_n)$, $\boldsymbol{v}_1 \in \mathcal{C}(G_n)$ a $\boldsymbol{v}_3 \in \mathcal{C}(G_n)$ a z věty 10 $\mathrm{w}(\boldsymbol{v}_1) \geq n-1$ i $\mathrm{w}(\boldsymbol{v}_3) = n-1$, tedy $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1)$. Pokud $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, pak $(\boldsymbol{v}_1) = \mathrm{w}(\boldsymbol{v}_3) = n-1$ a $\mathrm{w}(\boldsymbol{v}_2) = 0$. Opět z věty 10 máme $\boldsymbol{v}_1 = \boldsymbol{m}_x$ a $\boldsymbol{v}_3 = \boldsymbol{m}_y$ pro nějaká $x, y \in \{1, \cdots, 2^{n-2}(n-1)\}$. Protože $\boldsymbol{v}_2 = \boldsymbol{0}$, platí $\sum_{i\in I} \boldsymbol{q}_i = \sum_{k\in K} \boldsymbol{q}_k$, tedy $\sum_{i\in I} \boldsymbol{q}_i G_{n-1} = \sum_{k\in K} \boldsymbol{q}_k G_{n-1}$, a tak $\boldsymbol{v}_1 = \boldsymbol{v}_3$. Z toho dostáváme, že $\boldsymbol{v}$ je řádek matice M_n. Nyní uvažujme, že $\boldsymbol{v}_1 = \boldsymbol{0}$, pak $\sum_{i\in I} \boldsymbol{q}_i G_{n-1} = \sum_{i\in I} \boldsymbol{m}_i = \sum_{j\in J} \boldsymbol{g}_j$. Potom $\boldsymbol{v}_3 = \sum_{i\in I} \boldsymbol{q}_i G_{n-1} + \sum_{k\in K} \boldsymbol{q}_k G_{n-1}$, tedy $\boldsymbol{v}_3 = \boldsymbol{v}_2 G_{n-1}$. Tedy jestli $\boldsymbol{v}_3 = \boldsymbol{0}$, pak dle lemmatu 7 je $\boldsymbol{v}_2 = \boldsymbol{0}$ nebo $\boldsymbol{v}_2 = \boldsymbol{1}$. Kdyby $\boldsymbol{v}_2 = \boldsymbol{0}$, pak $\boldsymbol{v} = \boldsymbol{0}$. Kdyby naopak $\boldsymbol{v}_2 = \boldsymbol{1}$, potom $\mathrm{w}(\boldsymbol{v}) \geq 2^{n-1} > 2(n-1)$. Dále tedy uvažujme, že $\boldsymbol{v}_3 \neq \boldsymbol{0}$, pak i $\boldsymbol{v}_2 \neq \boldsymbol{0}$. Pak z indukčního předpokladu a lemmatu 9 dostáváme $\mathrm{w}(\boldsymbol{v}) \geq 2(n-1)$. Dále když $\mathrm{w}(\boldsymbol{v}) = 2(n-1)$, pak $\mathrm{w}(\boldsymbol{v}_3) = 2(n-2)$ a dle indukčního předpokladu $\boldsymbol{v}_3 = \boldsymbol{m}_x$ pro nějaké $x \in \{1, \cdots, 2^{n-2}(n-1)\}$. Tedy dostáváme $\boldsymbol{v}_2 G_{n-1} = \boldsymbol{v}_3 = \boldsymbol{m}_x = \boldsymbol{q}_x G_{n-1}$. Z lemmatu 7 tedy $\boldsymbol{v}_2 + \boldsymbol{q}_x = \boldsymbol{0}$ nebo $\boldsymbol{v}_2 + \boldsymbol{q}_x = \boldsymbol{1}$. My opět chceme $\mathrm{w}(\boldsymbol{v}_2) = 2$. Tedy dostáváme, že $\boldsymbol{v}_2 = \boldsymbol{q}_x$, a proto $\boldsymbol{v}$ je řádek matice M_n. Pro $\boldsymbol{v}_3 = \boldsymbol{0}$ provedeme důkaz obdobně.

□

Přestože jsme místo generujících matic pracovali s maticemi G_n a M_n, v následujících tvrzeních si ukážeme možnou podobu generujících matic kódů $\mathcal{C}(G_n)$ a $\mathcal{C}(M_n)$.

Tvrzení 12. *Generující matici kódu $\mathcal{C}(G_n)$ v odstupňovaném tvaru dostaneme z matice G_n vynecháním prvního řádku.*

Důkaz. Tvrzení dokážeme jednoduchou indukcí. Vidíme, že pro

$$G_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ a } G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

tvrzení platí. Předpokládáme-li pak, že tvrzení platí pro G_{n-1}. Z podoby matice G_n z lemmatu 3, které říká, že

$$G_n = \begin{pmatrix} G_{n-1} & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & G_{n-1} \end{pmatrix},$$

vidíme, že vynecháním prvního řádku G_n dostaneme opět matici v odstupňovaném tvaru. Z lemmatu 6 máme, že $\text{rank}(G_n) = 2^n - 1$, nově vzniklá matice je tvořena $2^n - 1$ řádky původní matice G_n a je stejné hodnosti jako G_n, jde tedy o generující matici kódu $\mathcal{C}(G_n)$.

□

Generující matici kódu $\mathcal{C}(G_n)$ budeme značit $\widetilde{G_n}$.

Řádky matice G_n generují stejný prostor jako řádky matice

$$\begin{pmatrix} G_{n-1} & 0 & G_{n-1} \\ 0 & I_{2^{n-1}} & G_{n-1} \end{pmatrix},$$

tedy její řádky také generují kód $\mathcal{C}(G_n)$. Navíc pokud odebereme první řádek této matice, dostaneme opět generující matici kódu $\mathcal{C}(G_n)$ v odstupňovaném tvaru. Z této matice už lze vidět, že by nebylo těžké dostat permutací sloupců a omezeným množstvím elementárních řádkových úprav matici ve standardním tvaru.

Pro konstrukci generující matice kódu $\mathcal{C}(M_n)$ s odstupňovanými řádky nejprve ukážeme, jak výběrem řádků matice ${G_n}^T$ dostaneme generující matice kódu $\mathcal{C}({G_n}^T)$ s odstupňovanými řádky. Pomocí matice ${G_n}^T$ zkonstruujeme matici P_n následujícím induktivním způsobem vyřazováním řádků právě z matice ${G_n}^T$. Nejprve z matice ${G_n}^T$ vyřadíme první blok $2^{n-2}(n-1)$ řádků. Prostřední blok o 2^{n-1} řádcích zachováme. S posledním blokem řádků pracujeme nyní induktivně jako předtím s řádky matice ${G_n}^T$, tedy nyní prvních $2^{n-3}(n-2)$ řádků tohoto bloku vyřadíme, prostředních 2^{n-2} zachováme a u posledních $2^{n-3}(n-2)$ řádků pokračujeme s indukčním krokem. Takto postupujeme dokud nám nezbude pouze jeden řádek, který také zachováme. Z konstrukce vyplývá, že platí

$$P_n = \begin{pmatrix} I_{2^{n-1}} & I_{2^{n-1}} \\ 0 & P_{n-1} \end{pmatrix}, \text{ kde } P_1 = {G_1}^T = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

Nyní zkonstruujeme matici K_n. Víme, že matice M_n a ${G_n}^T$ mají stejný počet řádků. Matici K_n vytvoříme výběrem řádků matice M_n tak, že budeme brát stejné řádky stejných indexů jako při tvorbě P_n, akorát nyní u matice M_n. Matici $\widetilde{M_n}$ sestrojíme z matice M_n následujícím způsobem. Z prostředních 2^{n-1} řádků matice M_n vybereme všechny řádky tohoto bloku kromě prvního řádku stejně jako v tvrzení 12. K tomu z posledního bloku řádků, tedy z posledních $2^{n-2}(n-1)$ řádků, matice M_n vybereme řádky dle konstrukce matice P_n. Tyto vybrané řádky pak tvoří naši matici $\widetilde{M_n}$. Dle konstrukce dostaneme matici

$$\widetilde{M_n} = \begin{pmatrix} \widetilde{G_{n-1}} & 0 & \widetilde{G_{n-1}} \\ 0 & P_{n-1} & K_{n-1} \end{pmatrix}.$$

Lemma 13. *Matice P_n z předchozí konstrukce je generující maticí kódu $\mathcal{C}({G_n}^T)$ a je v odstupňovaném tvaru.*

Důkaz. Důkaz vyplývá přímo z konstrukce a z podoby matice ${G_n}^T$, která díky lemmatu 3 vypadá následovně

$$ {G_n}^T = \begin{pmatrix} {G_{n-1}}^T & 0 \\ I_{2^{n-1}} & I_{2^{n-1}} \\ 0 & {G_{n-1}}^T \end{pmatrix}.$$

Vidíme, že matice, která zůstane výběrem řádků dle konstrukce P_n, bude zajisté v odstupňovaném tvaru. Bereme navíc postupně $2^{n-1}, 2^{n-2}, \cdots, 2, 1$ řádků, to nám dává geometrickou řadu, jejíž součet, a tedy počet řádků matice P_n, je $2^n - 1$. Z lemmatu 6 máme, že $\text{rank}(G_n^T) = \text{rank}(G_n) = 2^n - 1$. Máme tedy matici v odstupňovaném tvaru (s lineárně nezávislými řádky), tvořenou řádky z G_n^T, jejíž počet řádků je roven hodnosti matice G_n^T. Z toho už dostáváme, že taková matice je generující matice kódu $\mathcal{C}({G_n}^T)$ s odstupňovanými řádky.

□

Tvrzení 14. *Matice $\widetilde{M_n}$ je generující matici kódu $\mathcal{C}(M_n)$ a je v odstupňovaném tvaru.*

Důkaz. Matice $\widetilde{M_n}$ dle své konstrukce, tvrzení 12 a lemmatu 13 má $2^n - 2$ řádků a je v odstupňovaném tvaru. Z lemmatu 8 máme, že $\text{rank}(M_n) = 2^n - 2$, tedy matice $\widetilde{M_n}$, která má také hodnost $2^n - 2$, je generující maticí kódu $\mathcal{C}(M_n)$ a je v odstupňovaném tvaru.

□

V následujícím příkladu ukážeme, jak vypadají generující matice kódů $\mathcal{C}(G_3)$ a $\mathcal{C}(M_3)$.

Příklad. Matici G_3 máme již v prvním příkladu, snadno tedy dostaneme dle tvrzení 12 matici

$$\widetilde{G_3} = \left(\begin{array}{cccc|cccc|cccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right).$$

Vidíme, že tato matice je v odstupňovaném tvaru a první řádek G_3 je lineární kombinací všech řádků $\widetilde{G_3}$, tedy $\widetilde{G_3}$ je generující maticí $\mathcal{C}(G_3)$.

Matici $\widetilde{M_3}$ dostaneme pomocí konstrukce před tvrzením 14. Jednoduše dostaneme matici

$$\widetilde{G_2} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Pomocí konstrukce před lemmatem 13 dostaneme z matice G_2^T matici

$$P_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

a také výběrem stejných řádků z matice M_2 dostaneme matici

$$K_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Tedy dle zmíněné konstrukce

$$\widetilde{M_3} = \begin{pmatrix} \widetilde{G_2} & \mathrm{o} & \widetilde{G_2} \\ \mathrm{o} & P_2 & K_2 \end{pmatrix} = \left(\begin{array}{cccc|cccc|cccc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right),$$

což je generující matice kódu $\mathcal{C}(M_3)$ v odstupňovaném tvaru.

3 Duály kódů

V této kapitole nejprve ukážeme, že $\mathcal{C}(M_n) = \mathcal{C}(\mathcal{D}_n)$ a poté ukážeme jaká je minimální vzdálenost duálů kódů $\mathcal{C}(G_n) = \mathcal{C}(\mathcal{G}_n)$ a $\mathcal{C}(M_n) = \mathcal{C}(\mathcal{D}_n)$, tedy kódů $\mathcal{C}(\mathcal{G}_n)^\perp$ a $\mathcal{C}(\mathcal{D}_n)^\perp$. Pro dokázání věty o minimálních vzdálenostech těchto kódů nejprve zformulujeme a dokážeme jednoduchá lemmata.

Lemma 15. *Matice M_n, která je maticí sousednosti grafu $L(Q_n)$, je zároveň maticí incidence designu $\mathcal{D}_n$.*

Důkaz. Řádek matice M_n reprezentuje podle definice matice sousednosti nějaký vrchol $\{\boldsymbol{u}, \boldsymbol{v}\} \in E_n$. V tomto řádku jsou pak jedničky právě ve sloupcích, které reprezentují vrcholy sousedné s $\{\boldsymbol{u}, \boldsymbol{v}\}$. Pro $\{\boldsymbol{u}, \boldsymbol{v}\}, \{\boldsymbol{x}, \boldsymbol{y}\} \in E_n$ platí, že jsou sousedné právě tehdy, když $|\{\boldsymbol{u}, \boldsymbol{v}\} \cap \{\boldsymbol{x}, \boldsymbol{y}\}| = 1$. Ovšem pro design $\mathcal{D}_n$ platí, že blok $\overline{\{\boldsymbol{u}, \boldsymbol{v}\}} = \left\{\{\boldsymbol{x}, \boldsymbol{y}\} \in E_n \middle| |\{\boldsymbol{u}, \boldsymbol{v}\} \cap \{\boldsymbol{x}, \boldsymbol{y}\}| = 1\right\}$ pro $\{\boldsymbol{u}, \boldsymbol{v}\} \in E_n$. Z toho už vidíme, že pokud bereme, že řádky matice reprezentují nyní bloky, dostaneme jedničky na stejných pozicích jako když jsme uvažovali, že řádky reprezentují vrcholy v E_n.

□

Důsledek. Kód $\mathcal{C}(M_n)$ je roven kódu $\mathcal{C}(\mathcal{D}_n)$.

Protože v následujících důkazech budeme pracovat s bloky designů a s incidencí, budeme dále označovat kód $\mathcal{C}(G_n)$ jako $\mathcal{C}(\mathcal{G}_n)$ a $\mathcal{C}(M_n)$ jako $\mathcal{C}(\mathcal{D}_n)$.

Lemma 16. *Pro kódy $\mathcal{C}(\mathcal{G}_n)$ a $\mathcal{C}(\mathcal{D}_n)$ platí, že $\mathbf{1} \in \mathcal{C}(\mathcal{G}_n)$ a $\mathbf{1} \in \mathcal{C}(\mathcal{D}_n)$. Navíc pro matici G_n platí, že existují dvě disjunktní množiny řádků, každá o velikosti 2^{n-1}, takové, že lineární kombinace všech řádků obou množin dá právě jedničkový vektor $\mathbf{1}$.*

Důkaz. Nejprve ukážeme poslední část tvrzení. Pro $n = 1$ tvrzení platí triviálně. Pro $n = 2$ máme matici

$$G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Tedy $\mathbf{1}$ dostaneme sečtením prvního a posledního řádku a zároveň součtem druhého a třetího řádku také dostaneme $\mathbf{1}$, tedy pro $n = 2$ tvrzení platí.

Nyní předpokládejme, že tvrzení platí pro $n - 1$. Označíme A_1 množinu indexů řádků G_{n-1}, které se sčítají na $\mathbf{1}$ a A_2 druhou množinu indexů řádků G_{n-1}, které se sčítají na $\mathbf{1}$. Z lemmatu 3 máme:

$$G_n = \begin{pmatrix} G_{n-1} & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & G_{n-1} \end{pmatrix}.$$

Pokud z prvních 2^{n-1} řádků vezmeme řádky s indexy A_1 a z množiny druhých 2^{n-1} řádků vezmeme řádky s indexy A_2, dostaneme z podoby matice G_n jedničkový vektor $\mathbf{1}$. Pokud naopak z prvních 2^{n-1} řádků vezmeme řádky s indexy A_2 a z množiny druhých 2^{n-1} řádků vezmeme řádky s indexy A_1 dostaneme opět jedničkový vektor $\mathbf{1}$. Z toho dostáváme, že pro matici G_n platí, že existují dvě

disjunktní množiny řádků, každá o velikosti 2^{n-1} takové, že lineární kombinace všech řádků dané množiny dá právě jedničkový vektor $\mathbf{1}$. Triviálně z toho plyne, že $\mathbf{1} \in \mathcal{C}(\mathcal{G}_n)$.

Nakonec dokážeme, že $\mathbf{1} \in \mathcal{C}(\mathcal{D}_n)$. Využijeme opět podobu matice M_n dle lemmatu 5, tedy

$$M_n = \begin{pmatrix} M_{n-1} & {G_{n-1}}^T & \mathrm{o} \\ G_{n-1} & \mathrm{o} & G_{n-1} \\ \mathrm{o} & {G_{n-1}}^T & M_{n-1} \end{pmatrix}.$$

Navíc máme, že

$$G_{n-1}^T = \begin{pmatrix} G_{n-2}^T & \mathrm{o} \\ I_{2^{n-2}} & I_{2^{n-2}} \\ \mathrm{o} & G_{n-2}^T \end{pmatrix}.$$

Z prvních $2^{n-2}(n-1)$ řádků matice M_n vezmeme prostředních 2^{n-2} řádků a ty sečteme. Tak dostaneme vektor s jedničkami na prostředních 2^{n-2} pozicích a nulami jinde. To platí, protože prostředních 2^{n-2} řádků M_{n-1} dává blok $\begin{pmatrix} G_{n-2} & \mathrm{o} & G_{n-2} \end{pmatrix}$ a součet těchto řádků dá nulový vektor z lemmatu 7.

Pokud pak z druhých 2^{n-1} řádků vezmeme správné řádky dle předchozí části důkazu a sečteme je, dostaneme přesně vektor s jedničkami všude, kromě prostředních 2^{n-1} pozic.

Součtem těchto dvou vektorů pak dostáváme jedničkový vektor $\mathbf{1}$. Tedy máme $\mathbf{1} \in \mathcal{C}(\mathcal{D}_n)$.

□

Nyní už můžeme ukázat, jakou mají váhu kódy $\mathcal{C}(\mathcal{G}_n)^\perp$ a $\mathcal{C}(\mathcal{D}_n)^\perp$. Následující věta platí pouze pro $n \geq 3$. Ukážeme tedy nejdříve minimální váhu těchto kódů pro $n = 1$ a $n = 2$. Pro $n = 1$ existuje pouze kód $\mathcal{C}(\mathcal{G}_1) = \left\{ \begin{pmatrix} 1 \end{pmatrix}, \begin{pmatrix} 0 \end{pmatrix} \right\}$, tedy $\mathcal{C}(\mathcal{G}_1)^\perp = \left\{ \begin{pmatrix} 0 \end{pmatrix} \right\}$. Pro $n = 2$ máme

$$\begin{aligned} \mathcal{C}(\mathcal{G}_2) = \Big\{ &\begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}, \\ &\begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \Big\}, \end{aligned}$$

a tedy

$$\mathcal{C}(\mathcal{G}_2)^\perp = \left\{ \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \right\}.$$

Dále také:

$$\mathcal{C}(\mathcal{D}_2) = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \right\},$$

a proto

$$\mathcal{C}(\mathcal{D}_2)^\perp = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \right\}.$$

Dostáváme tak, že minimální váha kódu $\mathcal{C}(\mathcal{G}_2)^\perp$ je 4. Minimální váha kódu $\mathcal{C}(\mathcal{D}_2)^\perp$ je 2.

Nyní dokážeme minimální vzdálenost těchto kódů pro $n \geq 3$.

Věta 17. *Pro $n \geq 3$ mají kódy $\mathcal{C}(\mathcal{G}_n)^\perp$ a $\mathcal{C}(\mathcal{D}_n)^\perp$ minimální váhu 4.*

Důkaz. Dle lemmatu 8 máme $\mathcal{C}(\mathcal{D}_n) \subseteq \mathcal{C}(\mathcal{G}_n)$, tedy $\mathcal{C}(\mathcal{G}_n)^\perp \subseteq \mathcal{C}^\perp(\mathcal{D}_n)$. Ukážeme tedy, že $\mathcal{C}(\mathcal{G}_n)^\perp$ obsahuje slovo váhy 4 a také, že minimální váha kódu $\mathcal{C}(\mathcal{D}_n)^\perp$ je alespoň 4.

Proto, abychom nalezli slovo z $\mathcal{C}(\mathcal{G}_n)^\perp$ váhy 4, využijeme podobu generující matice z konce druhé kapitoly z tvrzení 12. Generující matice kódu je totiž zároveň kontrolní maticí duálu daného kódu. Tedy máme-li matici $\widetilde{G_n}$, pak z definice kontrolní matice pro $\boldsymbol{u} \in \mathbb{F}^{2^{n-1}n}$ platí, že $\boldsymbol{u} \in \mathcal{C}(\mathcal{G}_n)^\perp \iff \widetilde{G_n}\boldsymbol{u}^T = \mathbf{0}$. My víme, že $\widetilde{G_n}$ dostaneme z G_n odebráním prvního řádku. Dále víme, že

$$G_n = \begin{pmatrix} G_{n-1} & I_{2^{n-1}} & \mathrm{o} \\ \mathrm{o} & I_{2^{n-1}} & G_{n-1} \end{pmatrix},$$

a že

$$\widetilde{G_2} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Dostáváme z toho tedy, že pro $n = 2$ má slovo váhy 4 ležící v $\mathcal{C}(\mathcal{G}_n)^\perp$ podobu $\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$. Pro obecné n dostáváme z podoby matice G_n, že jedním ze slov váhy 4 ležící v kódu $\mathcal{C}(\mathcal{G}_n)^\perp$ je slovo $\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$.

Nyní ukážeme, že minimální váha kódu $\mathcal{C}(\mathcal{D}_n)^\perp$ je alespoň 4. Dle lemmatu 16 $\mathbf{1} \in \mathcal{C}(\mathcal{D}_n)$. Z toho dostáváme, že kód $\mathcal{C}(\mathcal{D}_n)^\perp$ musí být sudé váhy. Ukážeme nyní, že kód $\mathcal{C}(\mathcal{D}_n)^\perp$ neobsahuje slovo váhy 2. Uvažujme, že toto slovo má jedničky na pozicích $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}$,$\{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}$, kde $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\} \neq \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}$, pro $i, j \in \{1, \cdots, 2^{n-1}n\}$ a $\boldsymbol{x}, \boldsymbol{y} \in V_n$. Chceme ukázat, že pro libovolné $\boldsymbol{x}, \boldsymbol{y}$ existuje blok $\overline{\{\boldsymbol{u}, \boldsymbol{v}\}}$, kde $\boldsymbol{u}, \boldsymbol{v} \in V_n$, takový, že $\left|\overline{\{\boldsymbol{u}, \boldsymbol{v}\}} \cap \left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}\right\}\right| = 1$. Rozebereme jednotlivé možnosti.

Pokud $\boldsymbol{x} = \boldsymbol{y}$, nebo $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{e}_j$, pak $\boldsymbol{e}_i \neq \boldsymbol{e}_j$ a $\left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}\right\} = \left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_j\}\right\}$. Vezmeme blok $\overline{\{\boldsymbol{x}+\boldsymbol{e}_i, \boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j\}}$, ten obsahuje $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}$, ale neobsahuje $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_j\}$, tedy

$$\left|\overline{\{\boldsymbol{x}+\boldsymbol{e}_i, \boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j\}} \cap \left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}\right\}\right| = 1.$$

Pokud $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}_i$, nebo $\boldsymbol{x} + \boldsymbol{e}_i = \boldsymbol{y} + \boldsymbol{e}_j$, pak $\left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}\right\} = \left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{x}+\boldsymbol{e}_i, \boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j\}\right\}$, a proto $\boldsymbol{e}_i \neq \boldsymbol{e}_j$. Tedy vezmeme blok $\overline{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_j\}}$, ten obsahuje $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}$, ale neobsahuje $\{\boldsymbol{x}+\boldsymbol{e}_i, \boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j\}$, tedy

$$\left|\overline{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_j\}} \cap \left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}\right\}\right| = 1.$$

Nakonec pokud $\boldsymbol{x} \neq \boldsymbol{y}$ a $\boldsymbol{x} \neq \boldsymbol{y}+\boldsymbol{e}_j$, vezmeme $\boldsymbol{z} \in V_n$, takové, že $\boldsymbol{z} \neq \boldsymbol{x}$, $\boldsymbol{z} \neq \boldsymbol{x}+\boldsymbol{e}_i$, $\boldsymbol{z} \neq \boldsymbol{y}$ a $\boldsymbol{z} \neq \boldsymbol{y}+\boldsymbol{e}_j$ a blok $\overline{\{\boldsymbol{x}, \boldsymbol{z}\}}$. Pro ten opět platí

$$\left|\overline{\{\boldsymbol{x}, \boldsymbol{z}\}} \cap \left\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_j\}\right\}\right| = 1.$$

Tím jsme probrali všechny možnosti, a tedy v kódu $\mathcal{C}^\perp(\mathcal{D}_n)$ nemůže slovo váhy 2 existovat, tedy minimální váha kódu musí být alespoň 4.

Víme, že $\mathcal{C}(\mathcal{G}_n)^\perp$ obsahuje slova váhy 4, tedy i $\mathcal{C}(\mathcal{D}_n)^\perp$ obsahuje slova váhy 4, protože $\mathcal{C}(\mathcal{G}_n)^\perp \subseteq \mathcal{C}(\mathcal{D}_n)^\perp$. Dostáváme tak, že minimální vzdálenost kódů $\mathcal{C}(\mathcal{G}_n)^\perp$ a $\mathcal{C}(\mathcal{D}_n)^\perp$ je 4.

□

Důsledek. Kód $\mathcal{C}(\mathcal{G}_n)^\perp$ je lineární $[2^{n-1}n, 2^{n-1}n - 2^n + 1{,}4]_2$ kód a kód $\mathcal{C}(\mathcal{D}_n)^\perp$ je lineární $[2^{n-1}n, 2^{n-1}n - 2^n + 2{,}4]_2$ kód.

V předchozím důkazu jsme ukázali jedno možné slovo váhy 4 ležící v kódu $\mathcal{C}(\mathcal{G}_n)^\perp$, takových slov je ovšem víc. Lze ukázat, že kód $\mathcal{C}(\mathcal{G}_n)^\perp$ obsahuje slovo s jedničkami právě na pozicích $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}$, $\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_j\}$, $\{\boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j, \boldsymbol{x}+\boldsymbol{e}_i\}$ a $\{\boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j, \boldsymbol{x}+\boldsymbol{e}_j\}$, pro libovolné $\boldsymbol{x} \in V_n$. Takovéto slovo má zjevně váhu 4. Pro ukázání, že takové slovo leží v $\mathcal{C}(\mathcal{G}_n)^\perp$ nejprve označíme množinu těchto hran

$$S = \Big\{\{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_j\}, \{\boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j, \boldsymbol{x}+\boldsymbol{e}_i\}, \{\boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j, \boldsymbol{x}+\boldsymbol{e}_j\}\Big\}.$$

Vezmeme-li libovolný blok designu $\mathcal{G}_n$, $\overline{\boldsymbol{y}} = \Big\{\{\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_i\}\Big| i \in \{1, \ldots, n\}\Big\}$, dostaneme, že $|S \cap \overline{\boldsymbol{y}}| = 2$, pokud $\boldsymbol{y} \in \{\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_i, \boldsymbol{x}+\boldsymbol{e}_j, \boldsymbol{x}+\boldsymbol{e}_i+\boldsymbol{e}_j\}$, a $|S \cap \overline{\boldsymbol{y}}| = 0$ jinak. Tedy $\mathcal{C}^\perp(\mathcal{G}_n)$ obsahuje právě toto slovo váhy 4.

Naopak na druhou část důkazu, kde dokazujeme, že kód $\mathcal{C}(\mathcal{D}_n)^\perp$ neobsahuje slovo váhy 2, můžeme také opět použít generující matice kódu $\mathcal{C}(\mathcal{G}_n)$, tedy kontrolní matici jeho duálu. Stačí si uvědomit, co by znamenalo, kdyby kód $\mathcal{C}(\mathcal{G}_n)^\perp$ obsahoval slovo $\boldsymbol{u}$ váhy 2. Z definice kontrolní matice by $\widetilde{M_n}\boldsymbol{u}^T = \boldsymbol{0}$ pro $\boldsymbol{u}$ váhy 2 znamenalo, že matice $\widetilde{M_n}$ má dva stejné sloupce. Proto, abychom toto vyvrátili, stačí jednoduchou indukcí ukázat, že matice $\widetilde{G_n}$ nemá dva sloupce stejné, matice P_n nemá dva sloupce stejné a že matice $\widetilde{G_n}$, P_n, K_n nemají žádný sloupec nulový.

U matice $\widetilde{G_2}$ z příkladu v předchozí kapitole vidíme, že nemá nulový sloupec ani dva sloupce stejné. Indukcí pak z podoby matice $\widetilde{G_n}$ dostaneme také, že tato matice nemá nulový sloupec ani dva sloupce stejné. Pro matici P_n dostaneme to samé z podoby této matice zmíněné v konstrukci před lemmatem 13. Nakonec to, že matice K_n nemá nulový sloupec plyne z podoby matice M_n a toho, jakým způsobem řádky vybíráme v prvních dvou induktivních krocích. V prvním kroku dostaneme $\begin{pmatrix} G_n & 0 & G_n \end{pmatrix}$, v druhém však prostřední, doteď nulový, blok začnou tvořit dvě jednotkové matice vedle sebe, což plyne z podoby matice ${G_n}^T$. Tedy z těchto pozorování a podoby matice $\widetilde{M_n}$ dostaneme, že tato matice nemá dva stejné sloupce.

Závěr

V této práci jsme se zabývali kódy designu definovaného pomocí vrcholového grafu n-dimenzionální krychle, kódy indukovanými hranovým grafem n-dimenzionální krychle a duálů těchto kódů. Přičemž hlavním smyslem práce bylo ukázat základní parametry těchto kódů. U kódu $\mathcal{C}(G_n) = \mathcal{C}(\mathcal{G}_n)$ jsme dokázali, že jeho dimenze je $2^n - 1$ a jeho Hammingova vzdálenost je n. U druhého z kódů, $\mathcal{C}(M_n) = \mathcal{C}(\mathcal{D}_n)$ jsme dokázali, že jeho dimenze je $2^n - 2$ a jeho Hammingova vzdálenost je $2(n-1)$. U těchto kódů jsme také ukázali, jak vypadají jejich generující matice a tedy kontrolní matice duálů těchto kódů. Na konec jsme zkoumali duály těchto kódů, u nichž jsme ukázali, že Haminngova vzdálenost duálů obou kódů je 4 bez ohledu na velikosti n, pro $n \geq 3$.

U kódů $\mathcal{C}(G_n)$ a $\mathcal{C}(M_n)$ jsme tedy ukázali, že kód $\mathcal{C}(M_n)$ sice má menší dimenzi, tedy bude obsahovat méně kódových slov, ale jeho Hammingva vzdálenost je pro velká n mnohem větší (téměř dvakrát). Pro oba kódy dimenze a délka kódových slov rostou exponenciálně, kdežto Hammingva vzdálenost roste pouze lineárně. Pro velká n tedy nemusí působit tyto kódy moc dobře, z důvodu dlouhých kódových slov.

Mým přínosem v této práci bylo doplnění důkazů a případně jejich upřesnění, či pozměnění. U důkazu věty 11 jsem napsal program (Příloha A.1), který hrubou silou hledá minimální slova kódu $\mathcal{C}(M_4)$, abychom měli důkaz pro zahájení indukce od $n = 4$. Dále jsem také doplnil řadu technických tvrzení potřebných pro důkazy vět a ta jsem dokázal, konkrétně to jsou lemma 1, 2, 4, 5, 6, 7, 9, 15 a lemma 16. Zásadní myšlenky a tvrzení jsem ilustroval na konkrétních příkladech a obrázcích grafů. Na konci druhé kapitoly jsem navíc zkoumal podobu generujících matic kódů, nebo-li kontrolních matic duálů těchto kódů (tvrzení 12, tvrzení 14 a lemma 13), jimiž se článek Fish et al., 2010, ze kterého práce vychází, vůbec nezabývá.

Důvodem, proč jsme se zabývali kódy designů $\mathcal{D}_n$ a $\mathcal{G}_n$ a v čem je dobré se takovýmto kódům věnovat, je, že pomocí nich můžeme tvořit takzvané Hulls těchto designů. Pro design $\mathcal{D}$ je $\mathrm{Hull}(\mathcal{D}) = \mathcal{C}(\mathcal{D}) \cap \mathcal{C}(\mathcal{D})^{\perp}$, tedy samoortogonální kód. Ty se dále zkoumají v souvislosti s permutačním kódováním a především dekódováním. Těmto dvěma tématům se dále více zabývají právě články Fish et al., 2010, Fish et al., 2009a a Fish et al., 2009b.

Literatura

Beth, Thomas, 1985. *Design Theory*. Mannheim : Bibliographisches Institut. ISBN 3-411-01675-2.

Fish, Washiela; Key, Jennifer; Mwambene, Eric, 2009a. Codes, designs and groups from the Hamming graphs. *Journal of Combinatorics, Information & System Sciences*. Roč. 34.

Fish, Washiela; Key, Jennifer; Mwambene, Eric, 2009b. Graphs, designs and codes related to the n-cube. *Discret. Math.* Roč. 309, č. 10, s. 3255–3269. Dostupné z DOI: 10.1016/J.DISC.2008.09.024.

Fish, Washiela; Key, Jennifer; Mwambene, Eric, 2010. Binary codes from the line graph of the n-cube. *Journal of Symbolic Computation*. Roč. 45, č. 7, s. 800–812. ISSN 0747-7171. Dostupné z DOI: https://doi.org/10.1016/j.jsc.2010.03.012. Algebraic Coding Theory and Applications.

Matoušek, Jiří; Nešetřil, Jaroslav, 2000. *Kapitoly z diskrétní matematiky*. Praha: Karolinum. Druhé vydání. ISBN 80-246-0084-6.

Žemlička, Jan, 2024. *Samoopravné kódy* [online]. [cit. 2024-04-16]. Dostupné z: https://www.karlin.mff.cuni.cz/~zemlicka/23-24/SoKn.pdf.

Seznam obrázků

A Přílohy

A.1 Program hledající minimální slova kódu $\mathcal{C}(M_4)$

Program 1 Program hledající minimální slova kódu $\mathcal{C}(M_4)$

```
import numpy as np
import itertools

# induktivni tvorba matice Gn z G(n-1)
def make_Gn(G_nmin1, n):
    I_n = np.eye(2**(n-1))
    zeros_n = np.zeros_like(G_nmin1)
    G_n = np.block([[G_nmin1, I_n, zeros_n],
                    [zeros_n, I_n, G_nmin1]])
    return(G_n)
# funkce pro nalezeni minimalnich slov
def find_min_words(matrix, n):
    result = []
    predicted_min_weight = 2*(n-1)
    rankM = (2 ** n) - 2
    # vybrani radku, abychom je meli pouze jednou
    for row in matrix:
        if sum(np.array(row)) < (predicted_min_weight + 1):
            if not any(np.array_equal(row, w) for w in result):
                result.append(row)
    rows_list = result

    for i in range(2, rankM + 1): # scitani dvojic, trojic,...
        # nalezeni moznych kombinaci
        combinations_i = itertools.combinations(rows_list, i)
        # pres vsechny kombinace
        for combination in combinations_i:
            # linearni kombinace vektoru
            vec = np.array(np.sum(combination, axis=0) % 2)
            weight = sum(vec)
            if weight < predicted_min_weight+1 and weight > 0:
                if not any(np.array_equal(vec, w) for w in result):
                    result.append(vec)
    return result

def main():
    G1 = np.array([[1], [1]])
    G2 = make_Gn(G1, 2)
    G3 = make_Gn(G2, 3)
    G4 = make_Gn(G3, 4)
    M4 = np.matmul(np.transpose(G4), G4) % 2
    # nalezeni minimalnich slov kodu C(M4)
    min_words_C_M4 = find_min_words(M4, 4)
    print(min_words_C_M4)
    print(len(min_words_C_M4))

main()
```