Kapitola 1

Úvod

1.1 Jaké kódy?

Řekněme nejprve, jaké kódování nás v tomto textu bude zajímat a jaké ne. K jistému druhu kódování mají vztah například následující pojmy:

- *Kryptografie*, která používá šifrování dat pro zajištění jejich bezpečného přenosu. Té se nebudeme věnovat vůbec.
- *Komprese dat*, tedy kódování dat s cílem zmenšit jejich objem. Ta je našemu zaměření blíže a stručně se o ní zmíníme.
- *Samoopravné kódy*, které slouží k detekci a opravování chyb, vzniklých při přenosu dat. Právě těm se budeme věnovat v celé této přednášce.

1.2 Jednoduchý příklad samoopravného kódu

Představme si následující situaci. Potřebujeme poslat určitá data po telekomunikační lince, která není příliš spolehlivá, takže při přenosu pravděpodobně vlivem šumu dojde k řadě chyb. Pro nás je však důležité zajistit, aby příjemce obdržel data bez chyb, a za tím účelem jsme ochotni poslat i něco navíc, pokud to pomůže případné chyby eliminovat. Přenos je však drahý, a tak samozřejmě chceme, aby celkový objem posílaných dat byl co nejmenší.

Data, která odesíláme, jsou tvořena posloupností n *bitů* (symbolů 0 a 1). Při přenosu může u libovolného bitu dojít k chybě (tj. přijatý bit se liší od odeslaného). Pravděpodobnost chyby je u každého bitu p. Chyby jsou navzájem nezávislé.

Pošleme-li data bez jakékoli úpravy, pak pravděpodobnost, že budou přijata bez chyby, je $(1-p)^n$. Dejme tomu pro $n = 100$ a $p = 0.01$ je pravděpodobnost bezchybného příjmu slabých 37%. Jak ji zvýšit? Nejjednodušší způsob je poslat

každý bit víckrát (řekněme třikrát) a při příjmu pro něj zvolit 'většinovou' hodnotu (tedy tu, která v přijaté trojici převládá). Jinak řečeno, bit 0 při odesílání *kódujeme* jako posloupnost 000 a bit 1 jako posloupnost 111. Při příjmu pak trojice *dekódujeme* podle pravidel

$$000, 001, 010, 100 \to 0,$$
$$111, 110, 101, 011 \to 1.$$

Spočítejme pravděpodobnost správného dekódování. Jednotlivý bit se správně dekóduje právě tehdy, když při přenosu příslušné trojice nastane nejvýše jedna chyba, a k tomu dojde s pravděpodobností

$$(1-p)^3 + 3p(1-p)^2 = (1-p)^2(1+2p).$$

Celou posloupnost se nám tedy podaří bezchybně dekódovat s pravděpodobností $((1-p)^2(1+2p))^n$, což pro uvedené hodnoty n a p vychází na slušných 97%. Cenou, kterou za to platíme, je trojnásobný objem posílaných dat.

Jak uvidíme dále, v tomto příkladu jsme vlastně použili jistý jednoduchý kód, tzv. *opakovací kód délky* 3. V této přednášce se budeme zabývat existencí kódů, které umožňují co nejspolehlivější opravování chyb a vyžadují přitom co nejmenší nárůst objemu posílaných dat. Zaměříme se i na různé kombinatorické aspekty problému existence takových kódů.

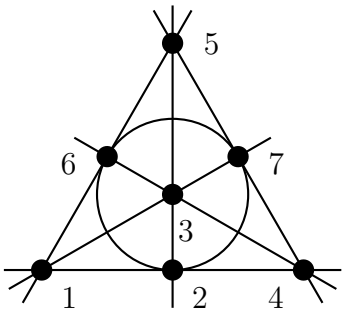
1.3 Hammingův kód $\mathcal{H}$

Příklad 'kódu' v minulém oddílu byl až trochu příliš jednoduchý. Ukažme si tedy ještě jeden příklad, tzv. Hammingův kód, který v naší přednášce bude hrát velmi důležitou úlohu.

Zkonstruujeme jej pomocí hypergrafu na obr. 1.1, známé *Fanovy roviny*. Má 7 vrcholů (*bodů*) a 7 hran (*přímek*), přičemž každá přímka obsahuje 3 body a každé dvě přímky se protínají právě v jednom bodě. (Na obr. 1.1 není přímka $\{2,6,7\}$ příliš 'přímá' — je nakreslena jako kružnice.)

Body jsou na tomto obrázku označeny čísly 1 až 7. Každou množinu $P \subset \{1,\ldots,7\}$ můžeme ztotožnit s jejím *charakteristickým vektorem*, tj. s vektorem 7 nul a jedniček, na jehož i-té pozici je 1, právě když $i \in P$. Zmíněnou přímku $\{2,6,7\}$ tedy reprezentuje vektor (0100011). (Časem budeme s těmito vektory počítat jako s prvky vektorového prostoru $\mathbb{F}_2^7$ nad dvouprvkovým tělesem $\mathbb{F}_2$.)

Nechť $\mathcal{H} \subset \mathbb{F}_2^7$ je množina, tvořená charakteristickými vektory všech 7 přímek a jejich 7 doplňků, a dále dvěma konstantními vektory $(0\ldots0)$ a $(1\ldots1)$. Těchto 16 vektorů budeme označovat jako *kódová slova*; množina kódových slov je *kód*, v našem případě *Hammingův kód*. (Přesnou definici kódu a příbuzných pojmů podáme v oddílu 1.5. O Hammingových kódech budeme mluvit v oddílu 3.3.)



Obrázek 1.1: Fanova rovina.

Náš kód má jednu zajímavou vlastnost: každá dvě kódová slova se liší alespoň ve třech souřadnicích. Platí dokonce silnější tvrzení: pro každý vektor z prostoru $\mathbb{F}_2^7$ existuje *právě jedno* kódové slovo, které se od něj liší v nejvýše jedné souřadnici. Ověření ponecháváme na čtenáři jako součást cvičení 1.3.1. Pro nás z této vlastnosti plyne důležitý důsledek: pokud se při přenosu kódového slova poruší nejvýše jeden bit, lze jej opravit. Stačí totiž vzít jednoznačně určené kódové slovo, které se od přijatého slova liší jen v jedné souřadnici. (Pokud se poruší více bitů, například všechny, pak nás samozřejmě tento kód nezachrání.)

Jak toto pozorování využít? Vraťme se k naší n-bitové posloupnosti. Rozdělíme-li ji do bloků o 4 bitech, pak každý z těchto bloků je dvojkovým zápisem nějakého čísla i od 0 do 15 a odpovídá mu tedy nějaké kódové slovo v_i. Naše strategie je jednoduchá: místo bloku po lince posílat příslušné kódové slovo.

Například pro posloupnost 00101110 získáme bloky 0010 a 1110, které ve dvojkovém zápisu odpovídají číslům 2 resp. 14. Dejme tomu, že v našem očíslování je $v_2 = (0110100)$ a $v_{14} = (0010111)$. Odesílaná posloupnost tedy bude 01101000010111. Příjemce naše kódování zná a z obdržených dat dokáže rekonstruovat původní posloupnost 00101110.

Přenášená posloupnost je opět delší (místo n bitů posíláme $7n/4$), ale díky uvedeným vlastnostem našeho kódu dokážeme správně rekonstruovat kódové slovo, při jehož přenosu došlo k nejvýše jedné chybě. To se stane s pravděpodobností

$$(1-p)^7 + 7p(1-p)^6 = (1-p)^6(1+6p),$$

a protože kódových slov je celkem $n/4$, příjemce data správně dekóduje s pravděpodobností

$$\Big((1-p)^6(1+6p)\Big)^{n/4} = (1-p)^{\frac{3n}{2}} \cdot (1+6p)^{\frac{n}{4}},$$

což pro $n = 100$ a $p = 0.01$ činí asi 95%. To je jen o málo méně než u opakovacího kódu, ale objem posílaných dat je nyní o více než třetinu menší!

Cvičení

▶ **1.3.1.** (i) Jakým množinám bodů Fanovy roviny odpovídají kódová slova Hammingova kódu H délky 7?

(ii) Ukažte, že každá dvě kódová slova kódu H se liší alespoň ve třech souřadnicích.

(iii) Ukažte, že pro každý vektor $x \in \mathbb{F}_2^7$ existuje právě jedno kódové slovo z kódu H, které se od vektoru x liší nejvýše v jedné souřadnici.

1.4 Kanál, kódování a dekódování

Po neformálním úvodu podáme poněkud přesnější popis situace. Nechť $\Sigma = \{s_0, \ldots, s_m\}$ je konečná *abeceda*, tj. množina *symbolů*. *Slovo* délky ℓ je uspořádaná ℓ-tice symbolů. Množinu všech slov délky ℓ značíme Σ^ℓ.

Popisujeme zařízení, kterému budeme říkat *kanál*. Na jednom konci kanálu stojí odesílatel, na druhém příjemce. Odesílatel má posloupnost $w_1 w_2 \ldots w_M$ *zdrojových slov* z množiny $W \subset \Sigma^\ell$, kterou potřebuje bez chyby přepravit k příjemci. Po kanálu lze posílat symboly z abecedy Σ (jeden po druhém). Pro každou dvojici $i, j \in \{0, \ldots, m\}$ je určena pravděpodobnost p_{ij}, že při odeslání symbolu s_i bude přijat symbol s_j. Tyto pravděpodobnosti samozřejmě pro každé i, j splňují podmínky

$$\sum_{k=1}^{m} p_{ik} = \sum_{k=1}^{m} p_{kj} = 1.$$

Přenosy jednotlivých symbolů jsou navzájem nezávislé náhodné procesy.

Pro zvýšení kvality komunikace odesílatel data *kóduje*. Za tím účelem používá *kód*, tj. vhodnou množinu slov $C \subset \Sigma^n$, a nějakou bijekci $\pi : W \to C$. Kód C i zobrazení π zná i příjemce. (V následujícím nás mnohem více než bijekce π bude zajímat kód C.)

Má-li odesílatel v úmyslu poslat zdrojové slovo w_i, odešle místo něj slovo $c = \pi(w_i)$ z kódu C (tzv. *odeslané slovo*). Příjemce z kanálu obdrží *přijaté slovo*[1] $\tilde{c}$. Jeho úkolem je toto slovo *dekódovat*, tj. určit odesílané slovo c, ze kterého pak už snadno rekonstruuje zdrojové slovo $\pi^{-1}(c)$. Protože výsledek přenosu slova c může teoreticky být zcela libovolný, dekódování se neobejde bez předpokladů. Obvyklým předpokladem, kterého se budeme držet v celém tomto textu, je, že odeslané slovo c je přijatému slovu nejbližší ve smyslu Hammingovy vzdálenosti, definované v následujícím oddílu. Dekódování s touto hypotézou se říká *dekódování na nejpodobnější slovo* (angl. *maximum likelihood decoding*).

[1] Náš popis kanálu je poněkud zjednodušený v tom ohledu, že zdrojové, odeslané i přijaté slovo jsou všechna nad jednou abecedou Σ. V literatuře se někdy berou v úvahu tři různé abecedy.

Není-li v konkrétním případě tento předpoklad splněn, dojde k nesprávnému dekódování. Kód C je pro daný kanál tím lepší, čím menší je pravděpodobnost porušení uvedeného předpokladu.

Nejobvyklejším typem kanálu je *binární symetrický kanál*. V tomto případě je $\Sigma = \{0, 1\}$, a označíme-li symboly $s_0 = 0, s_1 = 1$, pak

$$p_{01} = p_{10} = p, \quad p_{00} = p_{11} = 1 - p,$$

kde $p \in (0, 1)$. Číslo p je tedy pravděpodobnost chyby při přenosu jednoho symbolu.

1.5 Kód

Věnujme se nyní pojmu kódu, který se již objevil v předcházejících oddílech. *Kód*[2] nad abecedou Σ je libovolná množina $C \subset \Sigma^n$, kde číslo n je rovněž libovolné a označujeme jej jako *délku* kódu C. *Velikost* kódu je počet jeho prvků, tedy $|C|$. O prvcích množiny Σ^n hovoříme jako o *slovech*, o prvcích kódu C pak jako o *kódových slovech*.

Například Hammingův kód z oddílu 1.3 je kód o délce 7 a velikosti 16 nad abecedou o velikosti 2. Kódům nad dvouprvkovou abecedou se říká *binární* kódy. Tento případ je zdaleka nejdůležitější, zajímat nás však budou i kódy nad většími abecedami. Kód nad abecedou o velikosti q je *q-ární* kód.

Na množině Σ^n je přirozeně definován pojem vzdálenosti. Jsou-li $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ prvky množiny Σ^n, pak jejich *(Hammingova) vzdálenost* $d(x, y)$ je počet všech souřadnic, kde se liší, tedy počet všech i, pro která je $x_i \neq y_i$. Snadno se ukáže (viz cvičení 1.5.1), že $d(x, y)$ je metrika.

Podstatnou vlastností Hammingova kódu v našem příkladu je fakt, že vzdálenost každé dvojice jeho kódových slov je alespoň 3. *Minimální vzdálenost* (nebo prostě *vzdálenost*) kódu C, definovaná vztahem

$$\Delta(C) = \min_{x,y \in C} d(x, y),$$

je dalším ze základních parametrů kódu C.

Čím větší je minimální vzdálenost, tím více chyb může kód opravovat. Přesněji řečeno, předpokládejme, že $\Delta(C)$ je alespoň $2t + 1$, a že při přenosu daného slova c nastane nejvýše t chyb. Přijaté slovo $\tilde{c}$ vždy dekódujeme na nejpodobnější kódové slovo (viz oddíl 1.4), tj. na nejbližší slovo kódu C vzhledem k Hammingově vzdálenosti. Takové slovo je za daných předpokladů právě jedno a je to odeslané slovo c, takže dekódování proběhne správně. Proto o kódu C s $\Delta(C) \geq 2t + 1$ říkáme, že má schopnost *opravy t chyb*.

Shrňme základní parametry kódu C:

[2] Přesněji *blokový kód* (jde o kód, ve kterém mají všechna slova stejnou délku). Blokové kódy jsou v teorii kódů nejobvyklejší, i když se studuje i řada dalších typů kódů (např. konvoluční kódy). V tomto textu se budeme zabývat výlučně blokovými kódy.

- délka n,
- velikost $|C|$, místo které často uvažujeme její logaritmus (se základem $q = |\Sigma|$), $k = \log_q |C|$,
- minimální vzdálenost $d = \Delta(C)$.

O kódu s těmito parametry hovoříme[3] jako o *(n,k,d)-kódu*. Hammingův kód z našeho příkladu je tedy $(7, 4, 3)$-kód. Nezáleží-li na vzdálenosti, hovoříme také o (n, k)-kódu.

K těmto třem parametrům přistupuje ještě čtvrtý, velikost abecedy $q = |\Sigma|$. Je-li potřeba ji rovněž uvést, používáme označení $(n, k, d)_q$*-kód*.

Hustota kódu C je podíl

$$\alpha(C) = \frac{k}{n}.$$

Představme si pro jednoduchost, že k je celé číslo a že množina zdrojových slov je tvořena všemi slovy délky k nad abecedou Σ. Hustota kódu pak udává poměr délky zdrojového a kódového slova, takže $1/\alpha(C)$ je faktor, o který se slova prodlouží vlivem kódování.

Ideální kód tedy má co největší hustotu (takže se slova zakódováním 'příliš' neprodlouží), ale zároveň má co největší minimální vzdálenost (takže má schopnost opravy 'mnoha' chyb). Tyto požadavky jsou do jisté míry protichůdné. K nim v praxi přistupují další (např. efektivita dekódování). Vhodnost použití daného kódu tak silně závisí na konkrétní situaci.

Dva kódy, které se liší jen pořadím symbolů v kódových slovech, označujeme jako *ekvivalentní*. Takové dvojice kódů mají v podstatných ohledech stejné vlastnosti a často mezi nimi nebudeme rozlišovat.

Cvičení

▶ **1.5.1.** Ukažte, že Hammingova vzdálenost na množině Σ^n je metrika.

1.6 Jednoduché kódy

Nejjednodušším příkladem kódu je *totální kód* Σ^n, tvořený všemi slovy délky n nad abecedou Σ. Má parametry $(n, n, 1)$. *Opakovací kód* Rep_n délky n je $(n, 1, n)$-kód, složený ze všech slov tvaru $(xxx\ldots x)$, kde $x \in \Sigma$. Tyto dvě třídy kódů představují opačné extrémy, pokud jde o hodnoty k a d.

Dalším jednoduchým případem kódu je *paritní kód* nad abecedou $\mathbb{F}_2$, tvořený slovy $(x_1 \ldots x_n)$, pro která je $\sum x_i = 0$ (naše abeceda umožňuje sčítání!). Jinak řečeno, kódová slova jsou vektory nul a jedniček, ve kterých je počet jedniček sudý. Takových slov je 2^{n-1}. Jak je tomu s minimální vzdáleností? Nechť x a

[3] Zde se přidržujeme textu [9]. Jiní autoři by použili označení $(n, |C|, d)$*-kód*.

y jsou dvě kódová slova, a nechť X resp. Y je množina souřadnic i, pro něž je x_i resp. y_i rovno 1. Obě množiny X a Y mají tedy sudou velikost. Tvrdíme, že velikost symetrického rozdílu $X \oplus Y = X \cup Y - X \cap Y$ (a tedy vzdálenost slov x a y) je alespoň 2. Důvodem je, že

$$|X \oplus Y| = |X| + |Y| - 2|X \cap Y|$$

je sudé číslo. Dokázali jsme tedy, že paritní kód délky n je $(n, n-1, 2)$-kód.

1.7 Funkce $A(n,d)$ a Singletonův odhad

Kolik kódových slov může maximálně obsahovat binární kód délky n o minimální vzdálenosti d? To je jedna ze zásadních otázek teorie kódů a částečnou odpověď na ni nabízí několik známých odhadů. Jeden z nich hned uvidíme. Označme nejprve

$$A(n,d) = \max_C \log |C|,$$

kde C probíhá kódy o délce n a minimální vzdálenosti alespoň d.

Jak vychází číslo $A(n,d)$ pro malé hodnoty d? Je jasné, že $A(n,1) = n$. Pro $d = 2$ uvažme paritní kód z oddílu 1.6. Ten má minimální vzdálenost 2 a velikost 2^{n-1}, takže $A(n,2) \geq n-1$. Jak plyne z následujícího pozorování, platí dokonce rovnost $A(n,2) = n-1$.

Pozorování 1.7.1. *Pro každé $d \leq n$ je*

$$A(n,d) \leq A(n-1, d-1).$$

Důkaz. Mějme kód C délky n s minimální vzdáleností d. Odstraněním posledního symbolu každého kódového slova dostaneme kód délky $n-1$ o stejné velikosti. Jeho minimální vzdálenost je zjevně alespoň $d-1$. □

Opakovaným použitím pozorování 1.7.1 dostaneme první, nejjednodušší horní odhad funkce $A(n,d)$:

Věta 1.7.2 (Singletonův odhad)**.** *Pro každé $d \leq n$ je*

$$A(n,d) \leq n - d + 1. \quad \square$$

Rovnost $A(n,2) = A(n-1,1)$ lze mimochodem zobecnit na každé sudé d. Mějme $(n-1, k, d-1)$-kód C, kde k je libovolné. Přidejme ke každému slovu $c \in C$ jeho *paritní symbol*, tedy součet všech symbolů slova c v tělese $\mathbb{F}_2$. Výsledkem je (n,k,d)-kód, protože slova v (liché) vzdálenosti $d-1$ mají různé paritní symboly. V kombinaci s pozorováním 1.7.1 dostáváme následující tvrzení:

Tvrzení 1.7.3. *Pro každé* sudé *$d \leq n$ je*

$$A(n,d) = A(n-1, d-1). \quad \square$$

Pokud tedy jde o funkci $A(n,d)$, stačí se zaměřit na kódy s lichou minimální vzdáleností. Kolik tedy je $A(n,3)$? To uvidíme v oddílu 3.3.

Kapitola 2

Algebraické intermezzo 1

2.1 Grupy a tělesa

Grupa je dvojice $(G, *)$, kde G je množina a $*$ je binární operace na G splňující následující podmínky:

(i) $*$ je *asociativní*, tj. pro $a, b, c \in G$ platí

$$a * (b * c) = (a * b) * c,$$

(ii) existuje *neutrální prvek* operace $*$, tj. prvek n s vlastností

$$n * a = a * n = a$$

pro každé $a \in G$,

(iii) každý prvek $a \in G$ má *inverzní prvek* vzhledem k $*$, tj. prvek b s vlastností

$$a * b = b * a = n.$$

Není těžké ukázat, že neutrální prvek i inverzní prvek každého $a \in G$ jsou jednoznačně určeny (cvičení 5.1.1).

Platí-li pro každé $a, b \in G$ rovnost $a * b = b * a$, označujeme grupu $(G, *)$ jako *komutativní* nebo *abelovskou*.

Ke standardním příkladům komutativních grup patří číselné množiny se standardními operacemi: $(\mathbf{Z}, +)$, $(\mathbf{R}, +)$ nebo $(\mathbf{R} - \{0\}, \cdot)$. Nekomutativní je např. grupa všech permutací n-prvkové množiny ($n \geq 3$) s operací skládání nebo grupa všech regulárních matic o rozměrech $n \times n$ s operací násobení.

V následujícím textu budeme pro grupy používat obvykle *multiplikativní* zápis, tj. budeme grupovou operaci zapisovat jako násobení, neutrální prvek označovat symbolem 1 a inverzní prvek symbolem a^{-1}. Rovněž někdy budeme hovořit např. o grupě G bez explicitního uvedení grupové operace.

Těleso je trojice $(F, +, \cdot)$, kde $(F, +)$ je abelovská grupa s neutrálním prvkem (řekněme) 0, $(F - \{0\}, \cdot)$ je rovněž abelovská grupa, a operace + a $\cdot$ jsou svázány požadavkem *distributivity*:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Neutrální prvek vzhledem k operaci $\cdot$ označujeme 1. Stejně jako u grup někdy aritmetické operace v tělese nebudeme uvádět explicitně. *Multiplikativní grupu* $(F - \{0\}, \cdot)$ tělesa F označujeme symbolem F^*.

V teorii kódů hrají hlavní roli *konečná* tělesa, tj. tělesa s konečným počtem prvků. Jak uvidíme v odstavci 5.2, n-prvkové těleso existuje pouze pro určitá n, konkrétně pro mocniny prvočísel. Již teď ovšem můžeme snadno sestrojit tělesa $\mathbb{F}_p$, jejichž velikost je prvočíslo p: stačí vzít množinu $\{0, \ldots, p-1\}$ a definovat na ní operace $+$, $\cdot$ jako sčítání a násobení 'modulo p' (viz cvičení 2.1.1).

[*vektorové prostory nad konečnými tělesy?*]

Cvičení

▶ **2.1.1.** Nechť p je prvočíslo. Ukažte, že množina $\{0, \ldots, p-1\}$ spolu se sčítáním a násobením modulo p tvoří těleso. Ukažte, že pro neprvočíselná p tímto způsobem těleso nedostaneme.

Kapitola 3

Lineární kódy

3.1 Definice

Víme, že kód nad abecedou Σ je jakákoli podmnožina množiny Σ^n (pro libovolné n). Často je vhodné uvažovat kódy nad abecedou, která má strukturu tělesa (dejme tomu $\Sigma = \mathbb{F}_q$), a v takovém případě je přirozený požadavek, aby samotný kód byl podprostorem vektorového prostoru $\mathbb{F}_q^n$. Takový kód se označuje jako *lineární kód* nad tělesem $\mathbb{F}_q$. Například Hammingův kód $\mathcal{H}$ z oddílu 1.3 je lineární kód dimenze 4 o délce 7 nad $\mathbb{F}_2$. Má-li lineární kód C dimenzi k (jako podprostor), je $|C| = q^k$. Parametry lineárních kódů se uvádějí v hranatých závorkách: $[n, k, d]$-kód je automaticky lineární.

Jednou z výhod lineárních kódů je úsporný popis: namísto q^k prvků kódu C stačí uvést k prvků nějaké jeho báze. Obvyklým tvarem této informace je *generující matice* kódu C, tedy matice, jejíž řádky tvoří jeho bázi (je to tedy matice o rozměrech $k \times n$). Jednou z generujících matic kódu $\mathcal{H}$ je například matice

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{3.1}$$

Hammingova vzdálenost v lineárních kódech je ‘invariantní k posunutí’, tj. pro $x, y, z \in C$ platí

$$d(x, y) = d(x + z, y + z).$$

Speciálně pro $z = -x$ z této rovnosti plyne, že pro určení minimální vzdálenosti $\Delta(C)$ kódu C stačí uvažovat dvojice slov obsahující nulový vektor. Definujeme-li tedy *váhu* $w(x)$ slova x jako počet nenulových souřadnic (tedy $w(x) = d(x, 0)$), platí

$$\Delta(C) = \min_{x \in C} w(x).$$

V prostoru $\mathbb{F}_q^n$ je definován *skalární součin*, a to předpisem

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i,$$

kde $x = (x_1 \dots x_n)$ a $y = (y_1 \dots y_n)$ jsou prvky prostoru $\mathbb{F}_q^n$. Označení skalární součin není úplně přesné, protože standardní definice skalárního součinu vyžaduje, aby pro $x \neq 0$ bylo $\langle x, x\rangle \neq 0$. V našem případě tomu tak nemusí být. Například pro prvek $x = (1100)$ prostoru $\mathbb{F}_2^4$ je $\langle x, x\rangle = 0$ (a je tomu tak pro každý vektor se sudým počtem jedniček).

Duální kód k lineárnímu kódu C je jeho *ortogonální doplněk*, tedy podprostor

$$C^\perp = \{x \,:\, \langle x, y\rangle = 0 \text{ pro každé } y \in C\}.$$

Díky nestandardní povaze našeho skalárního součinu nás může zprvu překvapit, že průnik $C \cap C^\perp$ obecně nemusí být prázdný (jako by tomu bylo u 'opravdového' skalárního součinu). Na druhou stranu i zde platí důležitá vlastnost ortogonálního doplňku (viz cvičení 3.1.1):

$$\dim C^\perp = n - \dim C. \tag{3.2}$$

Generující matice M duálního kódu $C^\perp$ se nazývá *paritní* (nebo *kontrolní*) *matice* kódu C. 'Kontrolní' proto, že její řádky určují lineární rovnice, které musí každé slovo kódu C splňovat (a naopak, každý vektor, který je splňuje, je slovem kódu C). V řeči soustav lineárních rovnic:

$$C = \{x \,:\, M \cdot x = 0\}. \tag{3.3}$$

Generující matice libovolného lineárního kódu C se dá Gaussovou eliminací uvést do tvaru, ve kterém prvních k sloupců tvoří jednotkovou podmatici. Řádky výsledné matice nadále tvoří bázi kódu C. Z tohoto tvaru matice je vidět, že předepíšeme-li slovo $c \in \mathbb{F}_q^k$ délky k, pak existuje právě jedno kódové slovo z kódu C, které má na prvních k souřadnicích právě slovo c. Kódy s touto vlastností (ať jsou lineární nebo ne) se nazývají *systematické* na souřadnicích $1, \dots, k$. O prvních k symbolech každého kódového slova pak mluvíme jako o *informačních symbolech* (nesou informaci), o zbylých symbolech jako o *kontrolních* nebo *paritních symbolech*.

Cvičení

▶ **3.1.1.** Dokažte, že pro lineární kód délky n nad $\mathbb{F}_q$ platí

$$\dim C + \dim C^\perp = n.$$

3.2 Dekódování lineárních kódů

Popíšeme algoritmus pro dekódování libovolného lineárního kódu. Jak uvidíme později, pro konkrétní lineární kódy mohou existovat speciální efektivnější algoritmy.

Mějme lineární kód C délky n nad tělesem $\mathbb{F}_q$. Dejme tomu, že po odeslání slova $x \in C$ bylo přijato slovo $\tilde{x} \in \mathbb{F}_q^n$. Při přenosu mohly nastat nějaké chyby, které zachycuje *chybový vektor* $e = \tilde{x} - x$. Příjemce zná pouze slovo $\tilde{x}$ a chce najít kódové slovo y, které je slovu $\tilde{x}$ nejblíže.

Nechť P je paritní matice kódu C. *Syndrom* slova $z \in \mathbb{F}_q^n$ je součin $P \cdot z^T$. Kódová slova kódu C jsou (z definice paritní matice) právě slova s nulovým syndromem. Z toho plyne, že dvě slova jsou ve stejné třídě modulo podprostor C právě tehdy, když mají stejný syndrom. Dále platí $\tilde{x} - e = x \in C$, takže neznámé slovo e a známé slovo $\tilde{x}$ patří do stejné třídy. Dekódování je založeno na předpokladu, že chybový vektor je slovo s nejmenší vahou ve své třídě. K nalezení takového slova slouží předem připravená tabulka, která pro každý syndrom s udává (některé) slovo $m(s)$ s minimální vahou ve třídě slov se syndromem s. Toto slovo se označuje jako *reprezentant* své třídy.

Pro přijaté slovo $\tilde{x}$ je chybovým vektorem (podle odhadu tabulky) slovo $m(P \cdot \tilde{x}^T)$. Výsledkem dekódování je tedy slovo

$$y = \tilde{x} - m(P \cdot \tilde{x}^T).$$

Slovo y má mezi všemi kódovými slovy nejmenší vzdálenost od slova $\tilde{x}$. Má-li kód C minimální vzdálenost aspoň $2t + 1$, pak za předpokladu, že při přenosu došlo nejvýše k t chybám, je dekódování podle našeho algoritmu úspěšné.

Nevýhodou je nutnost udržovat tabulku reprezentantů. Je-li $\dim C = k$, pak počet tříd modulo C je 2^{n-k}, takže velikost tabulky může být exponenciální v n.

Příklad 3.2.1. Uvažme binární lineární kód C s generující maticí

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

Jedná se o $[5, 2, 3]$-kód. (Obsahuje jen 4 slova, takže minimální vzdálenost není problém určit.) Jak zjistíme vyřešením soustavy rovnic $M \cdot z^T = 0$, jedna paritní matice má tvar

$$M^\perp = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Následující tabulka uvádí pro každý z 2^3 možných syndromů reprezentanta příslušné třídy a pro úplnost i ostatní slova. K dekódování ovšem stačí znát reprezentanty.

syndrom	**reprezentant**	ostatní slova
000	**00000**	11100 00111 11011
001	**00001**	11101 00110 11010
010	**00100**	11000 00011 11111
011	**00010**	11001 00101 11110
100	**10000**	01100 10111 01011
101	**01010**	10001 01101 10110
110	**01000**	10100 10011 01111
111	**01001**	10101 10010 01110

Všimněme si, že u syndromu 000 jsou uvedena právě slova kódu C. U syndromů 101 a 111 je možná i jiná volba reprezentanta.

Dekódujme např. přijaté slovo $\tilde{x} = 00101$. Jeho syndrom je $M^{\perp} \cdot \tilde{x}^T = 011$. Reprezentantem příslušné třídy je slovo 00010. Vyvozujeme, že k chybě došlo ve čtvrté pozici a dekódujeme na slovo 00111.

Je-li přijaté slovo 01101, zjišťujeme syndrom 101, pro který je reprezentantem slovo 01010. Jeho váha je 2, takže v příslušné třídě neexistuje slovo váhy 1. Při přenosu tak muselo dojít alespoň k dvěma chybám! V daném případě jsme schopni alespoň detekovat, že na opravu chyb náš kód (s minimální vzdáleností pouze 3) nestačí. □

3.3 Hammingovy kódy

Vraťme se k naší otázce o hodnotě funkce $A(n, d)$, která udává maximální velikost binárního kódu délky n s minimální vzdáleností d. Zatím jsme určili její hodnoty pro $d \leq 2$, ale viděli jsme jen jediný kód s minimální vzdáleností 3, totiž kód $\mathcal{H}$. V tomto oddílu sestrojíme nekonečnou třídu *lineárních* binárních kódů s minimální vzdáleností rovnou 3, souhrnně označovaných jako Hammingovy kódy. Díky své minimální vzdálenosti mají tyto kódy schopnost opravovat jednu přenosovou chybu. Každý z nich je navíc největším možným kódem s danou délkou a minimální vzdáleností, a určuje tak pro příslušné n hodnotu funkce $A(n, 3)$.

Podívejme se nejprve na překvapivý vztah mezi kontrolní maticí M lineárního kódu C a jeho minimální vzdáleností $\Delta(C)$. Jednou z interpretací rovnosti (3.3) je, že každé slovo $x = (x_1 \dots x_n) \in C$ určuje nulovou lineární kombinaci sloupců $s_1, \dots, s_n$ matice M, totiž

$$\sum_{i=1}^{n} x_i s_i = 0.$$

Počet nenulových sčítanců je roven váze slova x. Pokud je tedy každých (řekněme) d sloupců matice M lineárně nezávislých, pak C neobsahuje slova váhy d. Jak víme, minimální váha (nenulového) slova $x \in C$ je rovna minimální vzdálenosti $\Delta(C)$. Dostáváme následující pozorování.

Pozorování 3.3.1 (O minimální vzdálenosti)**.** *Nechť M je kontrolní matice lineárního kódu C. Pak minimální vzdálenost $\Delta(C)$ je rovna největšímu číslu d, pro které platí, že každých $d-1$ sloupců matice M je lineárně nezávislých.* □

Chceme-li zkonstruovat co největší binární kódy s minimální vzdáleností rovnou 3, stačí zkonstruovat matice nad $\mathbb{F}_2$, které neobsahují lineárně závislé dvojice sloupců a rozdíl mezi počtem sloupců a počtem řádků (tj. dimenze konstruovaného kódu) je co největší. To je naštěstí jednoduché, protože dva vektory jsou lineárně závislé nad $\mathbb{F}_2$, právě když jsou shodné nebo jeden z nich je nulový. Takže bude-li naše matice M mít dejme tomu r řádků, můžeme jako její sloupce zvolit všech $2^r - 1$ nenulových vektorů v prostoru $\mathbb{F}_2^r$ (každý z nich použijeme jednou). Kód $\mathcal{H}_r$ s generující maticí M má délku $n = 2^r - 1$ a podle (3.2) je jeho dimenze

$$\dim \mathcal{H}_r = n - r = 2^r - r - 1. \tag{3.4}$$

Kódům $\mathcal{H}_r$ (a ekvivalentním) se říká *Hammingovy kódy*. Všimněme si, že jsme nespecifikovali pořadí sloupců v kontrolní matici. To ale nevadí, neboť pro jiné pořadí dostaneme ekvivalentní kód (viz cvičení 3.3.3). Minimální vzdálenost každého Hammingova kódu je 3. Platí tedy:

Věta 3.3.2. *Pro každé $r \geq 2$ má Hammingův kód $\mathcal{H}_r$ parametry $[2^r - 1, 2^r - r - 1, 3]$.* □

Hammingovy kódy lze definovat i nad tělesem $\mathbb{F}_q$ (viz cvičení 3.3.4).

Cvičení

► **3.3.1.** Ukažte, že kód $\mathcal{H}$ z oddílu 1.3 je Hammingův kód $\mathcal{H}_3$. Jak vypadá kód $\mathcal{H}_2$?

► **3.3.2.** Ukažte, že sloupce kontrolní matice Hammingova kódu o délce $2^r - 1$ jsou tvořeny binárními zápisy všech čísel od 1 do $2^r - 1$.

► **3.3.3.** Ukažte, že dva lineární kódy, jejichž kontrolní matice se liší jen pořadím řádků a sloupců, jsou ekvivalentní. Dokažte obdobné tvrzení pro generující matice.

► **3.3.4.** Definujte obdobu Hammingových kódů nad tělesem $\mathbb{F}_q$. Tyto kódy mají parametry $[n, n-r, 3]$, kde $r \geq 2$ a $n = (q^r - 1)/(q - 1)$.

3.4 Dekódování Hammingových kódů

Použijeme-li pro dekódování Hammingova kódu $\mathcal{H}_r$ obecný algoritmus pro lineární kódy, vystačíme s poměrně malou tabulkou reprezentantů tříd. Počet tříd je totiž

$$2^{n-k} = 2^{2^r-1-2^r+r+1} = 2^r = n + 1,$$

zatímco v obecném případě může být i exponenciální v n.

Věc je ale ještě jednodušší: tabulku reprezentantů vůbec nepotřebujeme. Podle cvičení 3.3.2 sloupce paritní matice P kódu $\mathcal{H}_r$ tvoří binární zápisy všech čísel od 1 do $2^r - 1$. Po přechodu k ekvivalentnímu kódu (permutaci pozic) můžeme předpokládat, že jsou uspořádány v tomto pořadí — viz cvičení 3.4.2. Hammingovy kódy mají minimální vzdálenost 3, proto při jejich dekódování předpokládáme, že při přenosu došlo nejvýše k jedné chybě (jinak na správné dekódování ani neaspirujeme). Předpokládáme tedy, že váha chybového vektoru e je ≤ 1. Jaký je syndrom takového slova?

Je-li $e = 0$, je syndrom nulový. Má-li e jedničku právě na i-té pozici, potom $P \cdot e^T$ je i-tý sloupec matice P, tedy v daném případě binární zápis čísla i.

Z oddílu 3.2 víme, že e a přijaté slovo $\tilde{x}$ mají stejný syndrom. Lze tedy dekódovat následovně. Je-li syndrom přijatého slova nulový, dekódujeme $\tilde{x}$ na $\tilde{x}$. Pokud je binárním zápisem nenulového čísla i, změníme i-tý bit slova $\tilde{x}$ a ostatní bity ponecháme. Došlo-li k nejvýše jedné přenosové chybě, je výsledek dekódování správný.

Cvičení

► **3.4.1.** Nechť P je paritní matice binárního kódu C. Dejme tomu, že při přenosu, jehož výsledkem je slovo $\tilde{x}$, došlo k chybám na pozicích $i_1, \ldots, i_m$. Jaký je vztah syndromu $P \cdot \tilde{x}^T$ a sloupců matice P?

► **3.4.2.** Kód $\mathcal{H}$ má generující matici (3.1).

(a) Odpovídají sloupce nějaké jeho paritní matice po řadě binárním zápisům čísel $1, 2, \ldots, 7$?

(b) Najděte ekvivalentní kód $\mathcal{H}'$, pro který tomu tak je. Vypište všechna jeho kódová slova.

(c) Pro kód $\mathcal{H}'$ pomocí algoritmu z tohoto oddílu dekódujte slova (1001110) a (0100010).

Kapitola 4

Perfektní kódy

4.1 Hammingův odhad

Má-li binární kód C délky n minimální vzdálenost $\Delta(C) \geq 2t+1$, pak pro každé slovo $x \in \mathbb{F}_2^n$ existuje nejvýše jedno kódové slovo ve vzdálenosti $\leq t$ od x. Jinými slovy, tzv. *(kombinatorické) koule* se středem x a poloměrem t,

$$B(x,t) = \{z \in \mathbb{F}_2^n \,:\, d(x,z) \leq t\},$$

jsou pro různá $x \in C$ disjunktní.

Odtud snadno dostaneme dostáváme horní odhad na velikost takového kódu. Kolik prvků obsahuje koule $B(x,t)$? Počet prvků ve vzdálenosti i od středu x je právě $\binom{n}{i}$ (vybíráme neuspořádanou i-tici souřadnic, ve kterých x změníme). Takže

$$|B(x,t)| = \sum_{i=0}^{t} \binom{n}{i}. \tag{4.1}$$

Tuto hodnotu nazveme *objem koule* $B(x,t)$ a označíme $V(n,t)$ (protože nezávisí na středu x, ale naopak závisí na n). Potom

Věta 4.1.1 (Hammingův odhad)**.** *Pro binární kód o minimální vzdálenosti alespoň* $2t+1$ *platí*

$$|C| \leq \frac{2^n}{V(n,t)}.$$

Důkaz. V množině $\mathbb{F}_2^n$ o 2^n prvcích je $|C|$ disjunktních koulí, z nichž každá má objem $V(n,t)$. □

Binární kód je *perfektní*, pokud pro něj platí rovnost v Hammingově odhadu (a má tedy právě $2^n/V(n,t)$ prvků). *Triviální* perfektní kódy jsou (viz cvičení 4.1.1):

- totální kód $\mathbb{F}_2^n$,
- opakovací kód liché délky,

- jednoprvkový kód $\{x\}$, kde $x \in \mathbb{F}_2^n$.

Vedle těchto triviálních příkladů existují i další perfektní kódy. Mezi nimi jsou i všechny Hammingovy kódy. Kód $\mathcal{H}_r$ má parametry $(2^r - 1, 2^r - r - 1, 3)$. Pro tyto hodnoty dostáváme

$$V(n,t) = V(2^r - 1, 1) = 2^r,$$

takže $2^n/V(n,t) = 2^{n-r} = 2^{2^r-r-1}$, což je přesně počet prvků kódu $\mathcal{H}_r$. Tím je jeho perfektnost dokázána.

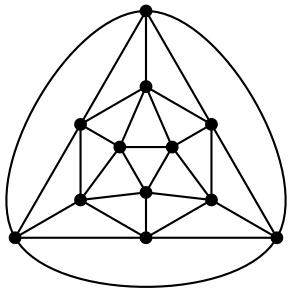
Cvičení

► **4.1.1.** Ověřte, že následující binární kódy jsou perfektní: totální kód $\mathbb{F}_2^n$, opakovací kód liché délky a jednoprvkový kód.

4.2 Binární Golayův kód

Existuje jen jediný netriviální perfektní binární kód s minimální vzdáleností alespoň 5. Je to slavný *Golayův kód*, objevený M. Golayem [3] v roce 1949. Tento kód má dosti překvapivé parametry: $(23, 12, 7)$. Dá se zkonstruovat mnoha způsoby, z nichž nejjednodušší si teď ukážeme.

Rovinný graf na obr. 4.1 je *dvacetistěn*, jeden z pěti rovinných grafů, ve kterých mají všechny vrcholy stejný stupeň a všechny stěny stejnou velikost[1]. Každý vrchol dvacetistěnu má 5 sousedů a každé dva vrcholy mají 0 nebo 2 společné sousedy. To lze snadno nahlédnout s pomocí následujícího lemmatu. Připomeňme, že *automorfismus* grafu $G = (V, E)$ je bijekce $\alpha : V \to V$ s vlastností, že pro každé dva vrcholy $x, y \in V$ je $xy \in E$ právě když $\alpha(x)\alpha(y) \in E$.



Obrázek 4.1: Dvacetistěn.

[1]Každý z těchto grafů odpovídá jednomu z tzv. *platónských těles*, mezi něž patří čtyřstěn, krychle, osmistěn, dvanáctistěn a dvacetistěn.

Lemma 4.2.1. *Nechť x, x', y, y' jsou vrcholu dvanáctistěnu D, pro které platí $d(x, y) = d(x', y')$. Potom existuje automorfismus α grafu D, který zobrazuje x na x' a y na y'.*

Důkaz. Cvičení 4.2.1. □

Automorfismus zachovává sousednost a nesousednost. Chceme-li tedy ukázat, že každé dva vrcholy mají 0 nebo 2 společné sousedy, stačí probrat tři případy: dvojici vrcholů ve vzdálenosti 1, 2 resp. 3.

Nechť V je množina všech vrcholů dvacetistěnu a E množina všech jeho hran. Pro každý vrchol $v \in V$ uvažme ještě jednu jeho kopii v^* a definujme V^* jako množinu všech těchto kopií. Každému vrcholu $v \in V$ přiřadíme množinu $C_v \subset V \cup V^*$ předpisem

$$C_v = \{v\} \cup \{w^* : vw \notin E\}.$$

Lineární binární kód délky 24 generovaný 12 charakteristickými vektory množinového systému $\{C_v : v \in V\}$ se nazývá *rozšířený binární Golayův kód* $\mathcal{G}_{24}$. Všimněme si, že pro každý vrchol v je $|C_v| = 8$. Ukážeme, že to je $(24, 12, 8)$-kód. Začneme prozkoumáním duálního kódu ${\mathcal{G}_{24}}^{\perp}$.

Dvě různá slova C_v, $C_w \in \mathcal{G}_{24}$ se liší jednak v 'souřadnicích' v a w, a jednak v souřadnicích odpovídajících vrcholům sousedícím s právě jedním z vrcholů v a w. Těch je 10 nebo 6, podle toho, zda v a w mají 0 nebo 2 společné sousedy. Každopádně se C_v a C_w liší v sudém počtu vrcholů. Tím pádem je $|C_v \cap C_w|$ sudé, takže

$$\langle C_v, C_w \rangle = 0. \tag{4.2}$$

Každé dva z generujících vektorů C_v jsou tedy navzájem ortogonální. Z bilinearity skalárního součinu ale plyne, že toto tvrzení platí pro každé dvě kódová slova:

Lemma 4.2.2. *Nechť má lineární kód C (nad tělesem F) bázi, v níž jsou každé dva vektory navzájem ortogonální. Potom platí $C \subset C^{\perp}$.*

Důkaz. Vezměme libovolné slovo $c \in C$ a vyjádřeme je jako lineární kombinaci $c = \sum \alpha_b \cdot b$, kde koeficienty α_b jsou prvky základního tělesa a b probíhá uvažovanou bázi B. Chceme ukázat, že skalární součin vektoru c s libovolným vektorem $c' \in C$ je nulový. Vyjádřeme tedy rovněž $c' = \sum \alpha'_{b'} \cdot b'$. Z bilinearity skalárního součinu je

$$\langle c, c' \rangle = \sum_{b,b' \in B} \alpha_b \cdot \alpha'_{b'} \cdot \langle b, b' \rangle = 0.$$

Proto $c \in C^{\perp}$ a také $C \subset C^{\perp}$. □

Platí tedy $\mathcal{G}_{24} \subset {\mathcal{G}_{24}}^{\perp}$! Ovšem protože dimenze kódu $\mathcal{G}_{24}$ i jeho duálu je 12, musí platit

$${\mathcal{G}_{24}}^{\perp} = \mathcal{G}_{24}. \tag{4.3}$$

Náš kód je tedy svým vlastním duálem, je *samoduální*.

Tvrzení 4.2.3. *Nechť C je samoduální binární kód, v jehož bázi má každé slovo váhu dělitelnou 4. Pak váha každého slova kódu C je násobkem 4.*

Důkaz. Pro libovolné vektory $u, v \in C$ platí

$$|u+v| = |u| + |v| - 2|u \cap v| \equiv |u| + |v| - 2\langle u, v\rangle \pmod 4. \tag{4.4}$$

V samoduálním kódu je ale $\langle u, v\rangle = 0$, takže váha součtu vektorů je modulo 4 rovna součtu jejich vah. Každý vektor z C je součtem bázových vektorů a má tedy váhu dělitelnou 4. □

Toto tvrzení je pro nás velmi výhodné. Chceme-li totiž ukázat, že minimální vzdálenost kódu $\mathcal{G}_{24}$ je alespoň 8, pak nám stačí ověřit, že neobsahuje slova o váze 4. Dejme tomu, že $c \subset V \cup V^*$ má váhu 4, přičemž $c = \sum_{v\in Y} C(v)$ a množina Y má k prvků ($k \in \{2, 3, 4\}$). Pak c nutně obsahuje právě $4-k$ prvků V^*, takže právě $4-k$ vrcholů dvacetistěnu má v Y lichý počet nesousedů — jinak řečeno, vrcholů, jejichž počet sousedů v Y má jinou paritu než k, je přesně $4-k$.

Uvažme případ $k = 2$. Ze cvičení 4.2.2 víme, že prvky Y mají 0 nebo 2 společné sousedy, a ani s jedním z nich pak nesousedí 2 resp. 6 vrcholů. S lichým počtem vrcholů v Y tak sousedí 10 resp. 4 vrcholy, což je spor. Případy $k = 3, 4$ nejsou o mnoho složitější a ponecháváme je jako cvičení 4.2.3. Dokázali jsme následující větu.

Věta 4.2.4. *Rozšířený Golayův kód $\mathcal{G}_{24}$ je $(24, 12, 8)$-kód.*

Pokud odstraníme z kódu $\mathcal{G}_{24}$ libovolnou souřadnici, dostaneme *Golayův kód* $\mathcal{G}_{23}$. Výsledek nezávisí na výběru odstraňované souřadnice (důkaz nebudeme provádět). Je jasné, že $\mathcal{G}_{23}$ je $(23, 12, 7)$-kód. Vzhledem k tomu, že

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{23-12},$$

jde o perfektní kód.

Cvičení

► **4.2.1.** Dokažte lemma 4.2.1.

► **4.2.2.** Ukažte, že každé dva vrcholy dvanáctistěnu mají 0 nebo 2 společných sousedů.

► **4.2.3.** Ukažte podrobně, že kód $\mathcal{G}_{24}$ neobsahuje slova o váze 4.

4.3 Váhový polynom perfektního kódu

Odbočme nyní na chvíli od Golayových kódů k tématu společnému všem perfektním kódům. Ukážeme, že pokud C je perfektní $[n, k, d]$-kód obsahující nulové slovo, lze z čísel n a d bezezbytku určit jeho váhový polynom (viz oddíl 15.1). Obecný princip budeme ilustrovat na příkladu Hammingova kódu $\mathcal{H}_3$.

Věta 4.3.1. *Binární $[7, 4, 3]$-kód C obsahující nulové slovo má váhový polynom*

$$P_C(x) = 1 + 7x^3 + 7x^4 + x^7.$$

Důkaz. Nechť $P_C(x) = \sum_{i=0}^{7} A_i x^i$. Víme, že $A_0 = 1$ a $A_1 = A_2 = 0$. Uvažme kouli $B(z, 1)$ se středem v nějakém kódovém slově $z \in C$ váhy m. Slova v kouli $B(z, 1)$ mají váhu mezi $m - 1$ a $m + 1$. Každé ze slov váhy $m - 1$ dostaneme změnou jedné z m jedniček slova z na nulu. Z malého zobecnění této úvahy plyne:

$$B(z,1) \text{ obsahuje } \begin{cases} m & \text{slov váhy } m-1, \\ 1 & \text{slovo váhy } m, \\ 7-m & \text{slov váhy } m+1. \end{cases} \tag{4.5}$$

Zaměřme se nyní na množinu J, tvořenou slovy z množiny $\mathbb{F}_2^n$ o dané váze j. Průniky $J \cap B(z, 1)$, kde z probíhá *perfektní* kód C, tvoří rozklad množiny J. Podle (4.5) je

$$|B(z,1) \cap J| = \begin{cases} j+1 & \text{pokud } |z| = j+1, \\ 1 & \text{pokud } |z| = j, \\ 7-j+1 & \text{pokud } |z| = j-1. \end{cases}$$

Protože $|J| = \binom{7}{j}$, dostáváme následující rovnici:

$$\binom{7}{j} = (8-j) \cdot A_{j-1} + A_j + (j+1) \cdot A_{j+1}, \tag{4.6}$$

kde $j = 1, \ldots, 6$. První neznámý koeficient, A_3, spočítáme z rovnice (4.6) pro $j = 2$:

$$21 = \binom{7}{2} = 6A_1 + A_2 + 3A_3,$$

a tedy $A_3 = 7$. Pro $j = 3$ dostaneme $A_4 = 7$, pro větší j pak $A_5 = A_6 = 0$ a $A_7 = 1$. □

Stejnou metodou lze spočítat i váhové polynomy ostatních perfektních kódů. Pro kód s parametry Golayova kódu $\mathcal{G}_{23}$ například platí následující věta, která se nám v oddílu 15.2 bude hodit k důkazu jednoznačnosti Golayova kódu $\mathcal{G}_{24}$.

Věta 4.3.2. *Binární $(23, 12, 7)$-kód C obsahující nulové slovo má váhový polynom*

$$P_C(x) = 1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}.$$

Důkaz. Cvičení 4.3.2. □

Cvičení

► **4.3.1.** Jaké další váhové polynomy dostaneme ve větě 4.3.1, pokud nebudeme požadovat, aby daný kód obsahoval nulové slovo?

Řešení: Pouze $x + 3x^2 + 4x^3 + 4x^4 + 3x^5 + x^6$.

► **4.3.2.** (a) Nechť $z \in \mathbb{F}_q^n$ je slovo váhy m. Kolik slov dané váhy j obsahuje koule $B(z, r)$, kde $m-r \leq j \leq m+r$? Výsledek bude záviset na parametrech n, m, r a q.

Řešení: $\sum_{t=0}^{\min\{j,(r-m+j)/2\}} (q-1)^t \binom{m}{j-t}\binom{n-m}{t}$.

(b) Dokažte větu 4.3.2.

► **4.3.3.** Určete váhový polynom ternárního $(11, 6, 5)$-kódu, který obsahuje nulové slovo.

4.4 Ternární Golayovy kódy

Vedle binárních Golayových kódů existují ještě *ternární Golayovy kódy* $\mathcal{G}_{12}$ a $\mathcal{G}_{11}$. Kód $\mathcal{G}_{12}$ je určen např. generující maticí

$$\left(\begin{array}{cccccc|cccccc} 1&0&0&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&0&0&1&0&1&-&-&1\\ 0&0&1&0&0&0&1&1&0&1&-&-\\ 0&0&0&1&0&0&1&-&1&0&1&-\\ 0&0&0&0&1&0&1&-&-&1&0&1\\ 0&0&0&0&0&1&1&1&-&-&1&0 \end{array}\right).$$

Je to samoduální $[12, 6, 6]$-kód a dá se ukázat, že každý ternární kód s parametry $(12, 6, 6)$ je kódu $\mathcal{G}_{12}$ ekvivalentní. Kód $\mathcal{G}_{11}$, který vznikne propíchnutím kódu $\mathcal{G}_{12}$ na libovolné pozici, je perfektní $[11, 6, 5]$-kód.

Zakončeme tuto kapitolu hlubokou větou o perfektních kódech. (Připomeňme, že triviální perfektní kódy jsou definovány v oddílu 4.1.)

Věta 4.4.1 (Tietäväinen a van Lint)**.** *Netriviální perfektní kód nad libovolným tělesem je buď Golayův kód, nebo má stejné parametry (n, k, d) jako některý Hammingův kód.*

(Poznamenejme, že jsou známy nelineární perfektní kódy s parametry Hammingových kódů, například libovolného binárního Hammingova kódu $\mathcal{H}_r$ pro $r \geq 4$.)

Kapitola 5

Algebraické intermezzo 2

5.1 Podgrupy

Podgrupa grupy G je libovolná grupa H, kde $H \subset G$ a grupová operace v grupě H je zúžením operace v grupě G na množinu H. Tento vztah zapisujeme $H \leq G$. *Řád* $|G|$ grupy G je velikost množiny G.

Věta 5.1.1 (Lagrange)**.** *Je-li H podgrupa konečné grupy G, pak $|H|$ dělí $|G|$.*

Důkaz. Cvičení 5.1.2. □

Podgrupa grupy G *generovaná* prvkem $a \in G$ je grupa $\langle a \rangle$ definovaná vztahem

$$\langle a \rangle = \{a^i \,:\, i \in \mathbb{N}\}.$$

Grupa G je *cyklická*, pokud pro nějaké $c \in G$ platí $G = \langle c \rangle$. *Řád prvku $a \in G$*, označovaný $\operatorname{ord} a$, je nejmenší přirozené k s vlastností, že $a^k = 1$ (nebo ∞, pokud takové k neexistuje).

Pozorování 5.1.2. *Pro $a \in G$ platí*

$$\operatorname{ord} a = |\langle a \rangle|.$$

Důkaz. Uvažme posloupnost

$$1, a, a^2, a^3, \ldots$$

a nejmenší k, pro které je a^k rovno některému předcházejícímu prvku a^i $(i < k)$. Z rovnosti $a^k = a^i$ plyne $a^{k-i} = 1$. takže z minimality k musí být $i = 0$. To znamená, že $k = \operatorname{ord} a$. Na druhou stranu je zjevné, že $\langle a \rangle = \{1, a, \ldots, a^{k-1}\}$. □

Důsledek 5.1.3. *Je-li grupa G konečná, pak pro každý prvek $a \in G$ platí*

(i) $a^k = 1$*, právě když* $\operatorname{ord} a$ *dělí* k*,*

(ii) $a^{|G|} = 1$*.*

Důkaz. (i) Nechť $k = l \cdot \operatorname{ord} a + r$, kde $0 \leq r < \operatorname{ord} a$. Potom

$$a^k = (a^{\operatorname{ord} a})^l \cdot a^r = 1 \cdot a^r = a^r.$$

Protože $r < \operatorname{ord} a$, tento výraz je roven 1, právě když $r = 0$ (a tedy k je dělitelné $\operatorname{ord} a$). (ii) Cvičení 5.1.3. □

Důsledek 5.1.4 (Malá Fermatova věta)**.** *Nechť a je přirozené číslo a p prvočíslo, které nedělí a. Potom*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Důkaz. Plyne přímo z důsledku 5.1.3(ii), aplikovaného na grupu $(\mathbf{Z}_p - \{0\}, \cdot)$. □

Cvičení

▶ **5.1.1.** Ukažte, že v grupě $(M, *)$ existuje jen jeden neutrální prvek a že každé $a \in M$ má jen jediný inverzní prvek.

▶ **5.1.2.** Dokažte větu 5.1.1.

▶ **5.1.3.** Dokažte důsledek 5.1.3(ii).

5.2 Charakteristika tělesa

Kromě násobení dvou prvků tělesa můžeme definovat součin $k \times a$, kde $k \in \mathbb{N}$ a $a \in F$, a to předpisem

$$k \times a = a + a + \cdots + a \qquad (k \text{ krát}).$$

Charakteristika $\operatorname{char}(F)$ tělesa F je nejmenší k, pro které platí $k \times 1 = 0$ (pokud takové k neexistuje, definujeme $\operatorname{char}(F) = \infty$).

Pozorování 5.2.1. *Charakteristika konečného tělesa F je prvočíslo.*

Důkaz. Cvičení 5.2.1. □

K tělesům patří například množina racionálních, reálných nebo komplexních čísel s obvyklými operacemi sčítání a násobení. Standardním příkladem konečného tělesa je těleso $\mathbb{F}_p$ (kde p je prvočíslo), což je množina $\{0, 1, \ldots, p-1\}$ se sčítáním a násobením modulo p.

Dvě grupy nebo tělesa, která mají různé prvky, ale jejich operace se však až na 'přeznačení prvků' shodují, lze považovat za identická. Přesnou formulaci umožňuje pojem isomorfismu. *Isomorfismus grup* $(G, +)$ a $(G', \oplus)$ je bijekce $f : G \to G'$, která zobrazuje neutrální prvek na neutrální prvek a splňuje pro $a, b \in G$ podmínku $f(a + b) = f(a) \oplus f(b)$.

Isomorfismus těles $(F, +, \cdot)$ a $(F', \oplus, \odot)$ je bijekce $h : F \to F'$, která je isomorfismem grup $(F, +)$ a $(F', \oplus)$ a indukuje isomorfismus grup $(F - \{0\}, \cdot)$ a $(F' - \{0\}, \odot)$. Dvě grupy nebo tělesa jsou *isomorfní*, pokud mezi nimi existuje isomorfismus.

Podobně jako podgrupy lze definovat podtělesa. Těleso F' je *podtělesem* tělesa F, pokud $F' \subset F$ a operace v tělese F' jsou zúžením operací v tělese F.

Tvrzení 5.2.2. *Nechť F je konečné těleso charakteristiky p. Potom*

(i) F obsahuje podtěleso isomorfní s $\mathbb{F}_p$,

(ii) $|F| = p^m$ pro nějaké přirozené $m \geq 1$.

Důkaz. (i) Nechť $F' = \{k \times 1 : k \in \mathbb{N}\}$. Množina F' je uzavřená na operace $+$ a $\cdot$ i na inverzní prvky vzhledem k těmto operacím a je tedy tělesem. Navíc je snadné najít isomorfismus s tělesem $\mathbb{F}_p$.

(ii) Těleso F můžeme nahlížet jako vektorový prostor nad tělesem F': $(F, +)$ je abelovská grupa a součin prvku $a \in F$ s prvkem λ tělesa F' definujeme přirozeně jako jejich součin v rámci tělesa F. Ovšem počet prvků vektorového prostoru F nad p-prvkovým tělesem je p^m, kde m je jeho dimenze (neboť každý prvek lze jednoznačně zapsat jako lineární kombinaci m prvků nějaké pevně zvolené báze). □

Z pozorování 5.2.1 a tvrzení 5.2.2 plyne, že počet prvků libovolného konečného tělesa je mocnina prvočísla. Můžeme se ptát, zda naopak platí, že pro každé prvočíslo p a přirozené číslo m existuje těleso s p^m prvky. Odpověď je kladná a k jejímu důkazu se dostaneme v následujícím odstavci.

Cvičení

▶ **5.2.1.** Dokažte pozorování 5.2.1.

5.3 Existence konečných těles

Nechť $f(x)$ je libovolný polynom stupně k nad tělesem $\mathbb{F}_p$. Uvažme množinu všech polynomů v proměnné α nad $\mathbb{F}_p$ stupně menšího než k. Definujme na této množině sčítání a násobení jako obvyklé sčítání a násobení polynomů, prováděné 'modulo $f(\alpha)$' (výsledek každé operace tedy nahrazujeme zbytkem při dělení polynomem $f(\alpha)$). Označme výslednou strukturu symbolem $\mathbb{F}_p[\alpha]/f$.

Pozorování 5.3.1. *$\mathbb{F}_p[\alpha]/f$ je komutativní okruh.*

Důkaz. Cvičení 5.3.1. □

Polynom $f(x)$ nad tělesem F nenulového stupně je *ireducibilní*, pokud neexistují polynomy $g_1(x)$, $g_2(x)$ menšího stupně tak, že $f = g_1 g_2$.

Ireducibilitu daného polynomu lze snadno ověřit kontrolou, zda je dělitelný některým polynomem menšího stupně. Například pro $F = \mathbb{F}_2$ zjistíme, že ireducibilní jsou následující polynomy stupně ≤ 3:

stupeň	polynom
1	x
	$x+1$
2	x^2+x+1
3	x^3+x+1
	x^3+x^2+1

Oproti tomu například polynom x^2+1 ireducibilní není, protože nad tělesem $\mathbb{F}_2$ platí

$$x^2+1 = (x+1)^2.$$

Je-li f ireducibilní polynom nad $\mathbb{F}_p$, lze pozorování 5.3.1 zesílit:

Věta 5.3.2. *Nechť $f(x)$ je ireducibilní polynom nad tělesem $\mathbb{F}_p$. Potom okruh $\mathbb{F}_p[\alpha]/f$ je těleso.*

Důkaz. Stačí ukázat, že k nenulovému prvku $g(\alpha) \in \mathbb{F}_p[\alpha]/f$ existuje inverzní prvek. Uvažme množinu všech součinů $g(\alpha)h(\alpha)$, kde $h(\alpha)$ probíhá $\mathbb{F}_p[\alpha]/f$. Jsou-li všechny tyto součiny různé, je jich právě tolik jako polynomů stupně menšího než je stupeň polynomu f, takže mezi nimi musí být polynom 1. Polynom $h(\alpha)$, pro který je $g(\alpha)h(\alpha) \equiv 1 \pmod{f(\alpha)}$, je pak inverzním prvkem k polynomu $g(\alpha)$.

Můžeme tedy předpokládat, že dva z uvažovaných součinů jsou stejné, tedy

$$g(\alpha)h_1(\alpha) \equiv g(\alpha)h_2(\alpha) \pmod{f(\alpha)}.$$

Pak ale $g(\alpha)(h_1(\alpha)-h_2(\alpha)) \equiv 0 \pmod{f(\alpha)}$. Polynom na levé straně je nenulový a jeho stupeň je nejvýše $2(\deg f(\alpha) - 1)$. Místo kongruence modulo $f(\alpha)$ proto musí platit dokonce rovnost. Ta je však ve sporu s faktem, že f je ireducibilní polynom. □

Dá se dokázat (my to však dělat nebudeme), že pro každé prvočíslo p a $k \geq 1$ existuje polynom nad $\mathbb{F}_p$ stupně k, který je ireducibilní nad $\mathbb{F}_p$. Ve spojitosti s tímto faktem dostáváme následující větu:

Věta 5.3.3. *Pro každé prvočíslo p a $k \geq 1$ existuje těleso s právě p^k prvky.*

Uvažme jako příklad těleso $\mathbb{F}_2$ a ireducibilní polynom $f(x) = x^3+x+1$. Množina polynomů v proměnné α stupně nejvýše 2 je

$$\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}.$$

Pro sčítání platí například

$$(\alpha^2 + 1) + (\alpha + 1) = \alpha^2 + \alpha.$$

Při násobení modulo $\alpha^3 + \alpha + 1$ můžeme pracovat s rovností $\alpha^3 = \alpha + 1$ (nad jiným tělesem než $\mathbb{F}_2$ bychom na pravě straně dostali ještě záporné znaménko). Tato rovnost nám umožňuje ze součinů postupně eliminovat všechny členy stupně většího než 2:

$$\alpha \cdot (\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = (\alpha + 1) + \alpha^2 = \alpha^2 + \alpha + 1.$$

Sestavíme-li tabulku násobení ve vzniklém tělese, ukáže se, že každý prvek je mocninou polynomu α:

k	α^k
1	α
2	α^2
3	$\alpha + 1$
4	$\alpha^2 + \alpha$
5	$\alpha^2 + \alpha + 1$
6	$\alpha^2 + 1$
7	1.

Prvky s touto vlastností se nazývají primitivní. Jak uvidíme dále, každé konečné těleso nějaký primitivní prvek obsahuje.

Cvičení

▶ **5.3.1.** Dokažte pozorování 5.3.1. Konkrétně dokažte, že:

(i) $\mathbb{F}_p[x]/f$ je abelovská grupa vzhledem ke sčítání,

(ii) násobení v $\mathbb{F}_p[x]/f - \{0\}$ je asociativní a komutativní, polynom 1 je jednotkovým prvkem,

(iii) pro sčítání a násobení v $\mathbb{F}_p[x]/f$ platí pravidlo distributivity.

5.4 Primitivní prvky

Věta 5.4.1. *Je-li F konečné těleso, pak grupa F^* je cyklická.*

Důkaz. Nechť $q = |F|$. Nejprve dokážeme, že pokud p^k je mocnina prvočísla, která dělí $q - 1$, pak F obsahuje prvek řádu p^k. Nechť tedy $q - 1 = p^k \cdot r$. Polynom $x^{(q-1)/p} - x$ má nejvýše $(q-1)/p < q-1$ různých kořenů a existuje tedy prvek α,

který jeho kořenem není. Položíme-li $\gamma = \alpha^r$, pak $\gamma^{p^k} = \alpha^{q-1} = \alpha^{|F^*|} = 1$, takže řád prvku γ dělí p^k. Na druhou stranu pro $i < k$ je $\gamma^{p^i} \neq 1$, neboť

$$(\gamma^{p^i})^{p^{k-i-1}} = \gamma^{p^i \cdot p^{k-i-1}} = \gamma^{k-1} = \alpha^{\frac{q-1}{p}} \neq 1.$$

Vidíme, že řád prvku γ je p^k.

Ve druhé části důkazu ukážeme, že je-li α prvek řádu a a β prvek řádu b, přičemž a a b jsou nesoudělná, pak $\alpha\beta$ je prvek řádu ab. Předpokládejme, že $\operatorname{ord}\alpha\beta = r$. Protože platí

$$(\alpha\beta)^{ab} = (\alpha^a)^b \cdot (\beta^b)^a = 1,$$

číslo r dělí součin $ab = \operatorname{ord}\alpha\beta$. Lze jej tedy psát ve tvaru $r = a'b'$, kde a' dělí a a b' dělí b. Předpokládejme, že $r \neq ab$. Potom bez újmy na obecnosti platí $a' < a$ a máme

$$(\alpha\beta)^{a'b} = \alpha^{a'b} \cdot (\beta^b)^{a'} = \alpha^{a'b}.$$

Levá strana rovnice je rovna 1, neboť r dělí $a'b$. Odtud také $\alpha^{a'b} = 1$, takže $a'b$ musí dělit a. To ovšem nejde, neboť a a b jsou nesoudělná a $a' < a$. Tím je důkaz druhé části proveden.

Nechť $q-1 = p_1^{k_1} \dots p_m^{k_m}$ je prvočíselný rozklad čísla $q-1$. Podle toho, co bylo řečeno výše, existuje pro každé $i = 1, \dots, m$ prvek γ_i řádu $p_i^{k_i}$. Vzhledem k tomu, že tyto řády jsou nesoudělné, má prvek $\gamma = \gamma_1 \dots \gamma_m$ řád $p_1^{k_1} \dots p_m^{k_m} = q-1$, a musí tedy platit $F^* = \langle\gamma\rangle$. □

Generátory multiplikativní grupy tělesa F se označují jako *primitivní prvky* tohoto tělesa.

5.5 Polynomy

Tvrzení 5.5.1. *Nechť $\alpha, \beta \in \mathbb{F}_{p^m}$, kde p je prvočíslo, a nechť $f(x)$ je polynom nad $\mathbb{F}_p$. Potom*

(i) $(\alpha + \beta)^p = \alpha^p + \beta^p$,

(ii) $f(\alpha^p) = (f(\alpha))^p$.

Důkaz. (i) Použijeme binomickou větu, která v konečných tělesech platí ve tvaru

$$(\alpha + \beta)^k = \sum_{i=0}^{k} (\binom{k}{i} \times 1) \cdot \alpha^i \beta^{k-i}. \tag{5.1}$$

Pro $k = p$ můžeme pravou stranu zjednodušit. Binomické koeficienty $\binom{p}{i}$, kde $1 \leq i \leq p-1$, jsou totiž dělitelné p, neboť ve zlomku

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i(i-1)\dots 1}$$

se v čitateli vyskytuje p, ale ve jmenovateli nikoli. V tělese charakteristiky p jsou tyto členy rovny 0. Platí tedy

$$(\alpha + \beta)^p = \alpha^p + \beta^p,$$

což jsme chtěli dokázat.

(ii) Nechť $f(x) = \sum_{i=0}^{n} a_i x^i$, kde $a_i \in \mathbb{F}_p$. Připomeňme si, že $a_i^p = a_i$. Platí tedy

$$\begin{aligned} f(\alpha^p) &= \sum_{i=0}^{n} a_i (\alpha^p)^i \\ &= \sum_{i=0}^{n} (a_i \alpha^i)^p \\ &= (\sum_{i=0}^{n} a_i \alpha^i)^p = (f(\alpha))^p, \end{aligned}$$

kde předposlední rovnost získáme p-násobným použitím tvrzení (i). □

Kapitola 6

MDS kódy

V minulé kapitole jsme se zabývali perfektními kódy, tj. kódy, které jsou extremální s ohledem na Hammingovu nerovnost. Nyní se zaměříme na třídu kódů, které jsou extremální z jiného hlediska. Podle Singletonova odhadu (věta 1.7.2) pro každý (n, k, d)-kód platí $d \leq n - k + 1$. Lineární kódy, pro které zde platí rovnost, se nazývají *MDS kódy* (z anglického *maximum distance separable*). S existencí MDS kódů jsou spojeny zajímavé a zatím ne zcela vyřešené problémy. V této kapitole odvodíme různé vlastnosti těchto kódů a ukážeme si nejdůležitější třídu MDS kódů, tzv. Reed–Solomonovy kódy.

6.1 Vlastnosti MDS kódů

Jak bylo řečeno výše, $[n, k, d]$-kód C je *MDS kód*, pokud platí $d = n - k + 1$. Pro které hodnoty n, k a q existují q-ární $[n, k]$-kódy?

Stejně jako u perfektních kódů tu existují triviální příklady:

- totální kód s parametry $[n, n, 1]$,
- opakovací kód s parametry $[n, 1, n]$,
- paritní kód s parametry $[n, n - 1, 2]$.

Nás budou zajímat především *netriviální* MDS kódy, tj. $[n, k, n-k+1]$-kódy, pro něž je $2 \leq k \leq n - 2$.

Věta 6.1.1. *Duální kód MDS kódu je rovněž MDS.*

Důkaz. Nechť C je $[n, k, n - k + 1]$-kód. Víme, že $C^\perp$ je $[n, n - k]$-kód; podle věty 1.7.2 je jeho minimální vzdálenost nejvýše $k + 1$. Stačí tedy ukázat, že $\Delta(C^\perp) \geq k + 1$.

Uvažme paritní matici $M^\perp$ kódu C. Podle pozorování 3.3.1 je každá $(n-k)$-tice sloupců matice $M^\perp$ lineárně nezávislá a tvoří tedy regulární čtvercovou podmatici matice $M^\perp$. Žádná netriviální lineární kombinace řádků matice $M^\perp$ tedy nemůže

obsahovat $n-k$ a více nul. Jinými slovy, minimální váha kódu $C^\perp$ je alespoň $k+1$. □

Důsledek 6.1.2. *Nechť C je $[n,k]$-kód s generující maticí M. Pak C je MDS, právě když každá k-tice sloupců matice M je lineárně nezávislá.*

Důkaz. Podle věty 6.1.1 je kód C MDS, právě když jeho duální kód $C^\perp$ je MDS. Ovšem podle pozorování 3.3.1 je $\Delta(C^\perp) \geq k+1$, právě když každá k-tice sloupců matice M je lineárně nezávislá. □

Věta 6.1.3. *Pokud existuje netriviální q-ární MDS $[n,k]$-kód, pak platí*

$$n-q < k < q.$$

Důkaz. Nejprve ukážeme $k > n-q$. Klíčový fakt je, že

$$\begin{gathered}\text{každá generující matice MDS } [n,k] \text{ kódu obsahuje} \\ \text{v každém řádku nejvýše } k-1 \text{ nul.}\end{gathered} \tag{6.1}$$

Jinak bychom totiž snadno dostali spor s důsledkem 6.1.2 (množina k sloupců, které mají nulu ve stejném řádku, je lineárně závislá).

Nechť M je generující matice ve tvaru $(I_k\ A)$. Podle (6.1) matice A neobsahuje nulové prvky. Můžeme předpokládat, že první řádek matice A obsahuje samé jedničky (po vynásobení každého sloupce vhodným skalárem vznikne generující matice ekvivalentního kódu, který je nutně rovněž MDS). Matice $M = (m_{ij})$ má aspoň 2 řádky, neboť $k > 1$. Kdyby platilo $k \leq n-q$, pak $n-k > q-1$, a tak ve druhém řádku matice M by se některá hodnota (dejme tomu $\alpha \in \mathbb{F}_q$) musela objevit dvakrát. Odečtením α-násobku prvního řádku matice A od druhého řádku získáme matici A', která generuje stejný kód a má ve druhém řádku alespoň k nul, což je spor s (6.1).

Dokázali jsme, že $k > n-q$. Aplikujeme-li tuto nerovnost na duální kód (který je MDS s parametry $[n, n-k]$, dozvíme se, že $n-k > n-q$, a tedy $k < q$. To je druhá z dokazovaných nerovností. □

6.2 Reed–Solomonovy kódy

Reed–Solomonovy kódy představují nejdůležitější třídu MDS kódů, a to i z hlediska praktických aplikací. Používají se mj. v každém CD přehrávači (pro korekci chyb vzniklých poškozením disku).

Nechť q je mocnina prvočísla a $k \geq 1$. Seřaďme všechny nenulové prvky tělesa $\mathbb{F}_q$ do pevné posloupnosti $\beta_1, \ldots, \beta_{q-1}$ (přirozenou možností je $\beta_i = \alpha^i$, kde α je primitivní prvek tělesa $\mathbb{F}_q$).

Reed–Solomonův kód $\mathrm{RS}_{q,k}$ je lineární kód délky $q-1$ nad tělesem $\mathbb{F}_q$, sestávající ze všech slov tvaru

$$[f] = (f(\beta_1), f(\beta_2), \ldots, f(\beta_{q-1})), \tag{6.2}$$

kde f probíhá všechny polynomy v proměnné x nad $\mathbb{F}_q$ stupně nejvýše $k-1$. Říkáme, že slova kódu $\mathrm{RS}_{q,k}$ jsou *evaluace* polynomů stupně $\leq k-1$ ve všech nenulových prvcích tělesa $\mathbb{F}_q$.

Příklad 6.2.1. Uvažme kód $\mathrm{RS}_{4,2}$. Těleso $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ obsahuje primitivní prvek α s vlastností $\alpha^2 = \alpha + 1 = \beta$. Nenulové prvky tělesa uvažujeme v pořadí $\alpha, \alpha^2 = \beta, \alpha^3 = 1$. Protože $k = 2$, zajímají nás evaluace polynomů stupňů 0 a 1 (tj. konstantních a lineárních polynomů). Každý takový polynom je tvaru $\sigma x + \tau$, kde $\sigma, \tau \in \mathbb{F}_4$. Jejich evaluace (v bodech $\alpha, \beta, 1$) uvádí následující tabulka.

σ \ τ	0	1	α	β
0	000	111	$\alpha\alpha\alpha$	$\beta\beta\beta$
1	$\alpha\beta 1$	$\beta\alpha 0$	01β	10α
α	$\beta 1\alpha$	$\alpha 0\beta$	$1\beta 0$	$0\alpha 1$
β	$1\alpha\beta$	$0\beta\alpha$	$\beta 01$	$\alpha 10$

Např. údaj v řádku β a sloupci 1 znamená, že pro polynom $f(x) = \beta x + 1$ platí $f(\alpha) = 0, f(\beta) = \beta$ a $f(1) = \alpha$. V tabulce je všech 16 slov kódu $\mathrm{RS}_{4,2}$.

Reed–Solomonovy kódy jsou lineární (neboť součet dvou kódových slov je evaluací součtu příslušných polynomů). Minimální vzdálenost kódu $\mathrm{RS}_{q,k}$ je snadné určit. Jsou-li f, g dva různé polynomy stupně nejvýše t, shodují se jejich hodnoty nejvýše v t bodech (jinak by nenulový polynom $f - g$ stupně $\leq t$ měl více než t kořenů). Hodnoty různých polynomů stupně $\leq k-1$ se tedy musí *lišit* alespoň v $q-k$ nenulových 'bodech' v tělese $\mathbb{F}_q$. Snadno navíc najdeme dvojici polynomů, které se liší právě v $q-k$ bodech (např. 0 a libovolný polynom s $k-1$ různými kořeny). Dostáváme následující tvrzení.

Tvrzení 6.2.2. *Minimální vzdálenost kódu* $\mathrm{RS}_{q,k}$ *je* $q-k$. □

Určení dimenze dá o trochu více práce. Polynomy stupně $\leq k-1$ tvoří lineární prostor P_k dimenze k nad $\mathbb{F}_q$ (jednou z bází je $\{1, x, x^2, \ldots, x^{k-1}\}$) a zdá se, že i kód $\mathrm{RS}_{q,k}$ (tedy prostor jejich evaluací) má dimenzi k. Tak tomu skutečně je:

Věta 6.2.3. *Kód* $\mathrm{RS}_{q,k}$ *má parametry* $[q-1, k, q-k]_q$.

Důkaz. Stačí dokázat, že dimenze je k. Větší být nemůže, protože prostor polynomů P_k má dimenzi k, a je-li polynom $f = \sum \alpha_i g_i$ lineární kombinací polynomů g_i, pak pro jeho evaluaci $[f]$, definovanou vztahem (6.2), platí

$$[f] = \sum \alpha_i [g_i].$$

Odtud plyne, že $\dim \mathrm{RS}_{q,k} \leq \dim P_k = k$.

Zbývá dokázat, že $\dim \mathrm{RS}_{q,k} \geq k$. K tomu stačí dokázat, že matice $M(\mathrm{RS}_{q,k})$ o rozměrech $k \times (q-1)$, jejíž řádky jsou slova $[1], [x], [x^2], \ldots, [x^{k-1}]$, tj. matice

$$M(\mathrm{RS}_{q,k}) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \beta_1 & \beta_2 & \ldots & \beta_{q-1} \\ \beta_1^2 & \beta_2^2 & \ldots & \beta_{q-1}^2 \\ \vdots & \vdots & & \vdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \ldots & \beta_{q-1}^{k-1} \end{pmatrix}, \tag{6.3}$$

má hodnost k (a je tedy generující maticí daného kódu). Vyberme z této matice prvních k sloupců. Dostaneme tzv. Vandermondovu matici $V(\beta_1, \beta_2, \ldots, \beta_k)$, která je podle cvičení 6.2.1 regulární. Hodnost matice $M(\mathrm{RS}_{q,k})$ je tedy k a věta je dokázána. □

Z věty 6.2.3 vidíme, že Reed–Solomonovy kódy jsou MDS.

Důkaz věty 6.2.3 nám poskytl explicitní generující matici (6.3) kódu $\mathrm{RS}_{q,k}$. Jak vypadá paritní matice?

Tvrzení 6.2.4. *Matice*

$$M^\perp(\mathrm{RS}_{q,k}) = \begin{pmatrix} \beta_1 & \beta_2 & \ldots & \beta_{q-1} \\ \beta_1^2 & \beta_2^2 & \ldots & \beta_{q-1}^2 \\ \vdots & \vdots & & \vdots \\ \beta_1^{q-k-1} & \beta_2^{q-k-1} & \ldots & \beta_{q-1}^{q-k-1} \end{pmatrix} \tag{6.4}$$

je paritní maticí kódu $\mathrm{RS}_{q,k}$.

Důkaz. Ze cvičení 6.2.1 plyne, že matice $M^\perp = M^\perp(\mathrm{RS}_{q,k})$ je regulární. Stačí tedy ukázat, že pro libovolné $i = 0, \ldots, k-1$ a $j = 1, \ldots, q-k-1$ je i-tý řádek matice $M(\mathrm{RS}_{q,k})$ ortogonální na j-tý řádek matice $M^\perp$, tj. že platí

$$\sum_{\ell=1}^{q-1} \beta_\ell^i \cdot \beta_\ell^j = 0. \tag{6.5}$$

Zvolme primitivní prvek α tělesa $\mathbb{F}_q$. Potom

$$\begin{aligned} \sum_{\ell=1}^{q-1} \beta_\ell^{i+j} &= \sum_{\ell=0}^{q-2} \alpha^\ell \\ &= \frac{\alpha^{q-1} - 1}{\alpha - 1} = 0, \end{aligned}$$

protože $\alpha^{q-1} = 1$. Důkaz je hotov. □

Cvičení

▶ **6.2.1.** Nechť $x_1, \ldots, x_n$ jsou různé prvky nějakého tělesa. *Vandermondova matice* $V(x_1, \ldots, x_n)$ je následující matice o rozměrech $n \times n$:

$$V(x_1, \ldots, x_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix}. \tag{6.6}$$

Dokažte, že

$$\det V(x_1, \ldots, x_n) = \prod_{i<j} (x_j - x_i)$$

a matice $V(x_1, \ldots, x_n)$ je tedy regulární.

Návod: Odečtením prvního sloupce od věech ostatních a vydělením i-tého sloupce faktorem $x_i - x_1$ (pro každé $i \geq 2$) dostaneme matici s determinantem rovným $\det V(x_2, \ldots, x_n)$.

6.3 Existence MDS kódů

V oddílu 6.2 jsme pro každou mocninu prvočísla q a libovolné $k \in \{0, \ldots, q-1\}$ zkonstruovali q-ární MDS kód s parametry $[q-1, k, q-k]$, totiž Reed-Solomonův kód $\mathrm{RS}_{q,k}$.

Pokud v libovolném MDS kódu odstraníme jednu ze souřadnic (z každého slova vypustíme i-tý symbol), dostaneme zjevně opět MDS kód. Opakováním této operace získáme pro libovolné předepsané n a k, kde $0 \leq k \leq n$, nějaký MDS kód s parametry $[n, k, n-k+1]$.

Jaká je maximální možná délka netriviálního q-árního MDS kódu? Na tuto otázku uvedená konstrukce neodpovídá. Uvidíme, že lze najít kódy s větší délkou než mají RS kódy (tj. než $q-1$), ale patrně ne o mnoho. Úplná odpověď zatím není známa.

Pokud paritní matici (6.4) rozšíříme o dva řádky a sloupce na matici

$$M_1^{\perp} = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ \beta_1 & \beta_2 & \ldots & \beta_{q-1} & 0 & 0 \\ \beta_1^2 & \beta_2^2 & \ldots & \beta_{q-1}^2 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ \beta_1^{q-k-1} & \beta_2^{q-k-1} & \ldots & \beta_{q-1}^{q-k-1} & 0 & 0 \\ \beta_1^{q-k} & \beta_2^{q-k} & \ldots & \beta_{q-1}^{q-k} & 0 & 1 \end{pmatrix}, \tag{6.7}$$

dostaneme paritní matici kódu C_1, který vznikne přidáním paritního symbolu na konec každého kódového slova. Každá $(k+2)$-tice sloupců této matice je zjevně

lineárně nezávislá, takže podle důsledku 6.1.2 je kód ${C_1}^\perp$, a tedy i C_1, MDS kód. Nalezli jsme tedy netriviální q-ární MDS kód libovolné dimenze k a délky $q+1$.

Pro $k = 3$ lze jít ještě o kousek dál, alespoň v případě, že q je mocnina dvojky (viz cvičení 6.3.1). Následující problém je ale patrně dosud otevřený.

Problém 6.3.1. Existuje pro nějaké q netriviální q-ární MDS kód o délce větší než $q+2$?

Cvičení

► **6.3.1.** Nechť M' je matice

$$M' = \Big(M \mid I_3\Big),$$

kde $M = M(\mathrm{RS}_{q,3})$ (viz (6.3)) a I_3 je jednotková matice. Dokažte, že každá trojice sloupců matice M' je lineárně nezávislá, právě když q je mocnina dvou. Odvoďte, že pro $q = 2^m$ a $k = 3$ nebo $k = q-1$ existují q-ární MDS kódy s parametry $[q+2, k]$.

Kapitola 7

Reed–Mullerovy kódy

7.1 Definice

Na Reed–Mullerovy kódy lze nahlížet jako na zobecnění kódů Reed–Solomonových. Vzpomeňme si, že kód $\mathrm{RS}_{q,k}$ sestává z evaluací polynomů stupně $< k$ nad tělesem $\mathbb{F}_q$, kde q je mocnina prvočísla. Reed–Mullerovy kódy dostaneme, pokud tuto definici zobecníme na polynomy více proměnných.

Již víme, jak pro daný okruh R vytvořit okruh polynomů $R[x]$ v proměnné x. Vyjdeme-li z okruhu $R = \mathbb{F}_q$ a iterujeme-li tuto konstrukci, získáme okruh polynomů $\mathbb{F}_q[x_1, \ldots, x_m]$ nad $\mathbb{F}_q$ v proměnných $x_1, \ldots, x_m$. Jeho prvky lze ztotožnit s výrazy tvaru

$$f(x_1, \ldots, x_m) = \sum_{(i_1,\ldots,i_m)} a_{i_1 \ldots i_m} x_1^{i_1} \cdot \cdots \cdot x_m^{i_m}, \tag{7.1}$$

kde sčítáme přes konečnou množinu m-tic $(i_1, \ldots, i_m)$ a každý koeficient $a_{i_1 \ldots i_m}$ je prvkem tělesa $\mathbb{F}_m$. Sčítání a násobení polynomů je definováno podle očekávání a má následující vlastnosti:

- sčítání polynomů je komutativní, takže např. $x_1^2 + x_2 = x_2 + x_1^2$,
- násobení polynomů je rovněž komutativní, speciálně pro každé i, j platí $x_i x_j = x_j x_i$,
- nultá mocnina proměnné je rovna 1, takže například $x_1^0 x_2^2 x_3^0 = x_2^2$.

Celkový stupeň polynomu $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ je číslo

$$\mathrm{td}(f) = \max(i_1 + \cdots + i_m),$$

přičemž maximum je bráno přes všechny členy $x_1^{i_1} \ldots x_m^{i_m}$ s nenulovým koeficientem v polynomu f. Je-li $\beta = (\alpha_1, \ldots, \alpha_m)$ uspořádaná m-tice prvků tělesa $\mathbb{F}_q$, pak symbolem $f(\beta)$ označíme hodnotu $f(\alpha_1, \ldots, \alpha_n)$. Nechť $\beta_0, \ldots, \beta_{q^m-1}$ je

očíslování všech uspořádaných m-tic tělesa $\mathbb{F}_q$. *Reed–Mullerův kód* $\mathcal{R}_q(r,m)$ je tvořen slovy

$$(f(\beta_0), f(\beta_1), \ldots, f(\beta_{q^m-1})),$$

kde f probíhá všechny polynomy v $\mathbb{F}_q[x_1,\ldots,x_m]$, jejichž celkový stupeň je nejvýše r. Kód $\mathcal{R}_q(r,m)$ je tedy q-ární a jeho délka je q^m.

Protože pro každý prvek $\alpha \in \mathbb{F}_q$ platí $\alpha^q = \alpha$, stačí se omezit na evaluace polynomů, v nichž každá proměnná x_i má stupeň menší než q. Speciálně v případě $q = 2$ (binární kódy) má každá proměnná stupeň 0 nebo 1; polynomům, které tak dostaneme, se říká booleovské. Budeme se jim věnovat v následujícím odstavci.

Cvičení

▶ **7.1.1.** Definujme okruh polynomů $\mathbb{F}_q[x_1,\ldots,x_m]$ $(m \geq 2)$ rekurentním vztahem

$$\mathbb{F}_q[x_1,\ldots,x_m] = (\mathbb{F}_q[x_1,\ldots,x_{m-1}])[x_m].$$

Zapište explicitně operaci sčítání a násobení polynomů v tomto okruhu.

7.2 Booleovské funkce a booleovské polynomy

Polynom $f(x_1,\ldots,x_m)$ v m proměnných nad $\mathbb{F}_2$ je *booleovský polynom*, pokud v každém členu součtu

$$f(x_1,\ldots,x_m) = \sum_{(i_1,\ldots,i_m)} a_{i_1\ldots i_m} x_1^{i_1} \cdot \cdots \cdot x_m^{i_m}$$

jsou všechny exponenty $i_1,\ldots,i_m$ rovny 0 nebo 1. Booleovský polynom $f(x_1,\ldots,x_m)$ je tedy součtem členů tvaru

$$x^{j_1} x^{j_2} \ldots x^{j_k}, \tag{7.2}$$

kde platí $1 \leq j_1 < \cdots < j_k \leq m$. Členy (7.2) označujeme jako *monomy*. Každé množině $I \subset \{1,\ldots,m\}$ odpovídá monom

$$x_I = \prod_{i\in I} x_i.$$

Monom $x_\emptyset$ označujeme symbolem 1. Mezi booleovskými polynomy má zvláštní místo ještě polynom 0, který je pro změnu součtem prázdné množiny monomů.

Protože v tělese $\mathbb{F}_2$ platí $0^2 = 0$ a $1^2 = 1$, je přirozené pro $i = 1,\ldots,m$ postulovat rovnost

$$x_i^2 = x_i. \tag{7.3}$$

S využitím tohoto vztahu můžeme součin dvou booleovských polynomů jednoznačně upravit na polynom, který je opět booleovský. Platí například

$$x_1x_2 \cdot (x_2 + x_3) = x_1x_2 + x_1x_2x_3.$$

Booleovská funkce m proměnných je libovolné zobrazení $h : \mathbb{F}_2^m \to \mathbb{F}_2$. Každý booleovský polynom f určuje booleovskou funkci $\hat{f}$: dosadíme-li za jednotlivé proměnné, je výsledná hodnota jednoznačně určena.

Protože počet booleovských funkcí m proměnných je shodný s počtem booleovských polynomů v proměnných $x_1, \ldots, x_m$ (viz cvičení 7.2.1), můžeme se ptát, zda každé booleovské funkci odpovídá polynom, který ji 'počítá'. Odpověď je kladná:

Věta 7.2.1. *Pro každou booleovskou funkci m proměnných h existuje booleovský polynom $f \in \mathbb{F}_2[x_1, \ldots, x_m]$ s vlastností, že $h = \hat{f}$.*

Důkaz. Nejprve tvrzení dokažme pro funkci $h_{i_1\ldots i_m}$, která má hodnotu 1 pouze v jediném bodě, a to $(i_1, \ldots, i_m) \in \mathbb{F}_2^m$. Pro každé $k = 1, \ldots, m$ vezměme booleovský polynom p_k v proměnné x_k, definovaný předpisem

$$p_k(x_k) = \begin{cases} x_k & \text{pokud } i_k = 1, \\ 1 + x_k & \text{jinak.} \end{cases}$$

Nyní stačí položit

$$f_{i_1\ldots i_m}(x_1, \ldots, x_k) = p_1(x_1) \cdot \cdots \cdot p_m(x_m)$$

a ověřit, že platí $\hat{f}_{i_1\ldots i_m} = h_{i_1\ldots i_m}$.

Pro obecnou booleovskou funkci h vezměme polynom

$$f = \sum_{h(i_1,\ldots,i_m)=1} f_{i_1\ldots i_m}.$$

Z definice plyne, že $\hat{f}(i_1, \ldots, i_m) = 1$, právě když $h(i_1, \ldots, i_m) = 1$. Platí tedy $\hat{f} = h$. □

Věta 7.2.1 nám umožňuje ztotožnit booleovskou funkci s jednoznačně určeným booleovským polynomem, který jí odpovídá. V následujících odstavcích proto nebudeme mezi těmito dvěma pojmy důsledně rozlišovat a použijeme vždy ten, který je v daném kontextu výhodnější.

Cvičení

▶ **7.2.1.** Ukažte, že počet booleovských funkcí m proměnných i počet booleovských polynomů v proměnných $x_1, \ldots, x_m$ je 2^{2^m}.

7.3 Binární Reed–Mullerovy kódy

Pro libovolný polynom $f \in \mathbb{F}_2[x_1, \ldots, x_m]$ označme

$$N(f) = \{(i_1, \ldots, i_m) \in \mathbb{F}_2^m \,:\, f(i_1, \ldots, i_m) = 1\}.$$

Dokážeme dolní odhad na velikost množiny $N(f)$, ze kterého plyne odhad minimální vzdálenosti Reed-Mullerových kódů.

Tvrzení 7.3.1. *Nechť $f \in \mathbb{F}_2[x_1, \ldots, x_m]$ je nenulový booleovský polynom celkového stupně nejvýše r. Pak*

$$|N(f)| \geq 2^{m-r}.$$

Důkaz. Indukcí přes m. Pro $m = 1$ je tvrzení zřejmé. Předpokládejme tedy, že $m > 1$. Nechť g je součet všech monomů, které se vyskytují v polynomu f a obsahují proměnnou x_1. Platí tedy

$$f = x_1 \cdot g + h, \tag{7.4}$$

kde g a h jsou polynomy v proměnných $x_2, \ldots, x_m$.

Je-li $g = 0$, pak každé $(m-1)$-tici $(i_2, \ldots, i_m) \in N(h)$ odpovídají dvě m-tice z $N(f)$, totiž $(0, i_2, \ldots, i_m)$ a $(1, i_2, \ldots, i_m)$. Z indukčního předpokladu, aplikovaného na polynom h v $m-1$ proměnných, proto plyne

$$|N(f)| = 2|N(h)| \geq 2 \cdot 2^{m-1-r} = 2^{m-r}.$$

Můžeme tedy předpokládat, že $g \neq 0$. Protože $\mathrm{td}(g) \leq r-1$, podle indukčního předpokladu je

$$|N(g)| \geq 2^{m-1-(r-1)} = 2^{m-r}.$$

Uvažme libovolnou $(m-1)$-tici $(i_2, \ldots, i_m) \in N(g)$. Dosazením do f získáváme funkci jedné proměnné $f(x_1, i_2, \ldots, i_m)$, pro kterou podle (7.4) platí

$$f(x_1, i_2, \ldots, i_m) = x_1 + h(i_2, \ldots, i_m).$$

Existuje tedy právě jedna hodnota proměnné x_1, pro kterou $(x_1, i_2, \ldots, i_m) \in N(f)$. Odtud

$$|N(f)| = |N(g)| \geq 2^{m-r}.$$

□

Důsledek 7.3.2. *Množina $B_r \subset \mathcal{R}(r, m)$, tvořená evaluacemi všech monomů celkového stupně nejvýše r, je bází kódu $\mathcal{R}(r, m)$.*

Důkaz. Protože každý polynom f ($\mathrm{td}(f) \leq r$) je součtem monomů celkového stupně nejvýše r, množina B_r generuje kód $\mathcal{R}(r,m)$. Dokážeme, že je lineárně nezávislá.

Podle tvrzení 7.3.1 je evaluace $[f]$ každého nenulového polynomu f je nenulová, neboť $|N(f)| \geq 2^{m-m} = 1$. To ovšem znamená, že množina evaluací všech monomů

$$\{[1], [x_1], [x_2], \ldots, [x_m], [x_1x_2], \ldots, [x_1x_2\ldots x_m]\}$$

je lineárně nezávislá. Tím pádem také množina B_r je lineárně nezávislá. □

Příklad 7.3.3. Uvažme jako příklad kód $\mathcal{R}(1,3)$. Z důsledku 7.3.2 plyne, že jedna jeho generující matice má jako řádky slova $[1]$, $[x_1]$, $[x_2]$, $[x_3]$. Bereme-li při evaluaci prvky množiny $\mathbb{F}_2^3$ v pořadí

$$000, 001, 010, 011, 100, 101, 110, 111$$

(závorky pro přehlednost vynecháváme), dostaneme matici

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

Důsledek 7.3.4. *Reed–Mullerův kód $\mathcal{R}(r,m)$ má délku 2^m, dimenzi $\binom{m}{0} + \cdots + \binom{m}{r}$ a minimální váhu 2^{m-r}.*

Důkaz. Z tvrzení 7.3.1 plyne, že minimální váha je alespoň 2^{m-r}. Tato hodnota se nabývá například pro slovo $[x_1x_2\ldots x_r]$. Tvrzení o dimenzi plyne z důsledku 7.3.2 a faktu, že monomů celkového stupně i je přesně $\binom{m}{i}$. □

Reed–Mullerovy kódy jsou k sobě navzájem duální, jak ukazuje následující tvrzení.

Věta 7.3.5. *Kódy $\mathcal{R}(r,m)$ a $\mathcal{R}(m-r-1,m)$ jsou navzájem duální.*

Důkaz. Dimenze kódu $\mathcal{R}(m-r-1,m)$ je rovna

$$\binom{m}{0} + \cdots + \binom{m}{m-r-1} = \binom{m}{r+1} + \cdots + \binom{m}{m},$$

takže

$$\dim \mathcal{R}(r,m) + \dim \mathcal{R}(m-r-1,m) = \sum_{i=1}^{m} \binom{m}{i} = 2^m.$$

Protože délka těchto kódů je rovněž 2^m, k důkazu duality stačí ukázat, že kódy jsou navzájem ortogonální. Můžeme se přitom omezit na jejich bázové vektory. Podle důsledku 7.3.2 je báze kódu $\mathcal{R}(r,m)$ tvořena slovy $[x_I]$, kde $|I| \leq r$.

Podobně báze kódu $\mathcal{R}(m-r-1,m)$ sestává ze slov $[x_J]$, kde $|J| \leq m-r-1$. Chceme ukázat, že skalární součin $\langle [x_I], [x_J] \rangle$ je nulový. Tento skalární součin je součtem výrazů

$$x_I(i_1,\ldots,i_m) \cdot x_J(i_1,\ldots,i_m)$$

přes všechny m-tice $(i_1,\ldots,i_m)$. Protože $x_I \cdot x_J = x_{I\cup J}$, platí

$$\langle [x_I], [x_J] \rangle = \sum_{(i_1,\ldots,i_m)} x_{I\cup J}(i_1,\ldots,i_m).$$

Daná m-tice $(i_1,\ldots,i_m)$ do tohoto součtu přispěje 1, právě když $i_k = 1$ pro každé $k \in I \cup J$. Takových m-tic je stejný počet jako nadmnožin množiny $I \cup J$, tedy $2^{m-|I\cup J|}$ — což je sudé číslo, neboť

$$m - |I \cup J| \geq m - (r + m - r - 1) = 1.$$

Uvažovaný skalární součin je tedy nulový a důkaz je hotov. □

7.4 Kódování a dekódování

Tento odstavec je věnován kódování a dekódování pomocí Reed-Mullerových kódů. Popíšeme Reedův algoritmus, který k dekódování těchto kódů používá tzv. většinovou logiku.

Předpokládejme, že odesílatel má binární zdrojové slovo a o délce $2^{V(m,r)}$, kde $V(m,r) = \sum_{i=0}^{r} \binom{m}{i}$. Symboly tohoto slova budeme indexovat množinami $I \subset \{1,\ldots,m\}$ o velikosti nejvýše r a psát

$$a = (a_I)_I,$$

kde I probíhá takové množiny. Slovo a odesílatel přiřadí booleovský polynom

$$f = \sum_{I,|I|\leq r} a_I x_I$$

a získá kódové slovo $[f]$ (evaluaci pro nějaké pevně zvolené uspořádání množiny $\mathbb{F}_2^m$). Délka slova tedy vzroste z $V(m,r)$ na 2^m, při správném dekódování se nám však podaří opravit až $2^{m-r-1}-1$ chyb vzniklých při přenosu.

Takové dekódování umožňuje Reedův dekódovací algoritmus. Předpokládejme, že odesílatel obdrží slovo y délky 2^m, jehož symboly jsou indexovány m-ticemi z $\mathbb{F}_2^m$. Symbol na pozici $(i_1,\ldots,i_m) \in \mathbb{F}_2^m$ budeme označovat symbolem $y_{i_1\ldots i_m}$. Cílem je rekonstruovat koeficienty a_I polynomu f.

Ideu algoritmu budeme ilustrovat na příkladu 7.3.3, kde jsme našli generující matici M kódu $\mathcal{R}(1,3)$. Všimněme si, že součet prvních dvou prvků na řádku $[x_3]$ matice M je roven 1, zatímco u ostatních řádků je roven 0 (při počítání modulo

2). To znamená, že pro libovolný booleovský polynom $f = \sum a_I x_I$ ($\mathrm{td}(f) \leq 1$) a $y = [f]$ platí

$$y_{000} + y_{001} = 1, \text{ právě když } a_{\{3\}} = 1.$$

Stejnou vlastnost navíc mají součty $y_{010} + y_{011}$, $y_{100} + y_{101}$ a $y_{110} + y_{111}$. Ve slově y tedy máme čtyři disjunktní dvojice symbolů, z nichž každá jednoznačně určuje koeficient $a_{\{3\}}$.

Tento koeficient tak dokážeme správně určit i v případě, že při přenosu kódového slova $[f]$ (jehož výsledkem je přijaté slovo y) došlo k jedné chybě. Stačí nechat uvedené čtyři součty 'hlasovat' o tom, zda $a_{\{3\}} = 1$, a přiklonit se k většinovému výsledku.

Uvažme konkrétní příklad: odeslané slovo je $[x_1 + x_3] = (01011010)$ a při přenosu došlo k chybě ve třetím symbolu, takže $y = (01111010)$. Příjemce slovo y rozdělí do bloků délky 2 a zjistí, že součty symbolů v jednotlivých blocích jsou

$$0 + 1 = 1, \qquad 1 + 1 = 0, \qquad 1 + 0 = 1, \qquad 1 + 0 = 1.$$

Proto správně rozhodne, že $a_{\{3\}} = 1$.

Než přistoupíme k obecné formulaci algoritmu, potřebujeme dokázat několik pomocných tvrzení a zavést vhodné značení.

Každé množině $B \subset \{1, \ldots, m\}$ přiřadíme její *charakteristický vektor* $\chi_B \in \mathbb{F}_2^m$, který má na pozici i prvek 1, právě když $i \in B$.

Pozorování 7.4.1. *Pro $J, B \subset \{1, \ldots, m\}$ platí*

$$x_J(\chi_B) = 1, \text{ právě když } J \subset B.$$

Je-li f booleovská funkce m proměnných a $I \subset \{1, \ldots, m\}$, definujme booleovskou funkci f^I v m proměnných vztahem

$$f^I(\chi_Y) = \sum_{B:\ Y \subset B \subset I \cup Y} f(\chi_B)$$

pro každé $Y \subset \{1, \ldots, m\}$.

Lemma 7.4.2. *Nechť $I, J, Y \subset \{1, \ldots, m\}$. Pak platí*

$$(x_J)^I(\chi_Y) = 1, \text{ právě když } I \subset J \cup Y.$$

Důkaz. Z definice funkce $(x_J)^I$ je

$$\begin{aligned}(x_J)^I(\chi_Y) &= \sum_{B:\ Y \subset B \subset I \cup Y} x_J(\chi_B) \\ &= \sum_{B:\ J \cup Y \subset B \subset I \cup Y} 1,\end{aligned}$$

přičemž druhá rovnost plyne z pozorování 7.4.1.

Protože počet množin B s vlastností $J \cup Y \subset B \subset I \cup Y$ je $2^{|(I \cup Y) - (J \cup Y)|} = 2^{|I - (J \cup Y)|}$, zjišťujeme, že $(x_J)^I(\chi_Y) = 1$ právě tehdy, když $I \subset J \cup Y$. □

Věta 7.4.3. *Nechť $f = \sum_J a_J x_J$ je booleovský polynom celkového stupně nejvýše $d \leq r$ v proměnných $x_1, \ldots, x_m$ a nechť $I, Y \subset \{1, \ldots, m\}$ jsou disjunktní množiny. Pokud $|I| = d$, pak platí*

$$a_I = f^I(\chi_Y).$$

Důkaz. Z definice plyne

$$\begin{aligned} f^I(\chi_Y) &= (\sum_J a_J x_J)^I(\chi_Y) \\ &= \sum_{B:\ Y \subset B \subset I \cup Y} (\sum_J a_J x_J)(\chi_B) \\ &= \sum_J a_J \cdot \sum_{B:\ Y \subset B \subset I \cup Y} x_J(\chi_B) \\ &= \sum_J a_J \cdot (x_J)^I(\chi_Y). \end{aligned}$$

Kdy k tomuto součtu množina J přispěje hodnotu 1? Nutnou a postačující podmínkou je $a_J = 1$ a $(x_J)^I(\chi_Y) = 1$, přičemž druhá rovnost podle lemmatu 7.4.2 nastává, právě když $I \subset Y \cup J$. Pro takovou množinu J platí $|J| \leq d$ (neboť $\mathrm{td}(f) \leq d$) a $I \subset J$ (neboť $I \cap Y = \emptyset$). Protože $|I| = d$, jediná množina J s nenulovým příspěvkem je $J = I$. Tím je důkaz proveden. □

Nyní již můžeme formulovat Reedův dekódovací algoritmus. Vstupem je přijaté slovo y, výstupem booleovský polynom f celkového stupně nejvýše r s vlastností, že pokud došlo při přenosu k méně než 2^{m-r-1} chybám, pak odeslané slovo bylo $[f]$.

Položíme $d := r$. Při každém průchodu algoritmem určíme jeden z koeficientů polynomu $f = \sum_J a_J x_J$.

1. Vezmeme některou ještě nezpracovanou množinu I velikosti d. Pokud taková množina neexistuje, přejdeme na krok 6.

2. Pro každou z 2^{m-d} množin Y s vlastností $I \cap Y = \emptyset$ spočítáme hodnotu

$$g(Y) = \sum_{B:\ Y \subset B \subset I \cup Y} y_{\chi_B}. \tag{7.5}$$

3. Každá taková množina Y hlasuje pro možnost $a_I = 1$, pokud $g(Y) = 1$, případně pro možnost $a_I = 0$, pokud $g(Y) = 0$. Většinový hlas vyhrává.

4. Je-li výsledek hlasování $a_I = 1$, položíme $y := y - [x_I]$.

5. Pokračujeme krokem 1.

6. Je-li $d > 0$, snížíme d o jednu a pokračujeme krokem 1. Jinak algoritmus končí a výstupem je polynom $\sum_J a_J x_J$.

Správnost algoritmu vyplývá z věty 7.4.3: o množině I hlasuje 2^{m-d} množin Y. Každá množina B v rovnici (7.5) přitom odpovídá pouze jediné z nich. Aby tedy rozhodnutí ohledně koeficientu a_I bylo chybné, musí při přenosu nastat alespoň $2^{m-d}/2 \geq 2^{m-r-1}$ chyb.

Kapitola 8

Algebraické intermezzo 3

8.1 Minimální polynom

Pozorování 8.1.1. *Každý prvek tělesa $\mathbb{F}_{p^m}$, kde p je prvočíslo, je kořenem polynomu*

$$x^{p^m} - x.$$

Pozorování 8.1.1 umožňuje následující definici. *Minimální polynom* prvku $\alpha \in \mathbb{F}_{p^m}$ nad tělesem $\mathbb{F}_p$ je polynom $M_\alpha(x)$, určený vlastnostmi:

(1) $M_\alpha(x)$ je (nenulový) monický polynom s koeficienty z $\mathbb{F}_p$,

(2) $M_\alpha(\alpha) = 0$,

(3) žádný polynom menšího stupně nesplňuje podmínky (1) a (2).

Minimální polynom je jednoznačně určen, neboť kdyby $M'_\alpha(x)$ byl další polynom s vlastnostmi (1)–(3), pak $M_\alpha - M'_\alpha$ je polynom menšího stupně s kořenem α a snadno dostaneme spor s vlastností (3).

Tvrzení 8.1.2. *Nechť $\alpha \in \mathbb{F}_{p^m}$ a nechť $f(x) \in \mathbb{F}_p[x]$ je polynom s vlastností $f(\alpha) = 0$. Potom polynom $M_\alpha(x)$ dělí $f(x)$.*

Důkaz. Pomocí věty o dělení polynomů vyjádřeme

$$f(x) = q(x) \cdot M_\alpha(x) + r(x),$$

kde $\deg r < \deg M_\alpha$. Protože $f(\alpha) = M_\alpha(\alpha) = 0$, dostáváme také $r(\alpha) = 0$. Je-li polynom $r(x)$ nenulový, pak vhodným vynásobením prvkem tělesa $\mathbb{F}_p$ získáme monický polynom, který splňuje podmínky (1) a (2) z definice minimálního polynomu. To je spor, proto $r = 0$ a polynom f je dělitelný polynomem M_α. □

Uvažme jako příklad těleso $\mathbb{F}_8$, zkonstruované pomocí ireducibilního polynomu $f(x) = x^3 + x + 1$. Prvky tohoto tělesa mají následující minimální polynomy:

$$M_1(x) = x + 1, \qquad M_{\alpha^4}(x) = x^3 + x + 1,$$
$$M_\alpha(x) = x^3 + x + 1, \qquad M_{\alpha^5}(x) = x^3 + x^2 + 1,$$
$$M_{\alpha^2}(x) = x^3 + x + 1, \qquad M_{\alpha^6}(x) = x^3 + x^2 + 1.$$
$$M_{\alpha^3}(x) = x^3 + x^2 + 1,$$

Můžeme si všimnout několika zajímavých skutečností:

- $M_\alpha(x) = f(x)$. Obecně platí, že minimální polynom prvku α tělesa $\mathbb{F}_{p^m}$, definovaného jako těleso polynomů v α 'modulo ireducibilní polynom f', je právě $f(x)$. (Viz cvičení 8.1.1.)
- $M_\alpha(x) = M_{\alpha^2}(x) = M_{\alpha^4}(x)$.

Zobecněním druhého z těchto pozorování je následující věta:

Věta 8.1.3. *Pro $\beta \in \mathbb{F}_{p^m}$ platí*

$$M_\beta(x) = M_{\beta^p}(x).$$

Důkaz. Podle tvrzení 5.5.1(ii) je

$$M_\beta(\beta^p) = (M_\beta(\beta))^p = 0.$$

□

Cvičení

► **8.1.1.** Nechť F je rozšíření tělesa $\mathbb{F}_p$ o kořen α ireducibilního polynomu $f(x)$. Potom minimální polynom prvku α nad $\mathbb{F}_p$ je právě $f(x)$.

Kapitola 9

Cyklické kódy

9.1 Kód jako množina polynomů

Lineární kód C (délky n nad tělesem $\mathbb{F}_q$) je *cyklický*, pokud je invariantní vzhledem k cyklickému posunu souřadnic, tedy

$$(a_0, \ldots, a_{n-1}) \in C \implies (a_1, \ldots, a_{n-1}, a_0) \in C$$

pro každé slovo $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$.

Cyklické kódy úzce souvisí s polynomy nad tělesem $\mathbb{F}_q$. Každou n-tici $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ formálně ztotožníme s polynomem

$$\sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q^n[x].$$

Protože se tato korespondence týká pouze prvních n mocnin proměnné x, můžeme a ztotožnit s třídou okruhu

$$R = \mathbb{F}_q[x]/\langle x^n - 1\rangle,$$

který si můžeme představovat jako okruh polynomů stupně $\leq n-1$ s počítáním 'modulo rovnost $x^n = 1$'. I v dalším textu se (s malou dávkou nepřesnosti) této představy přidržíme a ztotožníme každou třídu z okruhu R s jednoznačně určeným polynomem stupně $\leq n-1$, který tato třída obsahuje.

Cyklický posun souřadnic v řeči polynomů odpovídá násobení polynomem x, neboť

$$x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = a_{n-1} + a_0 x + \cdots + a_{n-2}x^{n-1}.$$

Cyklický kód je tedy (aditivní) podgrupa okruhu R, invariantní k násobení skalárem a polynomem x, tedy nutně i k násobení libovolným polynomem. Je to tedy totéž co *ideál v okruhu* R.

Následující tvrzení ukazuje, že každý ideál $J \subset R$ je *hlavní*, tj. je tvaru

$$\langle \beta \rangle = \{\sigma \cdot \beta \,:\, \sigma \in R\}$$

pro nějaké $\beta \in R$. Okruh R je tedy *obor hlavních ideálů*. Platí-li $J = \langle \beta \rangle$, říkáme, že β *generuje* ideál β. (Doporučujeme po přečtení důkazu provést cvičení 9.2.2.)

Tvrzení 9.1.1. *Nechť β je polynom minimálního stupně v cyklickém kódu C délky n. Potom platí:*

(1) β generuje kód C, tedy $C = \langle \beta \rangle$,

(2) β dělí polynom $x^n - 1$.

Důkaz. (i) Nechť γ je libovolný polynom z C. Podle věty o dělení se zbytkem (cvičení 9.2.1) je

$$\gamma = \sigma \cdot \beta + \tau,$$

kde τ je polynom menšího stupně než β a přitom zjevně $\tau \in C$. Z minimality stupně polynomu β je $\tau = 0$.

(ii) Opět podle věty o dělení se zbytkem je

$$x^n - 1 = \sigma \cdot \beta + \tau,$$

kde $\deg \tau < \deg \beta$. V okruhu R počítáme modulo $x^n - 1$, takže zde platí $\tau = -\sigma\beta$, a tedy $\tau \in C$. Odtud opět $\tau = 0$. □

Generující polynom cyklického kódu C je polynom, který jej generuje jako ideál. Důsledkem tvrzení 9.1.1 je, že každý cyklický kód obsahuje generující polynom β.

Všimněme si ještě, že ačkoli generujících polynomů může být více, polynom minimálního stupně v kódu C je jednoznačně určen až na konstantní násobek. Jsou-li totiž α, β dva různé polynomy minimálního stupně a jsou-li *monické* (tj. s vedoucím koeficientem 1), potom polynom $\alpha - \beta \in C$ má nižší stupeň, což je spor.

Z generujícího polynomu β kódu C lze odvodit elegantní tvar jeho generující matice. Dejme tomu, že $\deg \beta = k$. Množina $B = \{\beta, x\beta, \ldots, x^{n-k-1}\beta\}$ je lineárně nezávislá modulo $x^n - 1$, protože každá netriviální lineární kombinace z B má stupeň mezi k a $n-1$. Na druhou stranu B generuje celý kód C, protože každé $\gamma \in C$ je násobkem polynomu β. Množina B je tedy bází kódu C. Je-li $\beta = \sum_{i=0}^{k} b_i x^i$, pak jedna generující matice tohoto kódu má tvar

$$M(C) = \begin{pmatrix} b_0 & b_1 & \ldots & b_k & 0 & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{k-1} & b_k & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & & & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & b_k \end{pmatrix}.$$

Speciálně vidíme, že dimenze kódu C je $n-k$.

Jak vypadá duální kód $C^\perp$? Polynom β dělí x^n-1. Uvažme tedy polynom $\delta = \sum_{i=0}^{n-k} d_i x^i$ stupně $n-k$ s vlastností

$$\delta = \frac{x^n-1}{\beta}.$$

Při počítání modulo x^n-1 je každý koeficient součinu $\beta\cdot\delta$ nulový, takže pro všechna $j=0,\ldots,n-1$ je

$$b_0 d_j + b_1 d_{j-1} + \cdots + b_{n-1} d_{j-n+1} = 0, \tag{9.1}$$

přičemž všechny indexy redukujeme modulo n a definujeme $b_i = 0$ pro $i > k$, $d_i = 0$ pro $i > n-k$. Speciálně pro $j = 0,\ldots,n-k$ rovnice (9.1) znamenají, že vektor $d = (d_{n-k}, d_{n-k-1}, \ldots, d_0, 0, \ldots, 0)$ je ortogonální na všechny řádky generující matice $M(C)$, a je tedy prvkem duálního kódu $C^\perp$. Naopak každý prvek d duálního kódu (se stejně indexovanými složkami) splňuje rovnice (9.1) pro všechna j.

Všechny polynomy tvaru $x^i\delta$ mají s polynomem β nulový součin (modulo x^n-1). Proto také všechny cyklické posuny vektoru d patří do duálního kódu $C^\perp$. Dimenze duálního kódu je k. Množina[1] $\{\delta, x^{n-1}\delta, \ldots, x^{n-k+1}\delta\}$ je lineárně nezávislá, takže k cyklických posunů vektoru d tvoří bázi duálního kódu:

$$M(C^\perp) = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \ldots & d_0 & 0 & 0 & \ldots & 0 \\ 0 & d_{n-k} & \ldots & d_1 & d_0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & & & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & d_0 \end{pmatrix}.$$

Všimněme si, že se *nejedná* o kód $\langle\delta\rangle$! Tyto dva kódy se však liší jen pořadím souřadnic v kódových slovech a jsou tedy ekvivalentní.

9.2 Cyklotomické polynomy

Podle tvrzení 9.1.1 má každý cyklický kód délky n generující polynom, který dělí x^n-1. Je tedy namístě otázka, co lze říci o jednoznačném rozkladu polynomu x^n-1 na monické ireducibilní polynomy, kterým se v tomto případě říká *cyklotomické polynomy*. Každý cyklický kód délky n (nad příslušným tělesem) je totiž generován součinem některých z těchto ireducibilních faktorů. Známe-li tedy příslušný rozklad, známe všechny cyklické kódy délky n.

[1] Na první pohled vypadá přirozeněji volba $\{\delta, x\delta, \ldots, x^{k-1}\delta\}$, takto však vyjde elegantnější tvar generující matice.

Uvažme jednoduchý příklad nad $\mathbb{F}_2$. Polynom x^3-1 (alias x^3+1) má rozklad

$$x^3+1=(x+1)(x^2+x+1)$$

a jeho monickými děliteli jsou tedy polynomy 1, $x+1$, x^2+x+1 a 0 (poslední člen odpovídá součinu obou faktorů, který je 0 modulo x^3+1). Slova odpovídající jednotlivým dělitelům a kódy, které generují, jsou uvedeny v následující tabulce.

polynom	slovo	kód
1	(100)	$\{000,100,010,001,110,011,101,111\}$
$x+1$	(110)	$\{000,110,011,101\}$
x^2+x+1	(111)	$\{000,111\}$
0	(000)	$\{000\}$

Pro zbytek této kapitoly učiníme následující předpoklad:

$$\text{délka kódu } n \text{ je nesoudělná s velikostí tělesa } q. \tag{9.2}$$

Za této podmínky jsou kořeny polynomu x^n-1 v jeho rozkladovém nadtělese navzájem různé (viz cvičení 9.2.3). Z toho také plyne, že faktory v jeho ireducibilním rozkladu jsou různé. Je-li tento rozklad

$$x^n-1=p_1\cdot\dots\cdot p_m, \tag{9.3}$$

pak kódy odpovídající faktorům p_i se nazývají *maximální kódy* a značí se M_i^+, jejich duály (generované polynomy $(x^n-1)/p_i$) jsou *minimální kódy* M_i^-. Důvodem pro název minimální kód je, že tyto kódy neobsahují jiný cyklický kód jako vlastní podmnožinu.

Příklad 9.2.1. Určeme minimální kódy pro $q=3$ a $n=8$. Polynom $x^8-1\in\mathbf{Z}_3[x]$ má rozklad

$$x^8-1=(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1).$$

Označme faktory zleva doprava $p_1,\dots,p_5$. Platí např.

$$\frac{x^8-1}{x^2+x-1}=x^6-x^5-x^4-x^2+x+1,$$

takže kód M_4^- je generován cyklickými posuny vektoru $(0\ 1\ -1\ -1\ 0\ -1\ 1\ 1)$. Kromě nich už dokonce žádné nenulové prvky neobsahuje, protože jeho dimenze je 2 (stupeň polynomu $p_4=x^2+x-1$). Jedná se tedy o $[8,2,6]$-kód.

Podobně kód M_5^- je tvořen cyklickými posuny vektoru $(0\ 1\ 1\ -1\ 0\ -1\ -1\ 1)$ a nulovým vektorem. Sjednocení těchto kódů generuje kód $C((x-1)(x+1)(x^2+1))=\langle x^4-1\rangle$ (viz cvičení 9.2.5), což je $[8,4,2]$-kód, generovaný též cyklickými posuny vektoru $(1\ 0\ 0\ 0\ -1\ 0\ 0\ 0)$.

Kód M_1^- je 1-dimenzionální kód generovaný vektorem $(1\ 1\dots1)$, neboť $x^8-1=(x-1)(x^7+x^6+\dots+1)$. Zbylé minimální kódy lze určit podobně.

Příklad 9.2.2. (Hammingův kód $\mathcal{H}_3$) Nechť $q = 2$ a $n = 7$. Platí

$$x^7 - 1 = x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Kód $\langle x^3 + x + 1\rangle$ má generující matici

$$M(\langle x^3 + x + 1\rangle) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

a je to tedy Hammingův kód $\mathcal{H}_3$.

Jaký je řád rozkladového nadtělesa polynomu $x^n - 1$? Jinými slovy, jaké je nejmenší m, pro které platí, že v $\mathbb{F}_{q^m}$ existuje n různých prvků β s vlastností $\beta^n = 1$? Nutnou podmínkou je

$$n | q^m - 1, \tag{9.4}$$

neboť podle Lagrangeovy věty řád každého prvku multiplikativní grupy tělesa $\mathbb{F}_{q^m}$ dělí řád grupy. Takové m jistě existuje, neboť podle malé Fermatovy věty pro každé n a nenulové a platí

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

(ϕ je Eulerova funkce). Na druhou stranu, pokud je podmínka (9.4) splněna, pak stačí zvolit

$$\beta = \alpha^{(q^m-1)/n},$$

kde α je primitivní prvek daného tělesa. Prvky $\beta, \beta^2, \ldots, \beta^n$ jsou pak zjevně hledané kořeny polynomu $x^n - 1$. Dostáváme následující tvrzení:

Tvrzení 9.2.3. *Rozkladové těleso polynomu $x^n - 1$ nad $\mathbb{F}_q$ je těleso $\mathbb{F}_{q^m}$, kde m je nejmenší číslo s vlastností $q^m \equiv 1 \pmod{n}$.* □

Kořeny polynomu $x^n - 1$ v jeho rozkladovém tělese (a v rozšířeních tohoto tělesa) se nazývají *n-té odmocniny z jedné*. Jaký je vztah faktorů polynomu $x^n - 1$ nad $\mathbb{F}_q$ a jeho kořenů v rozkladovém nadtělese? Jsou to jejich minimální polynomy. Každý kořen β polynomu $x^n - 1$ je totiž kořenem právě jednoho polynomu p_i z rozkladu (9.3). Ten je ireducibilní a monický, a tak musí být minimálním polynomem prvku β nad $\mathbb{F}_q$.

Nechť α je primitivní prvek tělesa $\mathbb{F}_{q^m}$. Víme, že má-li prvek $\alpha^k \in \mathbb{F}_{q^m}$ minimální polynom $M^{(k)}$ nad $\mathbb{F}_q$, pak $M^{(k)}$ je rovněž minimálním polynomem všech prvků α^ℓ, kde ℓ patří do *cyklotomické třídy prvku k* modulo n nad $\mathbb{F}_q$,

$$C_k = \{k, qk, q^2k, \ldots, q^{t_k-1}k\} \subset \mathbf{Z}_{q^m-1},$$

přičemž t_k je nejmenší takové, že n dělí $q^{t_k}k$. Platí dokonce

$$M^{(k)} = \prod_{i \in C_k} (x - \alpha^i).$$

Ilustrujme tento fakt na příkladu 9.2.2, kde $q = 2$ a $n = 7$. Zajímá nás vyjádření ireducibilních faktorů polynomu $x^7 + 1$. Podle tvrzení 9.2.3 je rozkladovým tělesem rozšíření $\mathbb{F}_8 \supset \mathbb{F}_2$, dejme tomu s primitivním prvkem α, splňujícím rovnost $\alpha^3 + \alpha + 1 = 0$. Cyklotomické třídy vypadají takto:

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 2, 4\}, \\ C_3 &= \{3, 5, 6\}. \end{aligned}$$

Odtud dostáváme vyjádření cyklotomických polynomů

$$\begin{aligned} M^{(0)} &= x + 1, \\ M^{(1)} &= (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1, \\ M^{(3)} &= (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) = x^3 + x^2 + 1. \end{aligned} \tag{9.5}$$

Cvičení

► **9.2.1.** Ukažte, že v okruhu polynomů $\mathbb{F}_q[x]$ platí *věta o dělení se zbytkem*: jsou-li α, β dva polynomy z $\mathbb{F}_q[x]$ a $\beta \neq 0$, pak existují jednoznačně určené polynomy $\sigma, \tau \in \mathbb{F}_q[x]$ tak, že

$$\alpha = \sigma\beta + \tau$$

a stupeň polynomu τ je menší než stupeň polynomu β.

► **9.2.2.** Formulujte a dokažte tvrzení 9.1.1 zcela přesně, bez neformálního ztotožnění tříd z okruhu R s jejich reprezentanty.

► **9.2.3.** Nechť $f = \sum_{i=0}^{n} a_i x^i$ je polynom nad tělesem $\mathbb{F}_q$. Jeho *derivace*, definovaná předpisem

$$f' = \sum_{i=1}^{n} (i \cdot a_i) \times x^{i-1},$$

je rovněž polynom nad $\mathbb{F}_q$. Dokažte:

(a) Je-li z násobným kořenem polynomu f, potom $f'(z) = 0$.

(b) Je-li n nesoudělné s q, pak polynom $x^n - 1$ nemá žádné násobné kořeny.

► **9.2.4.** Je pravda, že pokud n je soudělné s q, pak $x^n - 1$ má nad $\mathbb{F}_q$ vždy násobný kořen?

► **9.2.5.** Nechť f, g jsou polynomy nad $\mathbb{F}_q$. Dokažte:

$$\langle f\rangle \cap \langle g\rangle = \langle \mathrm{nsn(f,g)}\rangle,$$
$$\langle f\rangle \cup \langle g\rangle \text{ generuje kód } \langle \mathrm{nsd(f,g)}\rangle,$$

kde nsn a nsd označují nejmenší společný násobek resp. největší společný dělitel.

9.3 BCH kódy

Nechť C je cyklický kód délky n nad $\mathbb{F}_q$ s generujícím polynomem g. Polynom g dělí $x^n - 1$ a je tedy součinem některých cyklotomických polynomů z rozkladu (9.3). Kód C lze specifikovat výčtem prvků rozkladového tělesa $\mathbb{F}_{q^m}$ polynomu $x^n - 1$, které mají být kořeny jeho generujícího polynomu. Takové prvky jsou pak samozřejmě kořeny všech polynomů z C, proto se jim říká *kořeny kódu* C.

Typicky ovšem každý určený kořen generujícího polynomu vynucuje ještě další kořeny. Je-li prvek α^i kořenem kódu C (kde α je primitivní prvek rozkladového nadtělesa), pak jsou kořeny i všechny prvky $\{\alpha^j : j \in C_i\}$.

Pomocí kořenů generujícího polynomu lze definovat i tzv. *BCH kódy* (název je zkratkou jmen Bose, Ray-Chaudhuri a Hocquenghem). BCH kód je určen několika hodnotami:

- velikost abecedy q (jde o lineární kód nad tělesem $\mathbb{F}_q$, kde q je mocnina prvočísla),
- délkou $n = q^m - 1$,
- *zadanou vzdáleností* δ.

Kód daný těmito parametry označíme $\mathrm{BCH}_{q,m,\delta}$. Je to cyklický kód[2] délky $n = q^m - 1$ nad $\mathbb{F}_q$, tvořený všemi polynomy s kořeny $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$, kde α je primitivní prvek tělesa $\mathbb{F}_{q^m}$.

Příklad 9.3.1. Hammingův kód $\mathcal{H}_3$ je BCH kód se zadanou vzdáleností 3, která předepisuje kořeny α a α^2 v tělese $\mathbb{F}_8$ s primitivním prvkem α splňujícím rovnost $\alpha^3 = \alpha + 1$. Oba tyto kořeny mají stejný minimální polynom, totiž $M^{(1)} = x^3 + x + 1$, a vynucují ještě třetí kořen tohoto polynomu, prvek α^4.

[2]Poznamenejme, že standardní definice BCH kódů je o něco širší; jednak α nemusí nutně být primitivní prvek, jednak posloupnost mocnin prvku α může začínat u nějaké vyšší mocniny α^t. Naše BCH kódy se obvykle označují jako *primitivní BCH kódy v užším smyslu*. Vše podstatné však i v této menší třídě zůstává zachováno.

Z definice plyne, že paritní maticí kódu $\mathrm{BCH}_{q,m,\delta}$ je matice H', kterou získáme, pokud v matici

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix}, \tag{9.6}$$

nahradíme každou mocninu $\alpha^j \in \mathbb{F}_{q^m}$ odpovídajícím vektorem délky m nad $\mathbb{F}_q$.

Protože každá $(\delta-1)$-tice sloupců matice H je lineárně nezávislá nad $\mathbb{F}_{q^m}$ (její determinant je Vandermondův determinant, viz cvičení 6.2.1), minimální vzdálenost BCH kódu je alespoň δ. Malým zobecněním tohoto faktu je následující pozorování:

Pozorování 9.3.2 (BCH nerovnost)**.** *Minimální vzdálenost kódu* $\mathrm{BCH}_{q,m,\delta}$ *je větší nebo rovna zadané vzdálenosti* δ*.* □

Paritní matice H' má $m(\delta-1)$ řádků (které ovšem nemusí všechny být lineárně nezávislé). Dostáváme tak dolní odhad na dimenzi kódu:

$$\dim \mathrm{BCH}_{q,m,\delta} \geq q^m - m(\delta-1) - 1. \tag{9.7}$$

9.4 BCH kódy jako specializace RS kódů

BCH kódy je rovněž možné velmi elegantně definovat jako jisté podmnožiny Reed–Solomonových kódů. Postup, který ukážeme, je převzat z [9]. Nechť jsou dána čísla q, m, δ jako v minulém oddílu. Učiníme navíc technický předpoklad[3], že m je prvočíslo. Příslušný kód budeme označovat $\mathrm{BCH}_{q,m,\delta}$. Získáme jej takto: nejprve vezmeme Reed–Solomonův kód o 'správné' délce n a minimální vzdálenosti δ (tedy kód $\mathrm{RS}_{q^m,q^m-\delta}$). To je ovšem kód nad tělesem $\mathbb{F}_{q^m}$, zatímco my potřebujeme q-ární kód. Vybereme tedy z daného RS kódu slova, která mají všechny složky v $\mathbb{F}_q$. Výsledkem je kód $\mathrm{BCH}_{q,m,\delta}$.

Je jasné, že délka tohoto kódu je n a jeho minimální vzdálenost d je *alespoň* δ. Trochu obtížnější je zdola odhadnout jeho dimenzi. Výchozí kód $\mathrm{RS}_{q^m,q^m-\delta}$ je tvořen evaluacemi polynomů stupně $< q^m - \delta$ v bodech $1, \alpha, \dots, \alpha^{q^m-2}$, kde α je zvolený primitivní prvek tělesa $\mathbb{F}_{q^m}$. My v něm potřebujeme najít dostatečně mnoho slov se všemi složkami v $\mathbb{F}_q$. K tomu nám dobře poslouží tzv. stopa.

Stopa prvku $z \in \mathbb{F}_{q^m}$ je prvek

$$\operatorname{tr} z = z + z^q + z^{q^2} + \dots + z^{q^{m-1}}. \tag{9.8}$$

[3]Bez tohoto předpokladu je v argumentu mezera, kterou jsem si uvědomil až při jeho sepisování. Ilustrací je polynom x^{10} nad $\mathbb{F}_{16}$, který má nulovou stopu a ukazuje, že některé cyklotomické třídy nemusejí poskytovat 'bázový' polynom s hodnotami v $\mathbb{F}_2$.

Podle cvičení 9.4.3 je stopa lineární funkce $\mathrm{tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$.

Stopu můžeme definovat i pro polynomy. Nejprve zavedeme pojem, který se nám bude hodit i později, v kapitole o cyklických kódech. Nechť i je prvek cyklické grupy $\mathbf{Z}_{q^m-1}$. *Cyklotomická třída* prvku i modulo $q^m - 1$ je množina

$$C_i = \{i, iq, iq^2, \ldots, iq^{m-1}\} \subset \mathbf{Z}_{q^m-1}. \tag{9.9}$$

Je zřejmé, že cyklotomické třídy tvoří rozklad grupy $\mathbf{Z}_{q^m-1}$.

Stopa monomu ax^i, kde $a \in \mathbb{F}_{q^m}$, je

$$\mathrm{Tr}\,(ax^i) = ax^i + a^q x^{\{iq\}} + a^{q^2} x^{\left\{iq^2\right\}} + \cdots + a^{q^{m-1}} x^{\left\{iq^{m-1}\right\}}, \tag{9.10}$$

kde zápis $\{iq^j\}$ označuje fakt, že číslo iq^j redukujeme modulo $q^m - 1$ (tj. interpretujeme jako prvek grupy $\mathbf{Z}_{q^m-1}$). Všimněme si, že polynom $\mathrm{Tr}\, x^i$ má nenulový koeficient u x^j právě tehdy, když $j \in C_i$ (a to díky předpokladu, že m je prvočíslo).

Nyní můžeme definovat stopu obecného polynomu $f(x) = \sum_{i=0}^{n} a_i x^i$ nad tělesem $\mathbb{F}_{q^m}$:

$$\mathrm{Tr}\, f = \mathrm{Tr}\, a_0 + \mathrm{Tr}\, a_1 x + \cdots + \mathrm{Tr}\, a_n x^n. \tag{9.11}$$

Stopa $\mathrm{Tr}\, f$ je polynom v x, jehož hodnoty jsou všechny v $\mathbb{F}_q$. Je-li jeho stupeň menší než $q^m - \delta$, pak určuje jedno slovo kódu $\mathrm{BCH}_{q,m,\delta}$. (Připomeňme, že se snažíme o dolní odhad na dimenzi tohoto kódu.) Kolik různých stop s daným omezením na stupeň dokážeme najít?

Množina B sestává z největších prvků všech cyklotomických tříd C_i ($i \geq 1$). (Uspořádáním je zde standardní uspořádání na množině $\{1, \ldots, q^m - 1\}$.) Pro $j \in B$ je stupeň polynomu $\mathrm{Tr}\, x^j$ právě j a tento polynom má nenulové koeficienty pouze u členů x^i s $i \in C_j$. Jak velká je množina B? Protože m je prvočíslo a velikost každé cyklotomické třídy musí dělit m, pro $i > 0$ platí $|C_i| = m$. Odtud $|B| = (q^m - 2)/m$.

Nechť nyní

$$B' = \{i \in B \,:\, i < q^m - \delta\}. \tag{9.12}$$

Každý prvek i množiny B' určuje monom x^i, jehož stopa má menší stupeň než $q^m - \delta$ a její evaluace tak patří do kódu $\mathrm{BCH}_{q,m,\delta}$. Zjevně

$$|B'| \geq |B| - \delta = \frac{q^m - 2}{m} - \delta. \tag{9.13}$$

Proto množina $\mathcal{B}$, sestávající z polynomů

$$\mathrm{Tr}\left(\sum_{i \in B'} \beta_i x^i\right), \tag{9.14}$$

kde koeficienty β_i probíhají $\mathbb{F}_{q^m}$, má velikost

$$|\mathcal{B}| = (q^m)^{\frac{q^m-2}{m} - \delta} = q^{q^m - 2 - m\delta},$$

a protože polynomy z $\mathcal{B}$ určují navzájem různá slova kódu $\mathrm{BCH}_{q,m,\delta}$, je dimenze tohoto kódu alespoň $q^m - m\delta - 2$. Naše zjištění shrnuje následující věta:

Věta 9.4.1. *Kód* $\mathrm{BCH}_{q,m,\delta}$ *má parametry* $[n,k,d]$, *kde* $n = q^m - 1$, $k \geq n - m\delta - 1$ *a* $d \geq \delta$. □

Poznamenejme, že skutečná vzdálenost BCH kódu může být větší než zadaná vzdálenost δ. Stejně tak dimenze je větší než náš dolní odhad (viz cvičení 9.4.5).

Cvičení

► **9.4.1.** Nechť $f(x) = \sum_{i=0}^{n} a_i x^i$ je polynom stupně n nad tělesem F. Dokažte:

(a) f má nejvýše n různých kořenů,

(b) je-li t násobný kořen polynomu f, pak derivace

$$f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}$$

má kořen v t. (Násobení číslem i je definováno jako i-násobné sečtení.)

► **9.4.2.** Nechť q je mocnina prvočísla, $m \geq 1$ a nechť F je těleso $\mathbb{F}_{q^m}$. Ukažte, že:

(a) pro každé $x, y \in F$ platí $(x+y)^q = x^q + y^q$,

(b) pro každé $x \in F$ je $x^{q^m} = x$,

(c) kořeny polynomu $x^q - x$ v tělese F tvoří těleso $F' \cong \mathbb{F}_q$.

► **9.4.3.** Nechť q je mocnina prvočísla, $m \geq 1$ a nechť F je těleso $\mathbb{F}_{q^m}$. Ukažte, že:

(a) stopa $\operatorname{tr} x$ libovolného prvku $x \in F$ (viz (9.8)) je prvkem tělesa F',

(b) pro každé $x, y \in F$ je $\operatorname{tr}(x+y) = \operatorname{tr} x + \operatorname{tr} y$.

► **9.4.4.** Ukažte, že prvky tělesa F' ze cvičení 9.4.2 jsou právě všechny součty

$$1 + \cdots + 1$$

v tělese $F = \mathbb{F}_{q^m}$.

► **9.4.5.** (a) Nechť C_i je cyklotomická třída prvku i modulo $q^m - 1$, kde q je mocnina prvočísla. Dokažte, že pokud pro nějaké j platí $q^m - 1 - qj \in C_i$, pak $q^m - 1 - j \in C_i$.

(b) Odvoďte odhad

$$|B'| \geq q^m - 2 - m\left\lceil \frac{q-1}{q} \cdot \delta \right\rceil$$

pro velikost množiny B' definované vztahem (9.12).

(c) Odvoďte, že pro libovolné t a prvočíslo m je dimenze binárního kódu $\mathrm{BCH}_{2,m,2t+1}$ alespoň $n - 1 - t\log(n+1)$, kde $n = 2^m - 1$. Porovnejte s Hammingovým odhadem.

▶ **9.4.6.** * Ukažte, že definice BCH kódů pomocí kořenů generujícího polynomu a pomocí RS kódů jsou ekvivalentní.

9.5 QR kódy

Nechť p je liché prvočíslo. *Kvadratický zbytek* (nebo jen *zbytek*) modulo p je každý nenulový prvek grupy $\mathbf{Z}_p$ tvaru a^2, kde $a \in \mathbf{Z}_p$. Prvkům množiny $\mathbf{Z}_p^* = \mathbf{Z}_p - \{0\}$, které nejsou kvadratické zbytky, budeme říkat *nezbytky*.

Pro pevné p nechť R je množina zbytků a N množina nezbytků modulo p. V posloupnosti $1^2, 2^2, \ldots, (p-1)^2$ se každý zbytek objeví dvakrát, protože $a^2 = (-a)^2$ a pro liché p platí $a \neq -a$. Odtud $|R| = |N| = (p-1)/2$.

Pro $r \in R$ platí $b \in R$, právě když $rb \in R$. Obě množiny R a N jsou tedy uzavřené na násobení kvadratickým zbytkem. Tvrdíme, že součin dvou nezbytků musí být zbytek. Pro $n \in N$ jsou totiž součiny $n \cdot b$, kde $b \in \mathbf{Z}_p^*$, navzájem různé a víme, že pro každé $b \in R$ jsou v R. Tím jsou vyčerpány všechny zbytky, takže pro $b \in N$ musí být $nb \in N$.

QR kódy (*quadratic residue codes*) jsou cyklické kódy nad $\mathbb{F}_q$ definované pomocí kvadratických zbytků modulo p, kde p prvočíslo s vlastností, že q je zbytek modulo p. Soustředíme se na binární případ $q = 2$, pro který platí následující věta.

Věta 9.5.1 (Gauss)**.** *Nechť p je liché prvočíslo. Číslo 2 je kvadratický zbytek modulo p, právě když platí*

$$p \equiv \pm 1 \pmod 8.$$

Nechť tedy p je pevné prvočíslo splňující podmínku z věty 9.5.1 a $R, N \subset \mathbf{Z}_p^*$ jsou příslušné množiny kvadratických zbytků resp. nezbytků modulo p. Předpoklad $2 \in R$ znamená, že pro $i \in R$ je $2i \in R$, a množina R je tedy sjednocením cyklotomických tříd modulo p nad $\mathbb{F}_2$.

Nechť α je primitivní prvek rozkladového těleso polynomu $x^p - 1$ nad $\mathbb{F}_2$. Definujme polynomy

$$r(x) = \prod_{i \in R}(x - \alpha^i),$$
$$n(x) = \prod_{i \in N}(x - \alpha^i).$$

Protože R je sjednocením cyklotomických tříd, polynom r má koeficienty z $\mathbb{F}_2$ (je součinem cyklotomických polynomů nad $\mathbb{F}_2$). Totéž platí pro polynom n. Navíc platí

$$x^p - 1 = (x-1) \cdot r \cdot n.$$

Cyklické kódy $\mathcal{R} = \langle r \rangle$ a $\mathcal{N} = \langle n \rangle$ (ideály v okruhu $\mathbb{F}_2[x]/\langle x^p - 1 \rangle$) se označují jako QR kódy.

Příklad 9.5.2. Hammingův kód $\mathcal{H}_3$ je binární QR kód délky 7. Kvadratické zbytky modulo 7 jsou 1, 2 a 4. Je-li α primitivní prvek tělesa $\mathbb{F}_8$ (což je rozkladové těleso polynomu $x^7 + 1$), pak

$$(x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1$$

(viz polynom $M^{(1)}$ v (9.5)).

Příklad 9.5.3. Golayův kód $\mathcal{G}_{23}$ je binární QR kód délky 23. V tomto případě totiž dostáváme

$$r = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

a dá se ukázat, že tento polynom generuje kód $\mathcal{G}_{23}$ (přesněji kód jemu ekvivalentní). Polynom r je dokonce jedním z ireducibilních faktorů polynomu $x^{23} + 1$ (jsou tři).

Je-li u libovolný kvadratický nezbytek v grupě $\mathbf{Z}_p$, pak polynom $r(x^u)$ má za kořeny právě všechny prvky α^i, pro něž je $i \cdot u$ kvadratickým zbytkem. Ovšem násobení libovolným kvadratickým nezbytkem u v grupě $\mathbf{Z}_p$ převádí zbytky na nezbytky a naopak, takže $r(x^u) = n(x)$. Tato úvaha rovněž ukazuje, že kódy $\mathcal{R}$ a $\mathcal{N}$ jsou ekvivalentní.

Protože kvadratických zbytků modulo p je $(p-1)/2$, je dimenze kódů $\mathcal{R}$ a $\mathcal{N}$ rovna $(p+1)/2$ (jak víme, dimenze cyklického kódu délky p s generujícím polynomem stupně k je $p - k$). Odhad na jejich minimální vzdálenost plyne z následující věty.

Věta 9.5.4 (Odmocninový odhad)**.** *Pro minimální vzdálenost d QR kódu $\mathcal{R}$ platí*

$$d^2 \geq p.$$

Důkaz. Uvažme polynom $c(x)$, odpovídající slovu minimální váhy d v kódu $\mathcal{R}$. Nechť u je kvadratický nezbytek modulo p. Z dosavadních úvah plyne, že polynom $c'(x) = c(x^u)$ odpovídá slovu (váhy d) v kódu $\mathcal{N}$. Polynom $c(x) \cdot c'(x)$ je tedy v průniku $\mathcal{R} \cap \mathcal{N}$, a je tedy násobkem polynomu

$$r(x) \cdot n(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}.$$

To znamená, že jeho váha je p. Odtud plyne dokazovaná nerovnost. □

Důsledek 9.5.5. *Kódy $\mathcal{R}$ a $\mathcal{N}$ mají parametry $[p, (p+1)/2, d]$, kde $d \geq \sqrt{p}$.*

Kapitola 10

Hadamardovy kódy a Plotkinův odhad

10.1 Hadamardovy matice

Hadamardova matice řádu n je čtvercová matice $H \in \mathbf{R}^{n\times n}$ s položkami ± 1 a s vlastností

$$H \cdot H^T = nI, \tag{10.1}$$

která je ekvivalentní podmínce, že každé dva různé řádky se shodují právě v polovině položek. Všimněme si, že z (10.1) plyne $H^T = nH^{-1}$, takže $H^T H = HH^T = nI$. Proto také každé dva různé *sloupce* mají právě polovinu shodných položek.

Tento typ matic studoval J. Hadamard v souvislosti s determinantem. Platí totiž

$$\det H = \sqrt{\det H \cdot \det H^T} = \pm n^{n/2}$$

a dá se ukázat, že $n^{n/2}$ je maximální možná absolutní hodnota determinantu reálné matice s prvky m_{ij}, kde $|m_{ij}| \leq 1$. (Není to tak těžké, uvědomíme-li si souvislost mezi determinantem a objemem rovnoběžnostěnu.)

Zde je několik Hadamardových matic malých řádů (místo ± 1 píšeme jen $+$ resp. $-$):

$$(\ +\ ) \qquad \begin{pmatrix} + & + \\ + & - \end{pmatrix} \qquad \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix}.$$

Tyto matice jsou *normalizované*: první řádek obsahuje pouze prvky $+1$. Protože změnou všech znamének v libovolném sloupci se neporuší 'hadamardovskost' matice, každou Hadamardovu matici lze převést do normalizovaného tvaru.

Hadamardova matice řádu n samozřejmě nemůže existovat pro liché $n \geq 3$. Vyloučit lze i další řády:

Věta 10.1.1. *Pokud existuje Hadamardova matice řádu n, pak n je* 1, 2 *nebo násobek* 4.

Důkaz. Mějme normalizovanou Hadamardovu matici H řádu $n > 2$. Nechť A je množina sloupců matice H, v nichž je na druhém řádku $+$, a nechť B je množina sloupců, v nichž je $+$ na třetím řádku. Protože první a druhý řádek se shodují v polovině položek, je $|A| = n/2$ a podobně $|B| = n/2$. Druhý a třetí řádek se rovněž shodují v polovině položek a ve zbylé polovině se liší, proto velikost symetrického rozdílu $A \oplus B$ je $n/2$. Vzhledem k tomu, že

$$|A \oplus B| = |A| + |B| - 2|A \cap B|,$$

dostáváme $|A \cap B| = n/4$ a n musí být dělitelné 4. □

Otázka, zda Hadamardova matice existuje pro každý řád dělitelný 4, je slavný otevřený problém. Minimálně pro $n < 428$ byla existence ověřena pomocí počítače (dnes je rekord asi ještě vyšší). Ukážeme si dvě konstrukce, které lze použít pro speciální hodnoty n.

První z nich, *Sylvesterova konstrukce* Hadamardových matic H_m řádu $n = 2^m$ je velmi jednoduchá. Vezměme $H_0 = (+)$ a pro $i \geq 0$ induktivně definujme

$$H_{i+1} = \begin{pmatrix} H_i & H_i \\ H_i & -H_i \end{pmatrix}.$$

Ověření, že výsledkem je Hadamardova matice, ponecháváme na cvičení 10.1.1.

Cvičení

▶ **10.1.1.** Ověřte, že výsledkem Sylvesterovy konstrukce jsou Hadamardovy matice.

10.2 Paleyho konstrukce

Pomocí druhé konstrukce Hadamardových matic, *Paleyovy konstrukce*, lze získat matice řádu $p + 1$, kde p je prvočíslo a $p \equiv 3 \pmod 4$. Konstrukce je založena na kvadratických zbytcích a nezbytcích modulo p, definovaných v oddílu 9.5, kde jsou rovněž odvozeny jejich základní vlastnosti.

Množinu kvadratických zbytků resp. nezbytků modulo p značíme R resp. N. Tvoří rozklad množiny $\mathbf{Z}_p^*$ na dvě části o velikosti $(p-1)/2$. *Legendreův symbol* je zobrazení $\chi : \mathbf{Z}_p \to \{-1, 0, 1\}$ definované vztahem

$$\chi(a) = \begin{cases} 1 & \text{pokud } a \in R, \\ -1 & \text{pokud } a \in N, \\ 0 & \text{pokud } a = 0. \end{cases}$$

Jacobsthalova matice je matice $Q = (q_{ij})$ o rozměrech $p \times p$, definovaná vztahem

$$q_{ij} = \chi(j - i),$$

kde $0 \le i, j \le p - 1$ a odečítání interpretujeme modulo p. Poznatky z oddílu 9.5 se dají vyjádřit vzorcem

$$\chi(ab) = \chi(a) \cdot \chi(b). \tag{10.2}$$

Příklad 10.2.1. Pro $p = 7$ je $R = \{1, 2, 4\}$ a $N = \{3, 5, 6\}$, takže

$$Q = \begin{pmatrix} 0 & + & + & - & + & - & - \\ - & 0 & + & + & - & + & - \\ - & - & 0 & + & + & - & + \\ + & - & - & 0 & + & + & - \\ - & + & - & - & 0 & + & + \\ + & - & + & - & - & 0 & + \\ + & + & - & + & - & - & 0 \end{pmatrix}.$$

Matice Q je vždy antisymetrická. Platí totiž $j - i = (-1)(i - j)$ a díky předpokladu, že $p \equiv 3 \pmod 4$, je prvek -1 kvadratický nezbytek (pro $-1 = a^2$ by řád prvku a v multiplikativní grupě $\mathbf{Z}_p^*$ byl 4, což je nemožné, protože $p - 1$ není dělitelné čtyřmi). Odtud $\chi(i - j) = -\chi(j - i)$.

Následující tvrzení ukazuje, že od Jacobsthalovy matice není příliš daleko k matici Hadamardově.

Tvrzení 10.2.2. *Pro Jacobsthalovu matici Q platí*

$$Q \cdot Q^T = pI - J,$$

kde J je matice ze samých jedniček.

Důkaz. Nechť $M = Q \cdot Q^T$ má prvky m_{ij}, kde $i, j = 0, \ldots, p - 1$. Rozepišme pro $i \neq j$

$$\begin{aligned} m_{ij} &= \sum_{k=0}^{p-1} \chi(k - i) \cdot \chi(k - j) \\ &= \sum_{k=1}^{p-1} \chi(k) \cdot \chi(k + i - j) \\ &= \sum_{k=1}^{p-1} \chi(k^2) \cdot \chi\Big(1 + \frac{i - j}{k}\Big). \end{aligned}$$

Smysl této úpravy je v tom, že člen $\chi(k^2) = 1$ zmizí. Dále výraz $1 + (i - j)/k$ probíhá celou grupu $\mathbf{Z}_p$ kromě prvku 1, takže poslední řádek je roven součtu

$$\Big(\sum_{k \in \mathbf{Z}_p} \chi(k)\Big) - \chi(1) = -1,$$

neboť součet Legendreových symbolů všech prvků grupy je roven 0 (vzpomeňme $|R| = |N|$). Pro $i \neq j$ je tedy $m_{ij} = -1$. Protože m_{ii} je triviálně $p-1$, dostáváme požadovanou rovnost. □

Definujme nyní matici

Věta 10.2.3. *Matice*

$$H = \begin{pmatrix} 1 & \dots & 1 & 1 \\ & & & 1 \\ & Q - I & & \vdots \\ & & & 1 \end{pmatrix}$$

je Hadamardova matice.

Důkaz. Nechť q_k označuje k-tý řádek matice Q. Podle tvrzení 10.2.2 pro $i \neq j$ platí

$$\langle q_i, q_j \rangle = -1. \tag{10.3}$$

Znázorněme schematicky řádky q_i a q_j s vyznačením i-tého a j-tého sloupce.

$$\begin{array}{rcccccc} q_i & = & \dots & 0 & \dots & q_{ij} & \dots \\ q_j & = & \dots & -q_{ij} & \dots & 0 & \dots \end{array}$$

Příspěvek sloupců i a j ke skalárnímu součinu (10.3) je nulový, v ostatních musí tedy nastat $(p-3)/2$ případů shody a $(p-1)/2$ případů neshody mezi řádky q_i a q_j. Při přechodu k matici H přidáváme poslední sloupec, kde vždy nastane shoda. Dále ve sloupcích i a j se nuly změní na $-$, čímž vznikne právě 1 shoda a 1 neshoda. Celkem tedy počet shod i neshod bude $(p+1)/2$. □

10.3 Hadamardovy kódy a Plotkinův odhad

Nechť H je normalizovaná Hadamardova matice řádu n s řádky $r_1, \dots, r_n$. *Hadamardův kód*[1] délky n je každý binární kód, jehož slova získáme záměnou

$$\begin{array}{rcl} + & \longrightarrow & 0, \\ - & \longrightarrow & 1 \end{array}$$

ve všech vektorech r_i a $-r_i$. Je to tedy $(n, \log 2n, n/2)$-kód. Obecně je nelineární, ačkoli například u Hadamardových matic Sylvesterova typu řádu 2^m se jedná o (lineární) Reed–Mullerův kód $\mathcal{R}(1, m)$. Ten mimochodem splývá s rozšířením duálu Hammingova kódu $\mathcal{H}_m$ o paritní symbol.

[1] Existuje několik drobných variací, kterým se rovněž říká Hadamardovy kódy; u jedné se například odstraňuje první sloupec matice H, takže dostaneme kód o délce $n-1$.

Pomocí pěkného geometrického argumentu z [9] lze dokázat, že pro danou délku a vzdálenost jsou Hadamardovy kódy největší možné. Výsledek rovněž plyne z tzv. Plotkinova odhadu, který dokážeme později.

Pro binární slovo $x = (x_1 \dots x_n) \in \mathbb{F}_2^n$ definujme reálný vektor $\phi(x) \in \mathbf{R}^n$, jehož i-tá složka je $(-1)^{x_i}$.

Lemma 10.3.1. *Pro dvě slova x, y platí*

$$\langle \phi(x), \phi(y) \rangle = n - 2d(x, y),$$

kde d je Hammingova vzdálenost.

Důkaz. Příspěvek i-té souřadnice ke skalárnímu součinu je 1, pokud $x_i = y_i$, a -1 v opačném případě. Proto

$$\langle \phi(x), \phi(y) \rangle = \Big(n - d(x, y)\Big) - d(x, y).$$

□

Nechť C je binární kód délky n s minimální vzdáleností alespoň $n/2$. Chceme ukázat, že $|C|$ je nejvýše $2n$. Podle lemmatu 10.3.1 pro skalární součin vektorů $\phi(x)$ a $\phi(y)$, kde $x, y \in C$, platí

$$\langle \phi(x), \phi(y) \rangle \leq 0. \tag{10.4}$$

Horní odhad na velikost kódu C tak plyne z následujícího tvrzení.

Tvrzení 10.3.2. *Nechť $z_1, \dots, z_k$ jsou nenulové vektory v $\mathbf{R}^n$ s vlastností*

$$\langle z_i, z_j \rangle \leq 0 \tag{10.5}$$

pro $i \neq j$. Potom $k \leq 2n$.

Důkaz. Indukcí podle n. Pro $n = 1$ není co dokazovat. Jinak zapišme

$$z_i = (x_i \; z_i'),$$

kde $x_i \in \mathbf{R}$ je první složka vektoru z_i. Skalární součin je invariantní k otočení, proto můžeme předpokládat $z_1 = (1, 0, \dots, 0)$. Aby vektor z_i ($i \geq 2$) měl nekladný součin s vektorem z_1, musí být $x_i \leq 0$. Pak ovšem pro $i, j \geq 2$

$$\langle z_i', z_j' \rangle = \langle z_i, z_j \rangle - x_i x_j \leq 0,$$

takže pro vektory $z_2', \dots, z_k'$ v prostoru $\mathbf{R}^{n-1}$ platí předpoklad (10.5). Ovšem pozor: pro některé z_i může být z_i' nulový vektor. Takové i je díky (10.5) nejvýše jedno. Po případném odstranění nulového vektoru z_i' dostáváme množinu $k-2$ vektorů, na které lze použít indukční předpoklad. Z něj plyne, že $k-2 \leq 2(n-1)$ a tedy $k \leq 2n$. □

Nyní dokážeme binární verzi tzv. *Plotkinova odhadu.*

Věta 10.3.3 (Plotkinův odhad)**.** *Pro velikost binárního kódu C délky n s minimální vzdáleností alespoň $d > n/2$ platí*

$$|C| \leq \frac{2d}{2d-n}. \tag{10.6}$$

Důkaz. Nechť $|C| = M$. Sečtěme Hammingovy vzdálenosti všech dvojic různých slov $x, y \in C$:

$$D = \sum_{x,y \in C} d(x,y) \geq \binom{M}{2} \cdot d. \tag{10.7}$$

Pro $i = 1, \ldots, n$ definujme funkci δ_i, jejíž hodnota pro dvě slova x, y činí

$$\delta_i(x,y) = \begin{cases} 1 & \text{pokud } x_i \neq y_i, \\ 0 & \text{jinak.} \end{cases}$$

Protože $d(x,y) = \sum_i \delta_i(x,y)$, dostáváme

$$D = \sum_{i=1}^{n} \sum_{x,y \in C} \delta_i(x,y). \tag{10.8}$$

Dejme tomu, že na i-té pozici ve slovech kódu C se a-krát objevuje symbol 0 a $(M-a)$-krát symbol 1. Potom

$$\sum_{x,y \in C} \delta_i(x,y) = a(M-a) \leq \frac{M^2}{4},$$

takže z (10.8) plyne

$$D \leq n \cdot \frac{M^2}{4}. \tag{10.9}$$

Složením nerovností (10.7) a (10.9) dostaneme

$$2M(M-1)d \leq nM^2,$$

z čehož snadno plyne (10.6). □

Plotkinova věta nabízí alternativní způsob, jak odvodit maximalitu Hadamardových kódů.

Důsledek 10.3.4. *Pro velikost kódu C o délce n a minimální vzdálenosti alespoň $n/2$ platí*

$$|C| \leq 2n.$$

Důkaz. Při prostém dosazení do Plotkinova odhadu bychom v (10.6) dostali nulový jmenovatel. Musíme proto použít následující trik. Pro $i = 0, 1$ definujme kód C_i délky $n - 1$ předpisem

$$C_i = \{c : \text{slovo } (i \quad c) \text{ je v kódu } C.\}$$

Jeden z těchto kódů (dejme tomu C_0) obsahuje aspoň $|C|/2$ slov. Má délku $n-1$ a minimální vzdálenost alespoň $n/2$. Pro kód C_0 Plotkinův odhad říká

$$|C_0| \leq n$$

a tedy $|C| \leq 2n$. □

Kapitola 11

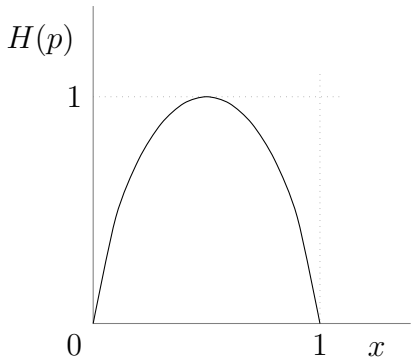
Shannonova věta

11.1 Entropická funkce

Entropická funkce $H(p) : [0,1] \to \mathbf{R}$ je definována předpisem

$$H(p) = \begin{cases} p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p} & \text{pro } p \in (0,1), \\ 0 & \text{pro } p = 0, 1, \end{cases}$$

přičemž logaritmy jsou (stejně jako v celé této přednášce) se základem 2. Graf entropické funkce je na obr. 11.1.



Obrázek 11.1: Entropická funkce.

Z našeho hlediska je klíčovou vlastností entropické funkce souvislost s objemem kombinatorické koule. Nechť x je prvek množiny $\mathbb{F}_2^n$. *Koule* se středem v x o poloměru r je množina

$$B(x,r) = \{y \in \mathbb{F}_2^n \,:\, d(x,y) \leq r\}.$$

Počet prvků ('objem') takové koule, který budeme označovat symbolem $V(n,r)$,

je zjevně

$$V(n,r) = \sum_{i=0}^{r} \binom{n}{i}.$$

Věta 11.1.1 (Objem koule)**.** *Pro* $0 \leq r \leq n/2$ *platí*

$$V(n,r) < 2^{nH(\frac{r}{n})}.$$

Důkaz. Nejprve si všimněme, že z definice entropické funkce po jednoduché úpravě pro $r > 0$ dostaneme

$$2^{nH(\frac{r}{n})} = \frac{n^n}{r^r \cdot (n-r)^{n-r}}.$$

Stejná rovnost navíc platí i pro $r = 0$, definujeme-li (jak je obvyklé) $0^0 = 0$.

Rozepišme podle binomické věty

$$\begin{aligned} n^n = (r + (n-r))^n &= \sum_{i=0}^{n} \binom{n}{i} r^i (n-r)^{n-i} \\ &> \sum_{i=0}^{r} \binom{n}{i} r^r (n-r)^{n-r}. \end{aligned}$$

(Nerovnost plyne z faktu, že pro $r \leq n/2$ hodnota výrazu $r^i(n-r)^{n-i}$ klesá pro i rostoucí k r.) Po vydělení dostáváme požadovaný vztah. □

Dá se dokonce ukázat (viz cvičení 11.4.3), že pro velká n platí $V(n,r) \approx 2^{nH(r/n)}$.

11.2 Několik definic

Nechť C je binární kód. Uvažme přenos po kanálu s pravděpodobností chyby p a dekódujme přijaté slovo w jako nejbližší kódové slovo (není-li jednoznačně určeno, volíme libovolně).

Definujme *spolehlivost* $\varrho_C(p)$ kódu C jako průměrnou pravděpodobnost, že přijaté kódové slovo je správně dekódováno, přičemž průměr je brán přes všechna slova kódu C a výsledek je funkcí pravděpodobnosti p.

Přenášíme binární slovo c délky n po kanálu s pravděpodobností chyby p a zajímá nás, kolik chyb při přenosu nastane. Nechť X_i $(i = 1, \ldots, n)$ je náhodná proměnná, jejíž hodnota je 1, pokud při přenosu i-tého bitu slova c dojde k chybě, a jinak 0 (její střední hodnota je tedy p). Podle linearity střední hodnoty je očekávaný počet chyb při přenosu roven

$$\mathbf{E}\Big[\sum_i X_i\Big] = \sum_i \mathbf{E}\Big[X_i\Big] = np.$$

S pomocí Černovovy nerovnosti lze ukázat, že počet chyb je 'silně koncentrován' kolem této střední hodnoty:

Věta 11.2.1 (Černovova nerovnost)**.** *Nechť $X_1, \ldots, X_n$ jsou nezávislé náhodné proměnné, nabývající hodnoty 1 s pravděpodobností p a hodnoty 0 s pravděpodobností $1-p$. Potom pro $\alpha > 0$*

$$\mathbf{Pr}\big[\sum_{i=1}^{n} X_i \geq n(p+\alpha)\big] \leq \mathrm{e}^{-n\alpha^2/2}.$$

Pravděpodobnost, že dojde při přenosu alespoň k $n(p+\alpha)$ chybám, je tedy nejvýše rovna výrazu na pravé straně Černovovy nerovnosti, který pro rostoucí α a pevné n exponenciálně klesá k 0. Stejně je omezena i pravděpodobnost, že chyb bude jen $n(p-\alpha)$ nebo méně (viz cvičení 11.4.1). Počet chyb tedy bude v intervalu $[n(p-\alpha), n(p+\alpha)]$ s pravděpodobností alespoň

$$1 - 2\mathrm{e}^{-n\alpha^2/2}.$$

Pro pevné α a velké n se tato pravděpodobnost blíží jedné.

11.3 Shannonova věta

Shannonova věta, kterou vyslovíme a dokážeme v tomto odstavci, je jednou z klíčových vět teorie kódů. Jejím obsahem je, že existují 'dobré' kódy — kódy s libovolně vysokou spolehlivostí a s hustotou, která se libovolně blíží jisté hranici (ta je, jak ukážeme v odstavci 11.4, nepřekročitelná). Shannonova věta existuje v různě obecných verzích; my ji dokážeme pro binární kódy a binární symetrický kanál.

Důkaz je netriviální, ale poměrně přímočarý. Důležité a v jistém smyslu charakteristické je, že jde o důkaz nekonstruktivní. Explicitní konstrukce 'dobrých' kódů je těžší problém, který byl po dlouhou dobu základním problémem teorie kódů. Budeme se mu věnovat v oddílu 12.5.

Věta 11.3.1 (Shannon)**.** *Nechť $p \in (0, 1/2)$ a $\kappa < 1 - H(p)$. Potom existují binární kódy C s hustotou alespoň κ a spolehlivostí $\varrho_C(p)$ libovolně blízkou 1.*

Důkaz. Nechť $\varepsilon > 0$. Hledáme kód se spolehlivostí alespoň $1-\varepsilon$ a hustotou alespoň κ. Nechť n je velké (jak přesně velké, vyplyne z důkazu). Můžeme předpokládat, že κn je celé číslo. Kód C zvolíme náhodně: nezávisle vybereme $2^{\kappa n}$ slov z množiny $\mathbb{F}_2^n$. Hustota kódu C je tedy κ. Tvrdíme, že je-li n skutečně dost velké, pak $\varrho_C(p) > 1 - \varepsilon$.

Abychom odhadli spolehlivost kódu C, představme si, že při přenosu kódového slova c bylo přijato slovo $\tilde{c}$. Proběhly tedy celkem dva náhodné procesy:

(a) volba kódu C,

(b) přenos kódového slova c z kódu C, který je v tuto chvíli již pevně zvolen.

Kdy může dojít k chybě při dekódování? Pouze v případě, že pro nějaké kódové slovo $x \neq c$ platí $d(\tilde{c}, x) \leq d(\tilde{c}, c)$. My ukážeme, že tato situace skoro jistě nenastane. Přesněji dokážeme, že při vhodné volbě poloměru r bude koule $B(\tilde{c}, r)$ skoro jistě obsahovat jediné kódové slovo, a to c.

Jaká je pravděpodobnost, že slovo $c \in C$ *není* prvkem koule $B(\tilde{c}, r)$? Tato pravděpodobnost nezávisí na volbě kódu C ani na slově c, ale jen na vlastním přenosu: je to pravděpodobnost, že při přenosu nastane více než r chyb. Podle odstavce 11.2 je očekávaný počet chyb np. Zvolme tedy r o málo větší, řekněme

$$r = n(p + \alpha),$$

kde $\alpha > 0$ je konstanta. Podle téhož odstavce je

$$P_1 := \mathbf{Pr}\big[c \notin B(\tilde{c}, r)\big] \leq \mathrm{e}^{-n\alpha^2/2}.$$

Pro libovolně malé pevné α se pravděpodobnost P_1 s rostoucím n blíží k nule. Slovo c je tedy 'skoro jistě' v kouli $B(\tilde{c}, r)$.

Zbývá omezit pravděpodobnost (dejme tomu P_2), že $B(\tilde{c}, r)$ obsahuje některé kódové slovo $x \neq c$. Ta zase závisí pouze na volbě kódu C, a nikoli na slovech c a $\tilde{c}$. Protože kódová slova kódu C jsou volena nezávisle, platí pro $x \neq c$

$$\mathbf{Pr}\big[x \in B(\tilde{c}, r)\big] = \frac{V(n, r)}{2^n} \leq 2^{nH(r/n)-n} = 2^{n(H(p+\alpha)-1)},$$

přičemž nerovnost plyne samozřejmě z odhadu na objem koule ve větě 11.1.1. Pravděpodobnost P_2, že se do koule $B(\tilde{c}, r)$ dostane některé z $2^{\kappa n} - 1$ 'špatných' kódových slov, je tedy

$$P_2 \leq 2^{n\kappa} \cdot 2^{n(H(p+\alpha)-1)} = 2^{n(H(p+\alpha)+\kappa-1)}.$$

Podle předpokladu je $H(p) + \kappa < 1$. Entropická funkce je spojitá, a tak pro malé α platí $H(p + \alpha) + \kappa < 1$. Pro takové α a velké n se pravděpodobnost P_2 blíží k nule.

Vidíme, že součet $P_1 + P_2$, který omezuje pravděpodobnost chybného dekódování přijatého slova c, je pro velké n menší než ε. Spolehlivost kódu C je tedy s nenulovou pravděpodobností alespoň $1 - \varepsilon$. □

11.4 Inverzní Shannonova věta

Podle Shannonovy věty pro každé $R < 1 - H(p)$ existují binární kódy s hustotou alespoň R, jejichž spolehlivost (pro kanál s pravděpodobností chyby p) se libovolně

blíží jedné. Je namístě otázka, zda lze najít takové kódy i pro hustoty $R > 1 - H(p)$, nebo zda jde o nějakou přirozenou hranici. Inverzní Shannonova věta, kterou vyslovíme a dokážeme dále, tvrdí, že platí druhá možnost: hranice $1-H(p)$ je nepřekročitelná. Z tohoto důvodu se číslu $1 - H(p)$ říká *kapacita* kanálu s pravděpodobností chyby p. Všimněme si, že důsledkem inverzní Shannonovy věty je skutečný opak Shannonovy věty: spolehlivost kódů s hustotou překračující kapacitu kanálu je shora omezena konstantou menší než 1.

Věta 11.4.1 (Inverzní Shannonova věta)**.** *Nechť $\varepsilon, p > 0$ a $R > 1-H(p)$. Potom existuje číslo N takové, že spolehlivost každého binárního kódu C s hustotou alespoň R a délkou alespoň N (pro kanál s pravděpodobností chyby p a pro libovolnou dekódovací funkci) je nejvýše ε.*

Důkaz. Sporem. Předpokládejme, že pro nějaké $\beta > 0$ existují libovolně dlouhé kódy se spolehlivostí aspoň β a hustotou aspoň R. Mějme takový kód C s 'velkou' délkou n (určíme ji později). Příslušnou dekódovací funkci (k níž se vztahuje údaj o spolehlivosti) označme D.

Strategie je následující. Dejme tomu, že při přenosu kódového slova $c \in C$ je přijato slovo $\tilde{c}$ (které je pro nás náhodnou proměnnou). Jak víme z odstavce **??**, vzdálenost slov c a $\tilde{c}$ je 'skoro jistě' zhruba np. Pro každé konkrétní slovo x ve vzdálenosti zhruba np od c je jen 'malá' pravděpodobnost, že $\tilde{c} = x$. Přitom ale spolehlivost (tj. průměrná pravděpodobnost správného dekódování) je 'velká' (je zdola omezena konstantou β). Z toho odvodíme, že 'mnoho' slov x ve vzdálenosti zhruba np od c se musí dekódovat na c. Slov $c \in C$ je ale také 'mnoho', konkrétně $2^{\kappa n}$, a z toho spočítáme, že všech slov délky n by muselo být více než 2^n, což je spor.

Proveďme nyní důkaz podrobně. Zvolme malé $\alpha > 0$. Určíme jej později, zatím poznamenáme, že α nebude záviset na n, ale jen na p a κ. Pro $c \in C$ nechť $S(c)$ je množina všech $x \in \mathbb{F}_2^n$, jejichž vzdálenost od c je v intervalu $[n(p-\alpha), n(p+\alpha)]$. Taková slova x budeme označovat jako *podstatná pro c*. Podle odstavce 11.2 se pravděpodobnost, že $\tilde{c}$ je podstatné pro c, při pevném α pro velké n blíží k jedné. Tato pravděpodobnost nezávisí na slově c. Zvolme tedy n dost velké, aby platilo

$$\mathbf{Pr}\big[\tilde{c} \in S(c)\big] \geq 1 - \beta/2. \tag{11.1}$$

Nechť $D^{-1}(c)$ je množina všech slov, která se dekódují na c. Podle předpokladu o spolehlivosti kódu máme

$$\sum_{c \in C} \mathbf{Pr}\big[\tilde{c} \in D^{-1}(c)\big] \geq |C| \cdot \beta \geq 2^{\kappa n}\beta. \tag{11.2}$$

Chceme zdola odhadnout pravděpodobnost, že $\tilde{c}$ je podstatné pro c a dekóduje se na něj, tedy že leží v průniku množin $D^{-1}(c)$ a $S(c)$. Můžeme použít odhad, který říká, že pravděpodobnost konjunkce $A \wedge B$ jevů A a B je alespoň $\mathbf{Pr}\big[A\big] +$

$\mathbf{Pr}\big[B\big] - 1$ (viz cvičení 11.4.2). Podle (11.1) a (11.2) je pak

$$\begin{aligned}\sum_{c\in C} \mathbf{Pr}\big[\tilde{c} \in D^{-1}(c) \cap S(c)\big] &= \sum_{c\in C} \mathbf{Pr}\big[\tilde{c} \in D^{-1}(c) \ \wedge \ \tilde{c} \in S(c)\big] \\ &\geq \sum_{c\in C} \Big(\mathbf{Pr}\big[\tilde{c} \in D^{-1}(c)\big] + \mathbf{Pr}\big[\tilde{c} \in S(c)\big] - 1\Big) \\ &\geq \sum_{c\in C} \Big(\mathbf{Pr}\big[\tilde{c} \in D^{-1}(c)\big] - \beta/2\Big) \\ &\geq 2^{\kappa n}\beta/2. \end{aligned} \tag{11.3}$$

Aby pro konkrétní slovo $x \in S(c)$ platilo $\tilde{c} = x$, musí při přenosu nastat alespoň $n(p-\alpha)$ chyb. Slovo x, které je bližší slovu c než jiné slovo x', má větší pravděpodobnost, že je rovno slovu $\tilde{c}$ (protože $p < 1/2$). Odtud pro každé $x \in S(c)$

$$\begin{aligned}\mathbf{Pr}\big[\tilde{c} = x\big] &\leq p^{n(p-\alpha)}(1-p)^{n(1-p+\alpha)} \\ &= 2^{-nH(p)} \cdot \Big(\frac{1-p}{p}\Big)^{n\alpha} \end{aligned} \tag{11.4}$$

Z nerovností (11.3) a (11.4) dostáváme vydělením

$$\begin{aligned}\sum_{c\in C} |D^{-1}(c) \cap S(c)| &\geq \frac{2^{\kappa n}\beta/2}{2^{-nH(p)}\big((1-p)/p\big)^{n\alpha}} \\ &= 2^{n\left(\kappa + H(p) - \alpha\log((1-p)/p) + \log(\beta/2)/n\right)}. \end{aligned} \tag{11.5}$$

Množiny $D^{-1}(c)$ jsou pro různá c navzájem disjunktní, takže pravá strana nerovnice musí být nejvýše 2^n. Podívejme se na dlouhou závorku v posledním výrazu. Podle předpokladu je $\kappa + H(p) > 1$. Zlomek $(1-p)/p$ je konstanta, takže můžeme zvolit α tak malé, že

$$\kappa + H(p) - \alpha \log \frac{1-p}{p} > 1.$$

Konečně poslední výraz v dlouhé závorce se pro $n \to \infty$ blíží k nule, takže pro dostatečně velké n bude celá závorka větší než 1. To ale znamená, že pravá strana nerovnice (11.5) je větší než 2^n, což je spor. Tím je důkaz u konce. □

Problém 11.4.2. Ve světle Shannonovy věty se nabízí otázka, jak je tomu s kódy o hustotě *rovné* kapacitě kanálu $1 - H(p)$: existují nebo ne? Přesněji: je pravda, že pro každé $\varepsilon, p > 0$ existují kódy s hustotou $1 - H(p)$ a spolehlivostí aspoň $1 - \varepsilon$? Co když požadujeme pouze spolehlivost zdola omezenou kladnou konstantou? Odpověď neznám.

Cvičení

▶ **11.4.1.** Dokažte pomocí Černovovy nerovnosti, že počet chyb při přenosu binárního slova délky n po kanálu s pravděpodobností chyby p bude v intervalu $[n(p-\alpha), n(p+\alpha)]$ s pravděpodobností alespoň

$$1 - 2\mathrm{e}^{-n\alpha^2/2}.$$

▶ **11.4.2.** Dokažte, že pravděpodobnost konjunkce náhodných jevů A a B je

$$\mathbf{Pr}\big[A \wedge B\big] \geq \mathbf{Pr}\big[A\big] + \mathbf{Pr}\big[B\big] - 1.$$

▶ **11.4.3.** * Dokažte, že pro $p \in (0,1)$ je

$$\lim_{n\to\infty} \frac{\log \binom{n}{pn}}{n} = H(p).$$

Odvoďte dolní odhad pro objem koule $V(n,r)$ analogický hornímu odhadu ve větě 11.1.1.

Kapitola 12

Asymptotika

V kapitole 1 jsme zavedli funkci $A(n, d)$, jejíž hodnotou je maximální k, pro které existuje binární (n, k, d)-kód. Singletonův a Hammingův odhad funkci $A(n, d)$ shora omezují. V této kapitole nejprve odvodíme dolní odhad pro funkci $A(n, d)$, a pak dokážeme asymptotické verze těchto odhadů.

12.1 Asymptotické chování kódů

Začněme otázkou, co je to dobrý kód. Hledisek pro posuzování kódů je více a vzájemně si odporují; obecně například chceme, aby kód měl velkou minimální vzdálenost (protože pak má schopnost opravovat hodně chyb) a zároveň obsahoval co nejvíce slov. Přesto existuje poměrně uspokojivé měřítko kvality kódu, nebo přesněji nekonečné třídy kódů. Připomeňme, že hustota (n, k, d)-kódu C je číslo

$$\alpha(C) = k/n.$$

Definujme podobně *relativní vzdálenost* $\delta(C)$ předpisem

$$\delta(C) = d/n.$$

Nekonečná třída binárních kódů $\mathcal{C}$ je *asymptoticky dobrá*, pokud existují kladné konstanty α, δ s vlastností, že pro každý kód $C \in \mathcal{C}$ je $\alpha(C) > \alpha$ a $\delta(C) > \delta$.

Které z nám známých tříd kódů jsou asymptoticky dobré? Hammingovy kódy mají velkou hustotu, ale jejich minimální vzdálenost je jen 3, takže relativní vzdálenost, $3/n$, se blíží k nule. Triviální třídy kódů (opakovací, totální, paritní kódy) rovněž nejsou dobré. Reed–Solomonovy kódy potřebují velkou abecedu, nejsou binární. Konečně se dá ukázat, že ani binární BCH kódy nejsou asymptoticky dobré. Existuje vůbec nějaká dobrá třída binárních kódů?

12.2 Gilbert–Varshamovův odhad

Věta 12.2.1. *Nechť n, k, d jsou přirozená čísla. Platí-li pro objem kombinatorické koule nerovnost*

$$V(n, d-1) < 2^{n-k+1}, \tag{12.1}$$

pak existuje binární (lineární) $[n, k, d]$-kód.

Důkaz. Pro $k \leq 1$ je tvrzení triviální. Pro vyšší k jej dokazujeme indukcí. Nerovnost (12.1) je splněna i pro $k-1$ na místě k, nechť tedy C je binární $[n, k-1, d]$-kód. Koule $B(c, d-1)$, kde c probíhá slova kódu C, nepokrývají prostor $\mathbb{F}_2^n$, protože jich je 2^{k-1}, každá má objem $V(n, d-1)$ a podle (12.1) je

$$2^{k-1} \cdot V(n, d-1) < 2^n.$$

Existuje tedy nějaké slovo z, které neleží v žádné kouli $B(c, d-1)$ a má tedy od každého slova kódu C vzdálenost aspoň d. Jinými slovy, každý součet $z + c$, kde $c \in C$, má váhu

$$|z + c| \geq d. \tag{12.2}$$

Nechť C' je lineární kód generovaný množinou $C \cup \{z\}$. Ten má dimenzi k (neboť $z \notin C$) a podle (12.2) má minimální váhu alespoň d, protože každý jeho prvek je tvaru c nebo $z + c$, kde $c \in C$. □

Důsledkem věty 12.2.1 je dolní odhad na funkci $A(n, d)$.

Věta 12.2.2 (Gilbert–Varshamovův odhad)**.** *Pro $d \leq n/2$ platí*

$$A(n, d) > n\Big(1 - H\Big(\frac{d-1}{n}\Big)\Big).$$

Důkaz. Podle věty 11.1.1 v kapitole 11 je

$$\log V(n, d-1) < nH\Big(\frac{d-1}{n}\Big).$$

Pokud tedy pro nějaké k platí

$$nH\Big(\frac{d-1}{n}\Big) \leq n - k + 1, \tag{12.3}$$

pak je splněna podmínka věty 12.2.1 a existuje tedy binární $[n, k, d]$-kód. Stačí proto zvolit

$$k = \Big\lfloor n\Big(1 - H\Big(\frac{d-1}{n}\Big)\Big) + 1\Big\rfloor,$$

což je podle vztahu $\lfloor x + 1 \rfloor > x$ větší než pravá strana dokazované nerovnosti. Důkaz je hotov. □

Pro libovolné dané d zvolme $n = 3d$. Podle Gilbert–Varshamovova odhadu existuje binární $[n, k, d]$-kód C_d dimenze $k > n(1 - H(1/3))$. Pro takový kód platí

$$\delta(C_d) \geq \frac{1}{3} \quad \text{a} \quad \alpha(C_d) \geq 1 - H(1/3) > 0.$$

Třída $\{C_d : d \in \mathbb{N}\}$ je tedy asymptoticky dobrá!

Na druhou stranu nám věta 12.2.1 nedává explicitní popis této třídy, důkaz je existenční. Konstrukce asymptoticky dobrých kódů byla po dlouhou dobu 'svatým grálem' teorie kódů. Historicky první nalezenou třídou s požadovanými vlastnostmi byla třída Justesenových kódů, se kterou se seznámíme v oddílu 12.5.

Cvičení

► **12.2.1.** Dokažte verzi Gilbert–Varshamovova odhadu pro q-ární kódy: je-li

$$V_q(n, d-1) < q^{n-k},$$

pak existuje $[n, k, d]_q$-kód.

► **12.2.2.** Dokažte *Gilbertův odhad*: platí-li

$$M \cdot V_q(n, d-1) < q^n,$$

potom existuje (ne nutně lineární) $(n, \log_q M, d)_q$-kód.

12.3 Asymptotické odhady

Asymptotické verze různých nerovností se dají stručně vyjádřit s použitím následující definice. Pro číslo $\delta \in [0, 1]$ položme

$$\alpha(\delta) = \limsup_{n\to\infty} \frac{A(n, \lceil \delta n \rceil)}{n}. \tag{12.4}$$

Dolní odhad pro funkci $\alpha(\delta)$ plyne z věty 12.2.2.

Věta 12.3.1 (Asymptotický Gilbert–Varshamovův odhad)**.** *Pro $\delta \leq 1/2$ platí*

$$\alpha(\delta) \geq 1 - H(\delta).$$

Důkaz. Nechť je dáno $\delta \leq 1/2$ a $n > 0$. Z věty 12.2.2 a z nerovnosti $\lceil x \rceil < x + 1$ plyne

$$\frac{A(n, \lceil \delta n \rceil)}{n} > 1 - H\Big(\frac{\lceil \delta n \rceil - 1}{n}\Big) > H(\delta).$$

□

Také Singletonův odhad má své asymptotické vyjádření.

Věta 12.3.2 (Asymptotický Singletonův odhad)**.** *Pro každé* $\delta \in [0,1]$ *platí*

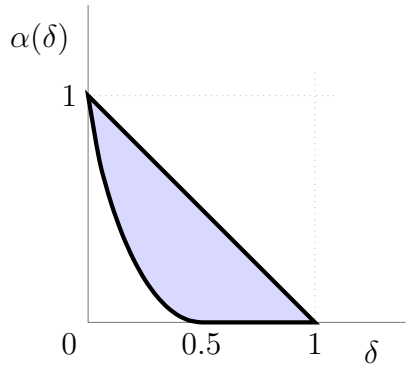
$$\alpha(\delta) \leq 1 - \delta.$$

Důkaz. Podle Singletonova odhadu (věta 1.7.2) platí $A(n,d) \leq n - d + 1$ a tedy

$$\frac{A(n, \lceil \delta n \rceil)}{n} \leq 1 - \frac{\lceil \delta n \rceil}{n} + \frac{1}{n} \leq 1 - \delta + \frac{1}{n}.$$

Pravá strana pro $n \to \infty$ konverguje k $1 - \delta$. □

Obrázek 12.1 znázorňuje oba odhady v grafu s osami δ a α.



Obrázek 12.1: Asymptotický Gilbert–Varshamovův a Singletonův odhad. Funkce $\alpha(\delta)$ leží ve vybarvené oblasti.

12.4 Asymptotický Hammingův odhad

Než dokážeme asymptotickou verzi Hammingova odhadu, potřebujeme zdola odhadnout číslo $V(n,k)$. Zatím jsme dokázali pouze horní odhad

$$V(n,k) < 2^{nH(k/n)},$$

a to ve větě 11.1.1.

Obvyklý důkaz dolního odhadu je založen na Stirlingově formuli, která udává asymptotické chování funkce $n!$. My jej odvodíme z jednodušššího vztahu, jehož důkaz ponecháváme jako cvičení.

Lemma 12.4.1. *Pro přirozené* $n \geq 50$ *platí*

$$\left(\frac{n}{\mathrm{e}}\right)^n < n! < \left(\frac{n}{\mathrm{e}}\right)^{n+1}.$$

Důkaz. Cvičení 12.4.1. □

Protože $V(n,k)$ je součtem kombinačních čísel od $\binom{n}{0}$ po $\binom{n}{k}$, plyne horní odhad čísla $V(n,k)$ z následujícího lemmatu.

Lemma 12.4.2. *Pro přirozená čísla $0 \leq k \leq n$, kde $n \geq 50$, platí*

$$\binom{n}{k} > \frac{\mathrm{e}^2}{k(n-k)} \cdot 2^{nH(k/n)}.$$

Důkaz. Podle lemmatu 12.4.1 máme

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\ &> \frac{(n/e)^n}{(k/e)^{k+1}((n-k)/e)^{n-k+1}} \\ &= \frac{\mathrm{e}^2}{k(n-k)} \cdot \frac{n^n}{k^k(n-k)^{n-k}} \\ &= \frac{\mathrm{e}^2}{k(n-k)} \cdot 2^{nH(k/n)}.\end{aligned}$$

□

Věta 12.4.3 (Asymptotický Hammingův odhad)**.** *Pro $\delta \in [0,1]$ platí*

$$\alpha(\delta) \leq 1 - H(\delta/2).$$

Důkaz. Z Hammingova odhadu (věta 4.1.1) plyne, že $A(n,d) \leq n - \log V(n, \lfloor (d-1)/2 \rfloor)$, tedy

$$\frac{A(n, \lceil \delta n \rceil)}{n} \leq 1 - \frac{\log V\Big(n, \Big\lfloor \frac{\delta n - 1}{2} \Big\rfloor\Big)}{n}.$$

Z lemmatu 12.4.2 je

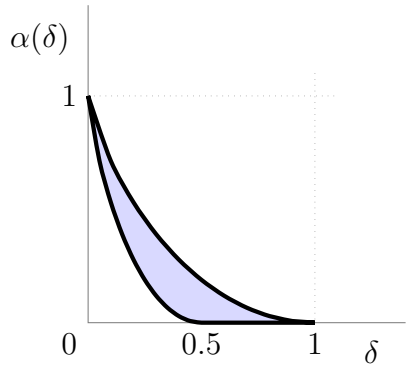
$$\frac{\log V(n,k)}{n} > \binom{n}{k} > H(k/n) + o(1),$$

kde $o(1)$ představuje člen jdoucí k 0 pro $n \to \infty$. Dosazením do první nerovnosti dostaneme

$$\begin{aligned}\frac{A(n, \lceil \delta n \rceil)}{n} &< 1 - H\Big(\Big\lfloor \frac{\delta n - 1}{2} \Big\rfloor / n\Big) - o(1) \\ &< 1 - H\Big(\frac{\delta n - 3}{2n}\Big) - o(1) \\ &= 1 - H\Big(\frac{\delta}{2} - \frac{3}{2n}\Big) - o(1),\end{aligned}$$

kde pravá strana poslední nerovnosti se pro $n \to \infty$ blíží $1 - H(\delta/2)$. □

Protože asymptotická forma Hammingova odhadu je ve všech bodech lepší než asymptotický Singletonův odhad, podařilo se nám zúžit oblast vyznačenou na obrázku 12.1. Obrázek 12.2 znázorňuje asymptotický Hammingův odhad.



Obrázek 12.2: Asymptotický Gilbert–Varshamovův a Hammingův odhad.

Cvičení

▶ **12.4.1.** Následující problémy jsou kroky k důkazu odhadu hodnot funkce $n!$.

(a) Pro $x \in \mathbf{R}$ dokažte, že platí

$$1 + x < \mathrm{e}^x < \frac{1}{1-x}.$$

(b) Odvoďte nerovnost

$$\left(1 + \frac{1}{n}\right)^n < \mathrm{e} < \left(1 + \frac{1}{n}\right)^{n+1},$$

kde $n \in \mathbb{N}$.

(c) Dokažte, že pro $n \geq 50$ platí

$$\left(\frac{n}{\mathrm{e}}\right)^n < n! < \left(\frac{n}{\mathrm{e}}\right)^{n+1}.$$

(Návod: ověřte nerovnost pro $n = 50$ a poté dokažte, že

$$a_{n+1}/a_n < b_{n+1}/b_n < c_{n+1}/c_n,$$

kde a_n, b_n a c_n je levá, prostřední, resp. pravá strana zkoumané nerovnice.)

12.5 Justesenovy kódy

Pro libovolné reálné číslo $\kappa \in (0, \frac{1}{2})$ zkonstruujeme nekonečnou třídu binárních kódů $J_{m,\kappa}$ (kde $m = 1, 2, \dots$) s hustotou alespoň κ, jejichž relativní vzdálenost je zdola omezena kladnou konstantou.

Pro dané přirozené číslo m nechť $q = 2^m$. Začneme s kódem $C = C_{m,\kappa}$, který je rozšířením Reed–Solomonova kódu $\mathrm{RS}_{q,q\kappa}$. Připomeňme, že tento RS kód je q-ární kód s parametry $[q-1, q\kappa, q(1-\kappa)]$, a C z něj vznikne přidáním paritního symbolu[1] jako v oddílu 6.2.

Těleso $\mathbb{F}_q$ je vektorovým prostorem dimenze m nad $\mathbb{F}_2$. Každému prvku $\beta \in \mathbb{F}_q$ tedy můžeme přiřadit vektor $\langle\beta\rangle$ délky m, jehož složky jsou souřadnice prvku β vzhledem k pevné bázi prostoru $\mathbb{F}_q$, dejme tomu k bázi $1, \alpha, \ldots, \alpha^{m-1}$, kde α je primitivní prvek tělesa $\mathbb{F}_q$. Vektor $\langle\beta\rangle$ je vlastně m-tice bitů.

Kód $J_{m,\kappa}$ dostaneme, pokud každý symbol c_i každého slova kódu $C_{m,\kappa}$ nahradíme 'zřetězením' vektorů $\langle c_i\rangle$ a $\langle\alpha^i c_i\rangle$:

$$J_{m,\kappa} = \{\langle c_0\rangle\langle c_0\rangle \ldots \langle c_i\rangle\langle\alpha^i c_i\rangle \ldots \langle c_{q-1}\rangle\langle\alpha^{q-1} c_{q-1}\rangle \,:\, c_0 \ldots c_{q-1} \in C_{m,\kappa}\}.$$

Kód $J_{m,\kappa}$ má parametry (n, k, d), kde:

- $n = 2m \cdot q = m \cdot 2^{m+1}$ (každý z q symbolů kódového slova jsme nahradili vektorem délky $2m$),
- $k = m \cdot q\kappa = \kappa m 2^m$ (dimenze nad $\mathbb{F}_q$ je $q\kappa$, přičemž $\mathbb{F}_q$ samo je vektorovým prostorem dimenze m nad $\mathbb{F}_2$).

Minimální vzdálenosti d teprve odhadneme. Klíčem k tomu bude následující úvaha. Libovolné slovo $c \in C_{m,\kappa}$ obsahuje $q(1-\kappa)$ nenulových symbolů. Při přechodu ke kódu $J_{m,\kappa}$ jsme každý takový symbol c_i nahradili $2m$-tic bitů $\langle c_i\rangle\langle\alpha^i c_i\rangle$. Podstatné je, že symbolům c_i a c_j, kde $i \neq j$, odpovídají *různé* $2m$-tice. Pokud každou $2m$-tici interpretujeme jako charakteristickou funkci podmnožiny $\{1, \ldots, 2m\}$, dostáváme $q(1-\kappa)$ různých podmnožin.

Lemma 12.5.1. *Nechť $\gamma \in (0,1)$ je pevné reálné číslo. Je-li $\mathcal{A}$ systém alespoň $\gamma \cdot 2^m$ různých podmnožin množiny $M = \{1, \ldots, 2m\}$, pak průměrná velikost množiny z $\mathcal{A}$ je alespoň*

$$2m \cdot H^{-1}\Big(\frac{1}{2}\Big) \cdot (1 - o(1)),$$

kde $o(1)$ označuje člen jdoucí k 0 pro $m \to \infty$ a funkce $H^{-1} : [0,1] \to [0, \frac{1}{2}]$ je inverzní k entropické funkci.

Důkaz. Nechť t je přirozené číslo. Počet podmnožin množiny M o méně než t prvcích je přesně $V(2m,t)$ (objem kombinatorické koule o poloměru t). Ostatní podmnožiny mají alespoň t prvků, takže průměrná velikost podmnožiny z $\mathcal{A}$ je

$$\begin{aligned} s &\geq \frac{t}{|\mathcal{A}|} \cdot \Big(|\mathcal{A}| - V(2m,t)\Big) = t\Big(1 - \frac{V(2m,t)}{|\mathcal{A}|}\Big) \\ &\geq t\Big(1 - \frac{2^{2mH(\frac{t}{2m})}}{\gamma \cdot 2^m}\Big) \end{aligned}$$

[1] Standardní konstrukce Justesenových kódů používá přímo kód $\mathrm{RS}_{q,q\kappa}$, ale s kódem C nám vyjdou trochu hezčí čísla.

z horního odhadu čísla $V(2m,t)$ a z faktu, že $|\mathcal{A}| \geq \gamma \cdot 2^m$. Zvolíme-li nyní

$$t = 2m \cdot H^{-1}\Big(\frac{1-\varepsilon}{2}\Big),$$

kde $\varepsilon = \varepsilon(m)$ je 'malé' číslo (jehož závislost na m určíme níže), odhad se zjednoduší a dostaneme

$$\begin{aligned} s &\geq t\Big(1 - \frac{2^{m(1-\varepsilon)}}{\gamma \cdot 2^m}\Big) = t\Big(1 - \frac{1}{\gamma \cdot 2^{\varepsilon m}}\Big) \\ &= 2m \cdot H^{-1}\Big(\frac{1-\varepsilon}{2}\Big)\Big(1 - \frac{1}{\gamma \cdot 2^{\varepsilon m}}\Big). \end{aligned}$$

Pokud se nám podaří zvolit $\varepsilon(m)$ tak, aby pro $m \to \infty$ bylo $\varepsilon \to 0$, ale $\varepsilon m \to \infty$, pak výraz v poslední závorce bude $1 - o(1)$ (ve smyslu znění lemmatu), zatímco výraz $H^{-1}((1-\varepsilon)/2)$ se pro velké m blíží $1/2$, a je tedy rovněž typu $H^{-1}(1/2)(1-o(1))$. Celkem vzato, daná volba parametru t ukazuje, že

$$s \geq 2m \cdot H^{-1}\Big(\frac{1}{2}\Big) \cdot (1 - o(1)),$$

což jsme chtěli dokázat. □

Vraťme se k minimální vzdálenosti kódu $J_{m,\kappa}$. Protože počet různých $2m$-tic bitů v každém jeho slově je alespoň $q(1-\kappa) = 2^m(1-\kappa)$, lze použít lemma 12.5.1 a odvodit dolní odhad na průměrnou váhu těchto $2m$-tic. Z něj plyne, že jejich celková váha (a tedy minimální váha kódu $J_{m,\kappa}$) je alespoň

$$2^m \cdot (1-\kappa) \cdot 2m \cdot H^{-1}\Big(\frac{1}{2}\Big) \cdot (1 - o(1))$$

a relativní vzdálenost se tak pro velké m blíží konstantě

$$H^{-1}\Big(\frac{1}{2}\Big) \cdot (1-\kappa).$$

Vzhledem k tomu, že i hustota je zdola omezena konstantou $\kappa/2$, našli jsme asymptoticky dobrou třídu kódů.

Kapitola 13

Konvoluční kódy

Kapitola 14

Kombinace kódů

14.1 Produktové kódy

14.2 Zřetězené kódy

14.3 Dekódování

Kapitola 15

Co se nevešlo

15.1 Váhové polynomy a věta MacWilliamsové

Váhový polynom $P_C(x)$ libovolného kódu C určuje pro každé $i = 0, \ldots, n$, kolik kódových slov má váhu i. Je definován jako

$$P_C(x) = \sum_{c \in C} x^{|c|},$$

kde $|c|$ je váha kódového slova c, takže počet slov váhy i zjistíme jako koeficient u členu x^i. V početní kombinatorice se podobné polynomy obvykle označují jako *vytvořující funkce*.

Pro lineární kód C platí překvapivý vztah mezi polynomem P_C a váhovým polynomem duálního kódu $P_{C^\perp}$: tzv. věta MacWilliamsové. Větu uvedeme pro binární kódy, obecný případ ponecháváme jako cvičení 15.1.1.

Věta 15.1.1 (MacWilliamsová)**.** *Pro binární kód C délky n platí*

$$P_{C^\perp}(x) = \frac{1}{|C|} \cdot (1+x)^n \cdot P_C\left(\frac{1-x}{1+x}\right).$$

Důkaz. Pro $a \in C$ položme

$$g(a) = \sum_{b \in F_2^n} (-1)^{a \cdot b} x^{|b|},$$

kde $a \cdot b$ je skalární součin. Na každý sčítanec se zde můžeme dívat jako na součin

n čísel ve tvaru $(-1)^{a_i b_i} x^{b_i}$:

$$\begin{aligned} g(a) &= \sum_{b\in F_2^n} \Big((-1)^{a_1 b_1} x^{b_1}\Big) \cdot \cdots \cdot \Big((-1)^{a_n b_n} x^{b_n}\Big) \\ &= \sum_{b\in F_2^n} \Big((-1)^{a_1} x\Big)^{b_1} \cdot \cdots \cdot \Big((-1)^{a_n} x\Big)^{b_n} \\ &= \Big(1+(-1)^{a_1} x\Big) \cdot \cdots \cdot \Big(1+(-1)^{a_n} x\Big) \\ &= (1-x)^{|a|} \cdot (1+x)^{n-|a|} = (1+x)^n \cdot \left(\frac{1-x}{1+x}\right)^{|a|}, \end{aligned}$$

takže sečtením polynomů $g(a)$ přes všechna $a \in C$ dostaneme téměř pravou stranu dokazované rovnice:

$$\sum_{a\in C} g(a) = (1+x)^n \cdot P_C\left(\frac{1-x}{1+x}\right).$$

Souvislost s kódem $C^\perp$ je dána faktem, že slovo $b \in F_2^n$ je buď ortogonální na všechna $a \in C$ (a pak patří do $C^\perp$), nebo je ortogonální přesně na polovinu slov $a \in C$. (Je-li totiž $ab = 1$, kde $a \in C$, pak pro každé $a' \in C$ platí $a'b = 0$ právě když $(a'+a)b = 1$.) Jinými slovy: v součtu $\sum_{a\in C} g(a)$ má polovina z $|C|$ členů pro libovolné slovo $b \notin C^\perp$ znaménko + a polovina znaménko −. Tyto členy tedy můžeme zanedbat. Dostáváme

$$\sum_{a\in C} g(a) = \sum_{a\in C} \sum_{b\in C^\perp} (+1) \cdot x^{|b|} = |C| \cdot P_{C^\perp}(x).$$

Odtud plyne tvrzení věty. □

Cvičení

► **15.1.1.** Dokažte větu MacWilliamsové pro kódy nad tělesem F_q, kde q je prvočíslo:

$$P_{C^\perp}(x) = \frac{1}{|C|} \cdot \Big(1+(q-1)x\Big) \cdot P_C\left(\frac{1-x}{1+(q-1)x}\right).$$

Návod: Definujte $g(a)$ jako komplexní polynom

$$g(a) = \sum_{b\in F_q^n} \omega^{a\cdot b} x^{|b|},$$

kde $\omega = \mathrm{e}^{2\pi i/q}$ je komplexní q-tá odmocnina z jedné, a použijte vztah $\sum_{j=0}^{q-1} \omega^j = 0$.

15.2 Jednoznačnost kódu $\mathcal{G}_{24}$

V tomto oddílu zahájíme důkaz, že existuje (až na isomorfismus) jen jediný binární $(24, 12, 8)$-kód obsahující nulové slovo, totiž kód $\mathcal{G}_{24}$. (Důkaz dokončíme v oddílu 15.4.) Nechť tedy C je kód s těmito vlastnostmi.

Zvolme i od 1 do 24 a připomeňme, že *propíchnutí* kódu C na pozici i znamená 'odstranění' i-té souřadnice ze všech kódových slov. V našem případě tím vznikne $(23, 12, 7)$-kód C' obsahující nulové slovo. Podle věty 4.3.2 je jeho váhový polynom jednoznačně určen a nezávisí na pozici i. Prozkoumáním tohoto polynomu zjistíme, že C' obsahuje jen slova, jejichž váha je tvaru $4t$ nebo $4t - 1$ (t celé). Z toho ale plyne, že váha každého slova kódu C je dělitelná 4, jinak bychom propíchnutím na vhodné pozici dostali slovo váhy 2 nebo 3 (mod 4).

Váhový polynom našeho kódu C tedy podle věty 4.3.2 musí být

$$P_C(x) = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}. \tag{15.1}$$

Uvažujme kód C jako podmnožinu vektorového prostoru $\mathbb{F}_2^{24}$. Je-li $u \in C$, pak kód $u + C = \{u + c : c \in C\}$ je rovněž $(24, 12, 8)$-kód (protože přičtení vektoru u nemění vzdálenosti) a obsahuje nulové slovo. Podle výše uvedené úvahy je $P_{u+C}(x) = P_C(x)$. Z toho plyne, že pro $u, v \in C$ je váha $|u + v|$ (tedy vzdálenost slov u, v) násobkem 4. Přitom podle (4.4) platí

$$2\langle u, v\rangle \equiv |u + v| - |u| - |v| \pmod 4$$

a tedy $\langle u, v\rangle = 0$ pro každé $u, v \in C$. Lineární kód $\tilde{C} \subset \mathbb{F}_2^{24}$, generovaný prvky kódu C, má bázi $B \subset C$, ve které pro každé $b, b' \in B$ platí $\langle b, b'\rangle = 0$. Podle lemmatu 4.2.2 je kód $\tilde{C}$ podmnožinou svého duálního kódu $\tilde{C}^\perp$. Protože je ale

$$12 = \dim C \le \dim \tilde{C} \le \dim \tilde{C}^\perp \quad \text{a} \quad \dim \tilde{C} + \dim \tilde{C}^\perp = 24,$$

musí být $C = \tilde{C}$. Kód C je tedy lineární a navíc samoduální!

Ukážeme nyní, že C (přesněji nějaký ekvivalentní kód) má generující matici ve speciálním tvaru

$$\left(\begin{array}{c|ccc} & 0 & 1 \ \dots & 1 \\ & 1 & & \\ I_{12} & \vdots & D & \\ & \vdots & & \\ & 1 & & \end{array}\right) \tag{15.2}$$

Víme, že C obsahuje slovo c váhy 12; po vhodné permutaci pozic můžeme předpokládat, že $c = (1 \dots 10 \dots 0)$. Kód dále obsahuje vektor $\mathbf{1}$ ze samých jedniček. Nechť G je generující matice s prvním řádkem c. Označme

$$G = \left(\begin{array}{ccc|ccc} 1 & \dots & 1 & 0 & \dots & 0 \\ & R & & & S & \end{array}\right).$$

Tvrdíme, že matice S musí mít plnou hodnost (tedy 11). Předpokládejme totiž, že nějaká množina $\{s_i : i \in I\}$ řádků matice S má nulový součet, a položme $g = \sum_{i\in I}(r_i \mid s_i)$, kde r_i je i-tý řádek matice R. Váhy kódových slov g a $g + c$ dávají v součtu 12, takže nemohou být obě alespoň 8. To je spor.

Matice S tedy generuje kód délky 12 a dimenze 11. Každé jeho slovo má nulový součet, protože každý řádek matice G je ortogonální na na vektor $c + \mathbf{1}$. To znamená, že matice S musí generovat paritní $[12, 11, 2]$-kód. Lze tedy bez újmy na obecnosti předpokládat, že je ve tvaru

$$S = \begin{pmatrix} & 1 \\ I_{11} & \vdots \\ & 1 \end{pmatrix}$$

Nyní již ve sloupcích 12 až 23 matice G snadno dostaneme podmatici I_{12} a po přerovnání sloupců získáváme hledaný tvar (15.2). O matici D se dá leccos říci.

Tvrzení 15.2.1. *Každý řádek matice D v (15.2) má váhu* 6. *Každé dva řádky mají právě* 3 *jedničky ve stejných sloupcích.*

Důkaz. Důvodem je, že kód $\mathcal{G}_{24}$ má minimální váhu 8 a všechny váhy dělitelné 4. □

K vlastnostem matice D se vrátíme v oddílu 15.4, kde uvidíme, že jí odpovídá kombinatorická struktura, tzv. design, která je pro dané parametry určena jednoznačně (až na isomorfismus). Z toho vyplyne jednoznačnost kódu $\mathcal{G}_{24}$ (věta 15.4.3).

15.3 Designy

Designy jsou množinové systémy vykazující velkou míru pravidelnosti. Nechť X je konečná množina (její prvky budeme označovat jako *body*) a nechť $\mathcal{D}$ je systém podmnožin množiny V (tzv. *bloků*). Řekneme, že $(X, \mathcal{D})$ je *design* s parametry t-(v, k, λ), kde všechna písmena označují přirozená čísla, pokud

(i) $|X| = v$,

(ii) velikost každého bloku je k,

(iii) každá t-tice prvků z X leží právě v λ blocích.

Příkladem designu je Fanova rovina na obr. 1.1, jejíž parametry jsou 2-$(7, 3, 1)$.

Z parametrů t, v, k, λ lze určit i některé další. Především je to počet bloků b, který získáme, spočítáme-li dvěma způsoby dvojice (A, B), kde $A \subset B \in \mathcal{D}$, $|A| = t$. Je totiž

$$\binom{v}{t} \cdot \lambda = b \cdot \binom{k}{t},$$

takže

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}. \tag{15.3}$$

Dále lze určit *stupeň* libovolného vrcholu $x \in X$, tj. počet bloků, ve kterých je obsažen. Vrchol x lze totiž $\binom{v-1}{t-1}$ způsoby doplnit na t-prvkovou množinu, a taková množina je obsažena v λ blocích. Každý tento blok jsme ovšem započítali $\binom{k-1}{t-1}$-krát, proto stupeň vrcholu x je

$$d = \lambda \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}. \tag{15.4}$$

Konečně spočítejme ještě jeden parametr: průměrnou velikost průniku dvou bloků designu $\mathcal{D}$. Zvolme pevně blok $B \in \mathcal{D}$ a spočítejme dvojice (b, C), kde $b \in B \cap C$ a $B \neq C \in \mathcal{D}$. Každý z k vrcholů bloku B je obsažen v $d = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$ blocích, mezi nimiž je ale i blok B. Bloků $C \neq B$ je $b - 1$. Průměrná velikost průniku $B \cap C$ je tak

$$\frac{k(d-1)}{b-1}.$$

Vzhledem k tomu, že toto číslo nezáleží na volbě bloku B, jedná se skutečně o průměrnou velikost průniku přes všechny dvojice bloků designu $\mathcal{D}$.

Incidenční matice množinového systému $(X, \mathcal{D})$ je matice, jejíž řádky odpovídají blokům z $\mathcal{D}$, sloupce prvkům množiny X, a jejíž položky jsou rovny 0 nebo 1 podle toho, zda příslušný prvek náleží danému bloku. Řečeno přesněji, položme $\mathcal{D} = \{B_1, \ldots, B_b\}$, $X = \{x_1, \ldots, x_v\}$, a definujme matici $M(X, \mathcal{D}) = (m_{ij})$ o rozměrech $b \times v$ předpisem

$$m_{ij} = \begin{cases} 1 & \text{pokud } x_j \in B_i, \\ 0 & \text{jinak.} \end{cases}$$

Matice $M(X, \mathcal{D})$ je *incidenční matice* systému $(X, \mathcal{D})$ (pro zvolené očíslování bloků a vrcholů).

V následujícím oddílu budeme potřebovat větu o speciálním typu designů. Design s parametry 2-(v, k, λ) je *čtvercový*, má-li stejný počet bloků a bodů, tj. $b = v$.

Věta 15.3.1. *Ve čtvercovém* 2-(v, k, λ) *designu mají každé dva bloky průnik o velikosti právě* λ.

Důkaz. Nechť $\mathcal{D}$ je čtvercový design s incidenční maticí M. Protože $b = v$ a $t = 2$, z rovnosti (15.3) plyne $k(k-1) = \lambda(v-1)$. Dosazením do (15.4) dostáváme, že stupeň d je roven k.

Každá dvojice bodů leží v λ blocích, každý bod v $d = k$ blocích. Odtud

$$M^T M = \lambda I + (k - \lambda)J, \tag{15.5}$$

kde I je identická matice a J je matice ze samých jedniček. K důkazu tvrzení stačí ukázat, že $MM^T = M^TM$.

Protože každý blok obsahuje k bodů a každý bod je v k blocích, platí

$$MJ = JM = kJ.$$

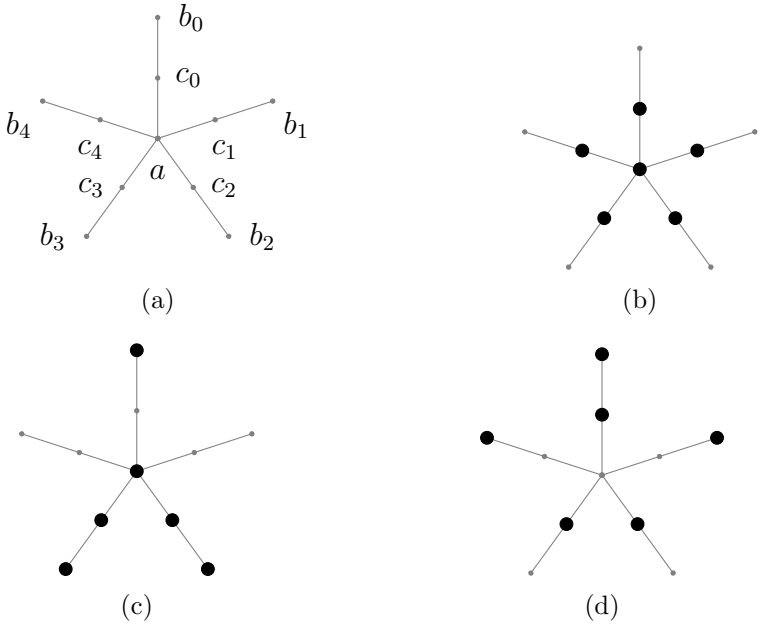
Matice M tedy komutuje s J a tedy s každou maticí tvaru $xI + yJ$, kde $x, y \in \mathbf{R}$. Díky (15.5) komutuje s M^TM, takže

$$MM^T = M\Big(M^T(MM^{-1})\Big) = \Big(M(M^TM)\Big)M^{-1} = \Big((M^TM)M\Big)M^{-1} = M^TM,$$

což jsme chtěli dokázat. □

15.4 Design s parametry 2-$(11, 6, 3)$

Nechť $\mathcal{D}_{11}$ je množinový systém na 11 bodech, jehož 11 bloků je znázorněno na obrázku 15.1. Rozborem případů se snadno ukáže, že jde o 2-$(11, 6, 3)$ design.



Obrázek 15.1: (a) Označení prvků množiny X. (b)–(d) Bloky designu $\mathcal{D}_{11}$ na X jsou všechny možné rotace vyznačených množin kolem středu.

Isomorfismus množinových systémů $(X, \mathcal{D})$ a $(X', \mathcal{D}')$ je taková bijekce $f : X \to X'$, že pro každou podmnožinu $B \subset X$ platí

$$B \in \mathcal{D} \quad \text{právě když} \quad f(B) \in \mathcal{D}'.$$

Věta 15.4.1. *Design* $\mathcal{D}_{11}$ *je jediný* 2-$(11, 6, 3)$ *design až na isomorfismus.*

Důkaz. Nechť $\mathcal{D}$ je design s těmito parametry. Budeme se snažit označit jeho body symboly a, b_i, c_i tak, aby vyšly přesně tytéž bloky jako na obrázku 15.1. To je samozřejmě jen způsob, jak specifikovat isomorfismus mezi oběma designy. V důkazu se nám bude hodit věta 15.3.1, z níž plyne, že každé dva bloky designu $\mathcal{D}$ mají tříprvkový průnik. Všimněme si, že průnik 3 bloků pak musí mít nejvýše 2 prvky.

Vezměme libovolný blok A designu $\mathcal{D}$ a označme jeden prvek bloku A jako a. Definujme na 5-prvkové množině $A - \{a\}$ graf H, ve kterém jsou hranou spojeny body b a b', pokud existuje blok B s vlastností, že $A \cap B = \{a, b, b'\}$ (je-li takových bloků víc, hrana bude vícenásobná). Pro libovolné $b \in A - \{a\}$ je dvojice a, b obsažena kromě A právě ve dvou dalších blocích, z nichž každý obsahuje ještě třetí prvek z A. Stupeň každého vrcholu grafu H je tedy přesně 2. Graf navíc neobsahuje násobné hrany, neboť dvojitá hrana mezi vrcholy b, b' by znamenala, že trojice a, b, b' je ve třech blocích, což je nemožné. Pak ovšem H musí být kružnice $b_0b_1b_2b_3b_4$ na 5 vrcholech.

Označme blok obsahující trojici a, b_i, b_{i+1} (různý od A) symbolem B_i. (Veškeré indexy nadále interpretujeme modulo 5.) Průnik $B_{i-1} \cap B_i$ obsahuje kromě bodů a, b_i ještě třetí bod, a ten nemůže ležet v A. Označme jej tedy c_i. Tvrdíme, že body c_i jsou navzájem různé. Kdyby ne, musel by nějaký bod c_i ležet ve třech 'po sobě jdoucích' blocích B_{j-1}, B_j, B_{j+1}. Průnik těchto bloků je pak $\{a, c_i\}$. Je snadné nahlédnout, že 3 bloky s dvouprvkovým průnikem musí pokrývat všech 11 bodů. Přitom však bod b_{j+3} neleží v žádném z nich, což je spor.

Každý blok B_i obsahuje body a, b_i, b_{i+1}, c_i a c_{i+1}. Šestý bod nemůže ležet v A (tam už 3 body jsou), takže zbývají možnosti c_{i-1}, c_{i+2} a c_{i+3}. Kdyby ale B_i obsahoval bod c_{i-1} resp. c_{i+2}, měl by alespoň 4 body společné s blokem B_{i-1} resp. B_{i+1}. Proto $c_{i+3} \in B_i$, takže blok B_i má tvar jako na obrázku 15.1(c). (Ten znázorňuje konkrétně blok B_2.) Dále blok A je shodný s obrázkem 15.1(b).

Zbývá nahlédnout, že ostatních 5 bloků je typu (d). Dvojice b_i, c_i jsou kromě bloků B_{i-1} a B_i v jednom dalším bloku, který označíme C_i. Ten jistě neobsahuje bod a (jinak by a, b_i, c_i byly ve 3 blocích). Tvrdíme, že C_i obsahuje body b_{i+2} a b_{i-2}. Dejme tomu, že ne. Protože $|C_i \cap A| = 3$, můžeme ze symetrie předpokládat, že $b_{i+1} \in C_i$. Pak ale prvek c_{i+1} ani prvek c_{i-2} nejsou v C_i, protože jinak by bloky B_i a C_i měly 4-prvkový průnik. Blok C_i tedy neobsahuje prvky a, c_{i+1}, c_{i-2} z bloku B_{i-2}, a musí tedy obsahovat všechny 3 ostatní prvky. Mezi nimi jsou b_{i-2} a b_{i-1}, takže spolu s prvky b_i a b_{i+1} již C_i obsahuje 4 prvky z bloku A. To je spor.

Jakmile víme, že b_{i+2} a b_{i-2} jsou v C_i, je snadné nahlédnout, že zbývající prvky tohoto bloku (kromě b_i a c_i) musí být c_{i+1} a c_{i-1}. Blok C_i je tedy skutečně jako na obrázku 15.1(d). Tím je isomorfismus nalezen. □

Větu 15.4.1 lze aplikovat na kód $\mathcal{G}_{24}$. Interpretujme matici D z tvrzení 15.2.1 jako incidenční matici množinového systému $\mathcal{G}$ na množině $V = \{1, \ldots, 11\}$.

Tvrzení 15.2.1 říká, že každý blok má velikost 6 a každé dva bloky mají průnik o velikosti 3. Je $(V, \mathcal{G})$ design?

Tvrzení 15.4.2. *Systém $(V, \mathcal{G})$ je design s parametry* 2-$(11, 6, 3)$.

Důkaz. Stačí ukázat, že každé dva prvky množiny V leží ve 3 blocích. Jaký je průměrný počet bloků obsahujících danou dvojici prvků? Každý z 11 bloků obsahuje $\binom{6}{2}$ z $\binom{11}{2}$ dvojic, takže počet bloků, v nichž je dvojice obsažena, je průměrně

$$\frac{11 \cdot \binom{6}{2}}{\binom{11}{2}} = 3$$

blocích. Není-li každá dvojice obsažena ve 3 blocích, pak existuje dvojice, která je obsažena ve 4 blocích $B_1, \ldots, B_4$. Nechť $|B_1 \cap \cdots \cap B_4| = m$, kde zjevně $2 \leq m \leq 3$.

Podle principu inkluze a exkluze platí pro velikost sjednocení

$$\begin{aligned} |\bigcup_i B_i| &= \sum_i |B_i| - \sum_{i<j} |B_i \cap B_j| + \sum_{i<j<k} |B_i \cap B_j \cap B_k| - |B_1 \cap B_2 \cap B_3 \cap B_4| \\ &\geq \binom{4}{1} \cdot 6 - \binom{4}{2} \cdot 3 + \binom{4}{3} \cdot m - m \\ &= 6 + 3m > 11, \end{aligned}$$

což je spor. Každá dvojice je tedy právě ve 3 blocích. □

Protože 2-$(11, 6, 3)$ design je jediný až na isomorfismus, je také incidenční matice takového designu jednoznačně určena až na pořadí řádků a sloupců. Z toho snadno plyne, že generující matice 15.2 kódu C (který má parametry Golayova kódu $\mathcal{G}_{24}$) je rovněž jednoznačně určena až na permutaci řádků a sloupců. Dokázali jsme následující větu.

Věta 15.4.3. *Každý binární* $(24, 12, 8)$*-kód obsahující nulové slovo je ekvivalentní Golayovu kódu* $\mathcal{G}_{24}$. □

Podobně platí, že každý binární $(23, 12, 7)$-kód obsahující nulové slovo je ekvivalentní perfektnímu kódu $\mathcal{G}_{23}$, vzniklému odstraněním propíchnutím kódu $\mathcal{G}_{24}$ v libovolné souřadnici.

Literatura

[1] J. Adámek, Kódování. SNTL, Praha, 1989.

[2] P. J. Cameron and J. H. van Lint, Designs, Graphs, Codes and their Links. Cambridge University Press, Cambridge, 1996.

[3] M. Golay, Notes on digital coding, Proc. IRE 37 (1949), p. 657.

[4] R. W. Hamming, Error detecting and error correcting codes. The Bell System Technical Journal 26,2 (1950), 147-160.

[5] J. H. van Lint, *Introduction to Coding Theory*, 3rd edition, Springer, 1999.

[6] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-correcting Codes. Elsevier, Amsterdam, 1988.

[7] S. Roman, Coding and Information Theory. Springer, 1992.

[8] C. E. Shannon, A mathematical theory of communication. The Bell System Technical Journal 27 (1948), pp. 379-423 and 623-656.

[9] M. Sudan, Algorithmic Introduction to Coding Theory. MIT, texty k přednášce na adrese `http://theory.lcs.mit.edu/~madhu/FT01/course.html`.