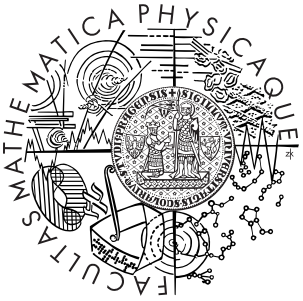
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Michal Szabados

Lineární rekurentní posloupnosti nad konečnými tělesy

Katedra algebry

Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
Studijní program: Matematika, obecná matematika

2010

Ďakujem Liborovi Bartovi za vedenie mojej bakalárskej práce.

Prehlasujem, že som svoju bakalársku prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a jej zverejňovaním.

V Prahe dňa Michal Szabados

Obsah

Názov práce: Lineárne rekurentné postupnosti nad konečnými telesami
Autor: Michal Szabados
Katedra (ústav): Katedra algebry
Vedúci bakalárskej práce: Mgr. Libor Barto, Ph.D.
e-mail vedúceho: libor.barto@gmail.com

Abstrakt: V tejto práci sa zaoberáme lineárnymi rekurentnými postupnosťami nad konečnými telesami. Obsahovo je práca rozdelená na tri časti. V prvej časti pripomíname základné tvrdenia o konečných telesách, v druhej časti analyzujeme lineárne rekurentné postupnosti pomocou charakteristického polynómu a sprievodnej matice. V tretej časti práce predstavujeme tzv. maximálne postupnosti, ktoré nám poslúžia na konštrukciu pseudonáhodného generátora čísel. Skúmame ich štatistické vlastnosti a prezentujeme súvisiace riešené cvičenia z knihy *Introduction to finite fields and their applications* od Lidla a Niederreitera [1]. Na záver práce uvádzame C++ program na generovanie pseudonáhodných čísel.

Kľúčové slová: lineárne rekurentné postupnosti, konečné telesá, pseudonáhodný generátor čísel

Title: Linear recurring sequences over finite fields
Author: Michal Szabados
Department: Department of Algebra
Supervisor: Mgr. Libor Barto, Ph.D.
Supervisor's e-mail address: libor.barto@gmail.com

Abstract: In this work we study linear recurring sequences over finite fields. The work is divided into three parts. In the first part we recall basic theorems concerning finite fields, in the second part we analyze linear recurring sequences using characteristic polynomial and companion matrix. In the third part we introduce maximal period sequences which are suitable for a construction of a pseudorandom number generator. We examine their statistical properties and present solutions of related exercises in the book *Introduction to finite fields and their applications* from Lidl and Niederreiter [1]. The work is concluded with a C++ program implementing algorithm for pseudorandom number generation.

Keywords: linear recurring sequences, finite fields, pseudorandom number generator

Kapitola 1

Úvod

Lineárne rekurentné postupnosti sú postupnosti zaujímavé hneď z dvoch dôvodov. Po prvé, z matematickej stránky vieme ich štruktúru dobre popísať a platia pre ne zaujímavé tvrdenia. Po druhé, rekurentné postupnosti majú praktické aplikácie. V tejto práci bude naše úsilie smerovať k jednej z nich – ku generovaniu pseudonáhodných čísel. Zavŕšením práce bude program, ktorý bude tieto čísla generovať.

Práca je rozdelená do troch častí. V prvej z nich zavedieme potrebné značenie a uvedieme tvrdenia z oblasti konečných telies, o ktorých predpokladáme, že sa s nimi čitateľ už niekedy stretol. Kapitola je skôr informatívna a znalý čitateľ ju môže bez problémov preskočiť.

V druhej časti leží jadro práce. Systematicky a detailne vybudujeme teóriu lineárnych rekurentných postupností nad konečnými telesami a zoznámime čitateľa so základnými nástrojmi na ich analýzu. Hlavnými vetami tejto časti bude explicitný vzorec na n-tý prvok postupnosti a tvrdenia zaoberajúce sa jej periódou.

Napokon v tretej časti, používajúc teoretický základ z druhej, predstavíme špeciálnu triedu tzv. maximálnych postupností. Tie, ako uvidíme, budú vhodné na generovanie pseudonáhodných čísel. Tiež uvádzame riešené cvičenia k tejto téme z knihy [1].

Na tomto mieste je vhodné uviesť, nakoľko je moja práca pôvodná. Pre Kapitolu 2 to nemá zmysel hovoriť, pretože sú v nej len základné tvrdenia o konečných telesách.

Vo zvyšku práce som čerpal z výbornej knihy Lidla a Niederreitera [1], avšak moja práca v žiadnom prípade nie je jej kópiou. Celá teória v Kapitole 3 je vybudovaná mojím vlastným spôsobom, z [1] som čerpal iba znenia niektorých

tvrdení. Všetky dôkazy, s výnimkou kanonicky známych a dôkazu Vety 3.25, som vymyslel sám.

V Kapitole 4, podobne ako v Kapitole 3, som z knihy čerpal hlavne znenia tvrdení, avšak miestami som sa nechal inšpirovať aj dôkazmi. Samozrejme to neplatí pre riešené cvičenia.

Napokon, program v C++ na generovanie pseudonáhodných čísel v Prílohe A som navrhol sám.

V tento moment už váženému čitateľovi nič nebráni v tom, aby sme sa spolu mohli pustiť do skúmania lineárnych rekurentných postupností nad konečnými telesami.

Michal Szabados

Kapitola 2

Značenie a základné tvrdenia z teórie konečných telies

2.1 Značenie

Zápis $v_{min} + \cdots + v_{max}$ respektíve $v_{min} \cdots v_{max}$ budeme chápať ako

$$\sum_{i=min}^{max} v_i \qquad \text{resp.} \qquad \prod_{i=min}^{max} v_i.$$

Špeciálne pre $max = min - 1$ bude výraz prázdna suma s hodnotou 0, respektíve prázdny súčin s hodnotou 1.

Ďalej budeme používať značenie:

$\mathbb{Z}, \mathbb{Z}_p$	celé čísla, celé čísla modulo p
$\mathbb{N}, \mathbb{N}_0$	kladné celé (prirodzené) čísla, nezáporné celé čísla
$\mathbb{F}_q$	q-prvkové konečné teleso
T^∞	množina všetkých postupností nad T s prvkami indexovanými $\mathbb{N}_0$
$M_n(T)$	priestor matíc $n \times n$ nad telesom T
$x^{\underline{n}}$	n-tá klesajúca mocnina: $x^{\underline{n}} = x(x-1)\cdots(x-n+1)$

2.2 Konečné telesá

V tejto časti kapitoly informatívne uvedieme základné tvrdenia z teórie konečných telies potrebné pre zvyšok práce. Znalý čitateľ môže kapitolu bez problémov

preskočiť, všetky tvrdenia a pojmy patria do základného kurzu konečných telies na Karlovej univerzite (skriptá Barta a Tůmy [2]). V prípade, keď je neskôr potrebné niektoré z tvrdení, je v dôkaze uvedená spätná referencia.

Definícia 2.1. *(Nekomutatívne) teleso* T je množina T s abelovskou grupou $(T, 0, +, -)$ a grupou $(T \setminus \{0\}, 1, \cdot, ^{-1})$ spĺňajúca tzv. distributívny zákon:

$$(a+b)c = ac + bc, \qquad c(a+b) = ca + cb, \qquad \forall a, b, c \in T.$$

Komutatívne teleso je teleso s komutatívnou operáciou „$\cdot$“. *Konečné teleso* je teleso s konečným počtom prvkov.

Značenie. Grupu s operáciou „$+$“ resp. „$\cdot$“ nazývame aditívna resp. multiplikatívna grupa.

Veta 2.2. *Pre p prvočíslo a $k \in \mathbb{N}$ existuje až na izomorfizmus práve jedno konečné teleso s p^k prvkami. Žiadne iné konečné telesá neexistujú.*

Značenie. Pre $q = p^k$ zo znenia vety značíme q-prvkové teleso ako $\mathbb{F}_q$. Pre $k = 1$ je $\mathbb{F}_p$ izomorfné $\mathbb{Z}_p$.

Tvrdenie 2.3. *Každý prvok konečného telesa $\mathbb{F}_q$ je jednoduchý koreň polynómu $x^q - x$.*

Tvrdenie 2.4. *Nech p je prvočíslo a $k \in \mathbb{N}$. Zobrazenie $\sigma : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ definované $x \mapsto x^p$ je automorfizmus a nazýva sa Frobeniov. Tento automorfizmus pomocou skladania generuje všetky automorfizmy $\mathbb{F}_{p^k}$.*

Tvrdenie 2.5. *Multiplikatívna grupa konečného telesa je cyklická.*

Veta 2.6. (Weddeburn) *Každé konečné teleso je komutatívne.*

2.3 Ireducibilné a primitívne polynómy

V tejto podkapitole budeme používať značenie q pre mocninu prvočísla, p pre prvočíslo a $k \in \mathbb{N}$.

Definícia 2.7. Polynóm f stupňa aspoň 1 je *ireducibilný*, ak v ľubovoľnom jeho rozklade na súčin polynómov $f = gh$ je g alebo h konštantný.

Tvrdenie 2.8. *Nech f je ireducibilný polynóm stupňa k nad $\mathbb{Z}_p$. Potom teleso $\mathbb{F}_{p^k}$ je izomorfné telesu polynómov $\mathbb{Z}_p[\alpha]/f(\alpha)$ a f má v tomto rozšírení koreň α.*

Veta 2.9. (O rozkladovom nadtelese) *Nech $f \in \mathbb{F}_q[x]$. Potom existuje k také, že f sa v $\mathbb{F}_{q^k}$ rozkladá na súčin lineárnych polynómov. Navyše všetky takéto minimálne rozšírenia sú si izomorfné.*

Tvrdenie 2.10. *Nech f je ireducibilný polynóm stupňa k nad $\mathbb{F}_q$ a α jeden jeho koreň v $\mathbb{F}_{q^k}$. Potom všetky jeho korene sú jednoduché a sú to čísla $\alpha, \alpha^q, \ldots, \alpha^{q^{k-1}}$. Tieto čísla nazývame ako* asociované *nad $\mathbb{F}_q$.*

Dôsledok 2.11. *Všetky korene ireducibilného polynómu f stupňa k nad $\mathbb{F}_q$ majú rovnaký rád v rozšírení $\mathbb{F}_{q^k}$.*

Tvrdenie 2.12. *Pre každé $k \in \mathbb{N}$ existuje ireducibilný polynóm stupňa k nad $\mathbb{F}_q$.*

Definícia 2.13. Generátor multiplikatívnej grupy $\mathbb{F}_q$ nazývame *primitívny prvok*. Ireducibilný polynóm stupňa k nad $\mathbb{F}_q$, ktorý má ako koreň primitívny prvok $\mathbb{F}_{q^k}$, nazývame *primitívnym polynómom*.

Tvrdenie 2.14. *Pre každé $k \in \mathbb{N}$ existuje primitívny polynóm stupňa k nad $\mathbb{F}_q$.*

Kapitola 3

Lineárne rekurentné postupnosti nad konečnými telesami

Cieľom tejto kapitoly je podať dostatočný teoretický základ pre analýzu rekurentných postupností ako pseudonáhodných generátorov čísel. Definujeme, čo to lineárna rekurencia je, odhalíme fundamentálny vzťah s charakteristickým polynómom a uvedieme základné fakty o periódach týchto postupností. To nám poslúži ako odrazový mostík pre analýzu maximálnych rekurentných postupností v ďalšej kapitole.

V celej kapitole budeme pracovať s oborom konečných telies.

3.1 Lineárne rekurentné postupnosti

Lineárne rekurentné postupnosti sú špeciálne typy postupností. Rekurentné znamená, že ďalší člen postupnosti závisí na predchádzajúcich a v lineárnych postupnostiach bude táto závislosť lineárna. Môžeme teda uviesť definíciu:

Definícia 3.1. *Lineárnou rekurentnou postupnosťou* rádu $k \in \mathbb{N}_0$ nad konečným telesom $\mathbb{F}_q$ nazveme postupnosť $\{s_n\}_{n=0}^{\infty}, s_n \in \mathbb{F}_q$ spĺňajúcu

$$s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_1 s_{n+1} + a_0 s_n, \qquad n \in \mathbb{N}_0 \tag{3.1}$$

pre nejaké $a_i \in \mathbb{F}_q,\ i \in \{0, \ldots, k-1\},\ a_0 \neq 0$.

V tom prípade hovoríme, že $\{s_n\}$ *spĺňa rekurenciu (rekurentný vzťah)* (3.1).

Značenie. Namiesto $\{s_n\}_{n=0}^{\infty}, s_n \in \mathbb{F}_q$ budeme jednoducho písať $s \in \mathbb{F}_q^{\infty}$. Vo zvyšku kapitoly, pokiaľ nebude uvedené inak, budeme používať značenie z tejto definície, predovšetkým k pre rád rekurencie a $n \in \mathbb{N}_0$.

Poznámka. Podmienka $a_0 \neq 0$ je čisto technická. Ak by vzťah platil pre $a_0 = 0$, mohli by sme tento člen vynechať a napísať rekurenciu menšieho rádu. Jediný rozdiel by bol v tom, že prvých pár členov postupnosti by mohlo byť ľubovoľných, pretože by pre ne neplatil žiaden vzťah. (Pretože rovnosť vyžadujeme pre $n \in \{0, 1, \dots\}$.)

Príklad.

- $s_0 = 0,\ s_1 = 1,\ s_{n+2} = s_{n+1} + s_n,\ s_n \in \mathbb{F}_q$ je Fibonacciho postupnosť v $\mathbb{F}_q$. Je to postupnosť rádu 2. Napríklad pre $\mathbb{F}_5$:

s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	$\dots$
0	1	1	2	3	0	3	3	1	4	0	$\dots$

- *Nulová postupnosť* $s_n = 0$ pre každé $n \in \mathbb{N}_0$ je rádu 0 a spĺňa každú rekurenciu.

Triviálny, avšak dôležitý dôsledok definície prezentuje nasledujúce tvrdenie:

Tvrdenie 3.2.

(i) Lineárne rekurentné postupnosti nad $\mathbb{F}_q$ tvoria lineárny priestor nad $\mathbb{F}_q$.

(ii) Lineárne rekurentné postupnosti nad $\mathbb{F}_q$ spĺňajúce tú istú rekurenciu tvoria lineárny podpriestor priestoru z časti (i).

Dôkaz. Obe časti sú triviálnym dôsledkom toho, že násobok lineárnej postupnosti a súčet dvoch lineárnych postupností je zase lineárna postupnosť. □

Definícia 3.3. Postupnosť s je *periodická s periódou* $p \in \mathbb{N}$, ak platí $s_n = s_{n+p}$ pre každé $n \in \mathbb{N}_0$.

Tvrdenie 3.4.

(i) Každá lineárna rekurentná postupnosť nad konečným telesom je periodická.

(ii) Každá periodická postupnosť nad konečným telesom je lineárna rekurentná postupnosť.

(iii) Počet lineárnych rekurentných postupností nad $\mathbb{F}_q$ spĺňajúcich tu istú lineárnu rekurenciu rádu k je q^k.

Dôkaz.

(i) Pre n väčšie než rád rekurencie závisí člen s_n len na predošlých k členoch. Všetkých možných k-tic je však len q^k, takže niekedy sa musia dve k-tice zopakovať, označme $(s_i, \ldots, s_{i+k-1}) = (s_j, \ldots, s_{j+k-1}),\ j > i \geqslant 0$.

Členy s_{i+k} a s_{j+k} majú rovnakých k predošlých členov, takže sa musia rovnať. Indukciou rovnosť rozšírime na $s_{i+n} = s_{j+n}, n \in \mathbb{N}_0$.

Zostáva rovnosť rozšíriť na členy skoršie než s_i. Úpravou rekurentného vzťahu (využívame z definície $a_0 \neq 0$)

$$s_n = (s_{n+k} - a_{n+k-1}s_{n+k-1} - \ldots - a_1 s_{n+1})/a_0$$

dostávame, že predošlý člen je jednoznačne určený k nasledujúcimi. Takže úvahu môžeme previesť aj opačným smerom a $s_n = s_{n+j-i},\ n \in \mathbb{N}_0$.

(ii) Ak je postupnosť periodická s perióodou p, spĺňa rekurenciu $s_{n+p} = s_n$.

(iii) Postupnosť s danou lineárnou rekurenciou rádu k je určená prvými k prvkami, na voľbu ktorých máme q^k možností.

□

Definícia 3.5. Nech postupnosť s spĺňa rekurenciu rádu k. Potom ako *n-tý stavový vektor* postupnosti označíme

$$\mathbf{s}_n = (s_n, \ldots, s_{n+k-1}).$$

Ako sa neskôr ukáže, stavový vektor je dôležitý pojem, ktorý nám uľahčí chápanie lineárnych rekurentných postupností. V tomto momente si môžeme napríklad uvedomiť, že n-tý stavový vektor jednoznačne určuje ďalší člen postupnosti s_{n+k}, čo sme využili v minulom dôkaze.

Predošlé dve tvrdenia nám ponúkajú vhľad do štruktúry všetkých postupností spĺňajúcich danú rekurenciu r rádu k. Zostrojme k postupností $e^{(i)}$ ($i \in \{0, \ldots, k-1\}$) tak, že počiatočný stavový vektor postupnosti $e^{(i)}$ bude

$$\mathbf{e}_0^{(i)} = (e_0^{(i)}, e_2^{(i)}, \ldots, e_i^{(i)}, \ldots, e_{k-1}^{(i)}) = (0, 0, \ldots, 1, \ldots, 0),$$

t.j. $e_i^{(i)} = 1$ a $e_j^{(i)} = 0$ pre $i \neq j$. Zvyšok postupnosti je určený rekurentným vzťahom.

Nech teraz máme konkrétnu postupnosť s spĺňajúcu tú istú rekurenciu r. Potom s vieme vyjadriť ako lineárnu kombináciu postupností $e^{(i)}$, konkrétne

$$s = s_0 e^{(0)} + \cdots + s_{k-1} e^{(k-1)}$$

Okrem toho sú $e^{(i)}$ zrejme lineárne nezávislé, takže tvoria bázu lineárneho priestoru z Tvrdenia 3.2(ii).

Príklad. Pre Fibonacciho postupnosť nad $\mathbb{F}_5$ zvoľme postupnosť začínajúcu $s_0 = 3,\ s_1 = 2$. Potom:

$$\begin{aligned} e^{(0)} &= (1, 0, 1, 1, 2, 3, 0, 3, \dots) \\ e^{(1)} &= (0, 1, 1, 2, 3, 0, 3, 3, \dots) \\ s &= (3, 2, 0, 2, 2, 4, 1, 0, \dots) \end{aligned}$$

Vidíme, že naozaj platí $3e_n^{(0)} + 2e_n^{(1)} = s_n$.

Tvrdenie 3.6.

(i) Priestor postupností spĺňajúcich tú istú rekurenciu rádu k má dimenziu k nad $\mathbb{F}_q$.

(ii) Lineárne rekurentné postupnosti $s^{(0)}, \dots, s^{(m-1)}, m \in \mathbb{N}$ spĺňajúce tú istú rekurenciu rádu k sú lineárne nezávislé práve vtedy, keď sú lineárne nezávislé ich počiatočné stavové vektory

$$\mathbf{s}_0^{(0)}, \dots, \mathbf{s}_0^{(m-1)}$$

Dôkaz.

(i) Vektory $e^{(0)}, \dots, e^{(k-1)}$ z predošlej úvahy tvoria bázu tohto priestoru.

(ii) Z predošlej úvahy taktiež vyplýva, že zobrazenie priradzujúce súradnice v báze z (i)

$$s \mapsto (s_0, \dots, s_{k-1}) = \mathbf{s}_0$$

z priestoru všetkých postupností spĺňajúcich tú istú rekurenciu rádu k do $\mathbb{F}_q^k$ je izomorfizmus vektorových priestorov, z čoho priamo plynie dokazované tvrdenie.

□

3.2 Charakteristický polynóm

Motiváciou k zavedeniu pojmu *charakteristický polynóm* je pokus o explicitné vyjadrenie n-tého člena rekurentnej postupnosti.

Majme rekurentný vzťah $s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n$ a postupnosť s, ktorá ho spĺňa. Skúsime najprv nájsť nejakú postupnosť t, ktorú by sme dokázali vyjadriť explicitne a tiež by daný vzťah spĺňala.

Vyskúšajme voľbu $t_n = \lambda^n$. V tom prípade má platiť

$$\begin{aligned} \lambda^{n+k} &= a_{k-1}\lambda^{n+k-1} + \cdots + a_0\lambda^n \\ \lambda^k &= a_{k-1}\lambda^{k-1} + \cdots + a_0 \qquad \text{pre } \lambda \neq 0 \\ 0 &= \lambda^k - a_{k-1}\lambda^{k-1} - \ldots - a_0. \end{aligned}$$

Teda λ je koreňom istého polynómu stupňa k. Ak tento polynóm má k rôznych nenulových koreňov $\lambda_0, \ldots, \lambda_{k-1}$, našli sme rovno k postupností spĺňajúcich danú rekurenciu.

Navyše v tom prípade musia byť tieto postupnosti lineárne nezávislé. Ich počiatočné stavové vektory sú totiž

$$\begin{gathered} (1, \lambda_0, \ldots, \lambda_0^{k-1}) \\ \vdots \\ (1, \lambda_{k-1}, \ldots, \lambda_{k-1}^{k-1}). \end{gathered}$$

Tie tvoria maticu, ktorej determinant je nenulový, pretože je to Vandermondov determinant pre rôzne čísla λ_i. Teda sú lineárne nezávislé a podľa Tvrdenia 3.6 sú nezávislé aj príslušné postupnosti.

Keďže týchto postupností je k, tvoria bázu priestoru všetkých rekurentných postupností spĺňajúcich danú rekurenciu. Špeciálne vieme aj postupnosť s napísať ako ich lineárnu kombináciu a dostávame žiadané explicitné vyjadrenie

$$s_n = c_0\lambda_0^n + \cdots + c_{k-1}\lambda_{k-1}^n.$$

Otázkou zostáva, kedy má spomenutý polynóm k koreňov, čo robiť, ak tomu tak nie je a ako nájsť príslušné koeficienty c_i. Odpovede na tieto otázky podávajú nasledujúce riadky.

Definícia 3.7. Pre rekurentný vzťah

$$s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n$$

definujeme *charakteristický polynóm*

$$f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_1 x - a_0.$$

Poznámka. Majme na pamäti, že z definície $a_0 \neq 0$, a teda 0 nie je koreňom f. Každý monický polynóm s $f(0) \neq 0$ je zrejme charakteristický pre práve jeden rekurentný vzťah, ktorý jednoznačne určuje.

Veta 3.8. *Majme postupnosť $s \in \mathbb{F}_q^\infty$ spĺňajúcu rekurentný vzťah z predošlej definície. Nech sa charakteristický polynóm príslušnej rekurencie rozkladá v nadtelese $\mathbb{F}_{q^l}, l \in \mathbb{N}$ na k lineárnych členov*

$$f(x) = (x - \lambda_0)^{\alpha_0} \cdots (x - \lambda_{m-1})^{\alpha_{m-1}},$$

kde $m \in \{0, \ldots, k-1\}$, $\alpha_0 + \cdots + \alpha_{m-1} = k$ a pre rôzne $i \in \{0, \ldots, m-1\}$ sú $\lambda_i \in \mathbb{F}_{q^l}$ rôzne.

Potom existujú polynómy $p_0, \ldots, p_{m-1} \in \mathbb{F}_{q^l}[x]$ také, že

$$s_n = p_0(n)\lambda_0^n + \cdots + p_{m-1}(n)\lambda_{m-1}^n \tag{3.2}$$

spĺňajúce $\deg(p_i) < \alpha_i$.

Poznámka. Všimnime si, že v rovnici 3.2 je na ľavej strane prvok $\mathbb{F}_q$, zatiaľ čo na pravej strane súčet prvkov $\mathbb{F}_{q^l}$. Rovnosť teda hovorí, že súčet na pravej strane padne do podtelesa $\mathbb{F}_q$ telesa $\mathbb{F}_{q^l}$.

Dôkaz. (Vety 3.8) Dôkaz budeme viesť vo viacerých krokoch. Budeme postupovať podobne, ako v texte vyššie.

1. *Pre $i \in \{0, \ldots, m-1\}, j \in \{0, \ldots, \alpha_i - 1\}$ postupnosti*

   $$t_n^{(i,j)} = n^{\underline{j}} \lambda_i^n$$

   spĺňajú rovnakú rekurenciu, ako postupnosť s.

   Vieme, že $\lambda_i \neq 0$ je α_i-násobný koreň polynómu f, takže bude tiež α_i-násobným koreňom polynómu $x^n f(x)$. Z algebry vieme, že λ_i je koreňom j-tej derivácie takéhoto polynómu pre $j < \alpha_i$:

   $$\begin{aligned} 0 &= \left[x^n f(x)\right]^{(j)}(\lambda_i) \\ &= \left[x^{n+k} - a_{k-1}x^{n+k-1} - \ldots - a_0 x^n\right]^{(j)}(\lambda_i) \\ &= \left[(n+k)^{\underline{j}} x^{n+k-j} - \ldots - a_0 n^{\underline{j}} x^{n-j}\right](\lambda_i) \\ &= (n+k)^{\underline{j}} \lambda_i^{n+k-j} - \ldots - a_0 n^{\underline{j}} \lambda_i^{n-j} \end{aligned}$$

   Prenásobením $\lambda_i^j \neq 0$ a prevedením záporných členov na druhú stranu napokon dostávame

   $$t_{n+k}^{(i,j)} = a_{k-1} t_{n+k-1}^{(i,j)} + \cdots + a_0 t_n^{(i,j)}.$$

2. *Postupnosti $t_n^{(i,j)}$ z predošlého bodu sú lineárne nezávislé.*

   Podľa Tvrdenia 3.6 stačí dokázať, že ich počiatočné stavové vektory sú lineárne nezávislé, t.j. že matica $k \times k$

$$\begin{aligned} V &= (\mathbf{t}_0^{(0,0)\,T}, \ldots, \mathbf{t}_0^{(0,\alpha_0-1)\,T}, \ldots, \mathbf{t}_0^{(m-1,0)\,T}, \ldots, \mathbf{t}_0^{(m-1,\alpha_{m-1}-1)\,T}) \\ &= \begin{pmatrix} 1 & 0 & 0 & \cdots & 1 & 0 & \cdots \\ \lambda_0 & 1 & 0 & \cdots & \lambda_{m-1} & 1 & \cdots \\ \lambda_0^2 & 2\lambda_0 & 2 & \cdots & \lambda_{m-1}^2 & 2\lambda_{m-1} & \cdots \\ \lambda_0^3 & 3\lambda_0^2 & 6\lambda_0 & \ddots & \lambda_{m-1}^3 & 3\lambda_{m-1}^2 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \end{aligned}$$

   je regulárna. To nastane práve vtedy, keď je regulárna matica W, ktorú z V dostaneme predelením každého stĺpcového vektora $\mathbf{t}_0^{(i,j)}$ číslom $j!$. Táto matica je tzv. *zovšeobecnená Vandermondova matica*, ktorá podľa Kalmana [3] má determinant

$$\det W = \prod_{0 \leqslant i < j < m} (\lambda_j - \lambda_i)^{\alpha_i \alpha_j}.$$

   Ten je vďaka rôznym λ_i nenulový, a teda aj V musí byť regulárna.

3. Spojením predošlých dvoch bodov dostávame, že k postupností $t_n^{(i,j)}$ tvorí bázu priestoru všetkých postupností spĺňajúcich tú istú rekurenciou ako s, a teda s sa dá napísať ako ich lineárna kombinácia:

$$\begin{aligned} s_n &= \sum_{i=0}^{m-1} \sum_{j=0}^{\alpha_i-1} c_{i,j}\, t_n^{(i,j)} = \sum_{i=0}^{m-1} \sum_{j=0}^{\alpha_i-1} c_{i,j}\, n^{\underline{j}}\, \lambda_i^n \\ &= \sum_{i=0}^{m-1} c_{i,0}\lambda_i^n + \cdots + c_{i,\alpha_i-1} n \cdots (n-\alpha_i+2)\lambda_i^n. \end{aligned}$$

   Po roznásobení a zoskupení koeficientov pri rovnakých mocninách n dostávame žiadané tvrdenie

$$s_n = \sum_{i=0}^{m-1} \left(\tilde{c}_{i,0} + \cdots + \tilde{c}_{i,\alpha_i-1} n^{\alpha_i-1}\right) \lambda_i^n.$$

□

Dôsledok 3.9. *Nech s je lineárna rekurentná postupnosť rádu k nad $\mathbb{F}_q$, ktorej charakteristický polynóm je ireducibilný nad $\mathbb{F}_q$.*

Potom existujú $\lambda, c_0, \ldots, c_{k-1} \in \mathbb{F}_{q^k}$ také, že

$$s_n = c_0\lambda^n + c_1\lambda^{qn} + \cdots + c_{k-1}\lambda^{q^{k-1}n}.$$

Dôkaz. Označme charakteristický polynóm f a λ nech je jeden jeho koreň v nadtelese $\mathbb{F}_{q^k}$. Keďže f je ireducibilný, z Tvrdenia 2.10 vieme, že všetky jeho korene sú jednoduché a sú to práve čísla $\lambda, \lambda^q, \ldots, \lambda^{q^{k-1}}$.

Aplikáciou predošlej vety dostávame, že existujú polynómy p_i také, že

$$s_n = p_0(n)\lambda^n + \cdots + p_{k-1}(n)\lambda^{q^{k-1}n}.$$

Ale podmienka na stupne dáva $\deg(p_i) < 1$, takže p_i sú konštanty z $\mathbb{F}_{q^k}$. □

Príklad. Nech s je Fibonacciho postupnosť nad $\mathbb{F}_q$. Jej charakteristický polynóm je $f(x) = x^2 - x - 1$.

- Nad $\mathbb{F}_3$ je tento polynóm ireducibilný, pretože 0, 1 ani 2 nie sú koreňom. Vezmime si rozšírenie $\mathbb{F}_{3^2}$, ktoré zostrojíme napr. ako $\mathbb{F}_3[\alpha]/f(\alpha)$. Korene $f(x)$ v tomto rozšírení sú α a $\alpha^3 = 2\alpha + 1$. Potrebujeme nájsť konštanty c_0, c_1 tak, aby
$$s_n = c_0\alpha^n + c_1(2\alpha + 1)^n.$$
Z počiatočných podmienok $s_0 = 0$ a $s_1 = 1$ dostávame sústavu rovníc
$$\begin{aligned} s_0 &= 0 = c_0 + c_1 \\ s_1 &= 1 = c_0\alpha + c_1(2\alpha + 1), \end{aligned}$$
ktorej vyriešením získame $c_0 = \alpha + 1, c_1 = 2\alpha + 2$. Môžeme teda explicitne vyjadriť
$$s_n = (\alpha + 1)\alpha^n + (2\alpha + 2)(2\alpha + 1)^n.$$
- Nad $\mathbb{F}_5$ sa tento polynóm rozkladá ako $f(x) = (x - 3)^2$. To znamená, že riešenie budeme hľadať v tvare
$$s_n = c_0 3^n + c_1 n 3^n.$$
Dosadením počiatočných podmienok dostávame rovnice
$$\begin{aligned} s_0 &= 0 = c_0 \\ s_1 &= 1 = 3c_0 + 3c_1. \end{aligned}$$
Riešením je $c_0 = 0$ a $c_1 = 2$, takže explicitné vyjadrenie je
$$s_n = 2n3^n.$$

Poznámka. Podobným spôsobom sa dá nájsť explicitný vzorec pre postupnosti nad celými číslami. Rozdiel je iba v tom, že korene charakteristického polynómu hľadáme v komplexnom obore. Napríklad v prípade Fibonacciho postupnosti sú korene zlatý rez φ a mínus jeho prevrátená hodnota, takže explicitné vyjadrenie bude v tvare

$$F_n = c_0\varphi^n + c_1(-\varphi)^{-n}.$$

Pohľadom na explicitný vzorček ihneď vidíme, že táto postupnosť sa bude správať exponenciálne. Navyše člen φ^{-n} konverguje k nule, teda pre veľké n bude $F_n \approx c_0\varphi^n$. Z toho hneď dostávame známe tvrdenie, že podiel dvoch za sebou idúcich Fibonacciho čísel konverguje k zlatému rezu.

Pre úplnosť dodávame, že konštanty vyjdú $c_0 = 1/\sqrt{5}$ a $c_1 = -1/\sqrt{5}$.

Ako sme už spomenuli, lineárna rekurentná postupnosť spĺňa viac rekurentných vzťahov – ak má periódu p, tak určite spĺňa vzťahy $s_n = s_{n+kp}$ pre každé $k \in \mathbb{N}$. Každému z týchto vzťahov prislúcha charakteristický polynóm. Ukážeme si, že tieto vzťahy spolu úzko súvisia – ich charakteristické polynómy takmer tvoria ideál.

Na dokázanie presného tvrdenia budeme potrebovať mierne technickú lemu. Zavádzame preto nasledujúcu pomocnú definíciu:

Definícia 3.10. Pre $a_i \in \mathbb{F}_q,\ i \in \{0, \ldots, k\}$ nazveme vzťah

$$a_k s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n.$$

zovšeobecneným rekurentným vzťahom (rekurenciou). Príslušným *zovšeobecneným charakteristickým polynómom* myslíme polynóm

$$a_k x^k - a_{k-1}x^{k-1} - \ldots - a_0.$$

Poznámka. Na rozdiel od pôvodnej definície pripúšťame $a_0 = 0$ a tiež pripúšťame koeficient pri najvyššom člene. Jedná sa teda o zovšeobecnenie pojmov rekurentný vzťah a charakteristický polynóm. Všimnime si, že sa navzájom jednoznačne určujú.

Poznamenajme ešte, že ak s spĺňa zovšeobecnenú rekurenciu a $a_k \neq 0$, tak pre m najmenšie také, že $a_m \neq 0$, postupnosť spĺňa tiež jednoznačne určenú klasickú rekurenciu[1]

$$s_{n+k-m} = (a_{k-1}s_{n+k-m-1} + \cdots + a_m s_n)/a_k.$$

[1]Pozorný čitateľ by mohol namietnuť, že rekurencia platí až od nejakého člena n_0. Avšak vďaka tomu, že s je periodická, musí platiť už pre prvé členy.

Lema 3.11. *Nech lineárna rekurentná postupnosť $s \in \mathbb{F}_q^\infty$ spĺňa dve zovšeobecnené rekurencie so zovšeobecnenými charakteristickými polynómami $f(x)$ a $g(x)$. Potom s spĺňa aj zovšeobecnené rekurencie so zovšeobecnenými charakteristickými polynómami*

(i) $cx^m f(x)$ *pre* $c \in \mathbb{F}_q, m \in \mathbb{N}_0$,

(ii) $f(x) + g(x)$,

(iii) $h(x)f(x)$ *pre* $h(x) \in \mathbb{F}_q[x]$,

(iv) $f(x) \bmod g(x)$.

Dôkaz. V celom dôkaze sa bude jednať o zovšeobecnené rekurencie a charakteristické polynómy, budeme preto slovo „zovšeobecnený“ vynechávať.

Označme

$$f(x) = a_u x^u - a_{u-1}x^{u-1} - \ldots - a_0, \qquad g(x) = b_v x^v - b_{v-1}x^{v-1} - \ldots - b_0.$$

Pôvodná postupnosť potom spĺňa rekurencie

$$a_u s_{n+u} = a_{u-1}s_{n+u-1} + \cdots + a_0 s_n, \qquad b_v s_{n+v} = b_{v-1}s_{n+v-1} + \cdots + b_0 s_n.$$

(i) Prenásobením prvej rekurencie c a posunutím o m členov dostávame, že s spĺňa tiež rekurenciu

$$ca_u s_{n+m+u} = ca_{u-1}s_{n+m+u-1} + \cdots + ca_0 s_{n+m}.$$

Tejto rekurencii prislúcha práve charakteristický polynóm $cx^m f(x)$.

(ii) Prevedením na jednu stranu a súčtom oboch rekurencií dostávame vzťah

$$\begin{aligned} 0 = \quad & a_u s_{n+u} - a_{u-1}s_{n+u-1} - \ldots - a_0 s_n \\ + \quad & b_v s_{n+v} - b_{v-1}s_{n+v-1} - \ldots - b_0 s_n. \end{aligned}$$

Tomu prislúcha práve charakteristický polynóm $f(x) + g(x)$.

(iii) Opakovaným použitím (i) a (ii) dokážeme vytvoriť ľubovoľný polynomiálny násobok $f(x)$.

(iv) Pre $h(x) = f(x) \operatorname{div} g(x)$ použitím všetkých troch bodov dostávame, že s spĺňa aj rekurenciu $f(x) - h(x)g(x) = f(x) \bmod g(x)$.

□

Definícia 3.12. *Minimálnou rekurenciou* postupnosti s nazveme (ľubovoľný) rekurentný vzťah najmenšieho možného rádu, ktorý postupnosť s spĺňa.

Minimálnym polynómom nazveme charakteristický polynóm minimálnej rekurencie.

Tvrdenie 3.13. *Minimálny polynóm postupnosti delí charakteristický polynóm každej rekurencie, ktorú s spĺňa.*

Dôkaz. Označme $f(x)$ tento minimálny polynóm. Pre spor predpokladajme, existuje rekurencia s charakteristickým polynómom $g(x)$ takým, že $f(x) \nmid g(x)$.

Postupnosť s podľa predošlej lemy musí spĺňať zovšeobecnenú rekurenciu s charakteristickým polynómom $h(x) = g(x) \bmod f(x)$. Nutne $\deg(h) < \deg(f)$, takže ak je $h(x)$ nenulový polynóm, určuje zovšeobecnenú rekurenciu menšieho rádu. Tá sa podľa poznámky vyššie dá prepísať na klasickú rekurenciu tiež menšieho rádu, a to je spor. Preto $h(x) \equiv 0$ a $f(x) \mid g(x)$. □

Dôsledok 3.14. *Minimálny polynóm a teda aj minimálna rekurencia postupnosti sú jednoznačne určené.*

Dôsledok 3.15. *Ak postupnosť spĺňa rekurenciu s ireducibilným charakteristickým polynómom, tak je tento polynóm minimálny.*

Predchádzajúca lema a tvrdenie dokopy hovoria, že zovšeobecnené charakteristické polynómy pre všetky zovšeobecnené rekurentné vzťahy danej postupnosti nad $\mathbb{F}_q$ tvoria spomínaný ideál v okruhu polynómov $\mathbb{F}_q[x]$. Ten je nutne hlavný a jeho generátorom je minimálny polynóm postupnosti.

3.3 Minimálna perióda

Podobne, ako postupnosť spĺňa viacero rekurencií, má aj viacero períód – napríklad celočíselný násobok periódy je tiež perióda. *Minimálna perióda* označuje tú najkratšiu z nich.

Tvrdenie 3.16. *Minimálna perióda delí ľubovoľnú periódu postupnosti.*

Dôkaz. Nech p je minimálna perióda a q nejaká iná, t.j. $s_n = s_{n+p} = s_{n+q}$. Potom

$$s_n = s_{n+q} = s_{n+q-p(q \operatorname{div} p)} = s_{n+(q \bmod p)}.$$

Ak by $p \nmid q$, tak by $(q \bmod p)$ bola menšia perióda než p, čo je spor. □

Tvrdenie 3.17. *Nech postupnosť $s \in \mathbb{F}_q^\infty$ spĺňa rekurenciu rádu k. Potom jej minimálna perióda je nanajvýš $q^k - 1$.*

Dôkaz. Ďalší člen postupnosti závisí na k-tici predošlých členov. Všetkých možných k-tic je q^k, takže medzi q^k za sebou idúcimi sa musí nejaká zopakovať. V tom prípade sa postupnosť zacyklí a teda minimálna perióda je nanajvýš q^k.

Avšak ak postupnosť obsahuje k za sebou idúcich núl, všetky ďalšie členy sú nulové a z periodicity je to nulová postupnosť. Tá má periódu 1. Inak postupnosť túto k-ticu neobsahuje a teda minimálna perióda je nanajvýš $q^k - 1$. □

Poznámka. Táto horná hranica sa dá dosiahnuť pre každé $\mathbb{F}_q$. Voľme $k = 1$, označme α primitívny prvok v $\mathbb{F}_q$ a položme

$$s_0 = 1, \qquad s_{n+1} = \alpha s_n.$$

Potom $s_n = \alpha^n$ prejde všetkých $q - 1$ prvkov multiplikatívnej podgrupy $\mathbb{F}_q$ a potom sa zacyklí. Neskôr si ukážeme, že maximum $q^k - 1$ sa dá dosiahnuť pre každé $k \in \mathbb{N}$.

Naše kroky budú smerovať k dvom vetám, ktoré nám dajú nástroj na určenie dĺžky minimálnej periódy. Prvá veta sa bude týkať sprievodnej matice, ktorú si vzápätí predstavíme a druhá bude využívať vlastnosti minimálneho polynómu.

Tvrdenie 3.18. *Nech postupnosť s spĺňa rekurenciu $s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n$ rádu $k \in \mathbb{N}$. Označme*

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix},$$

pre $k = 1$ definujeme $A = (a_0)$. Potom

$$\mathbf{s}_0 A^n = \mathbf{s}_n$$

Dôkaz. Násobením overíme, že

$$\begin{aligned} \mathbf{s}_n A &= (s_n,\ \ldots\ ,\ s_{n+k-1})A \\ &= (s_{n+1},\ \ldots\ ,\ s_{n+k-1},\ a_{k-1}s_{n+k-1} + \cdots + a_0 s_n) \\ &= (s_{n+1},\ \ldots\ ,\ s_{n+k-1},\ s_{n+k}) = \mathbf{s}_{n+1}. \end{aligned}$$

Odtiaľ tvrdenie plynie indukciou. □

Definícia 3.19. Pre danú rekurenciu budeme maticu z predošlého tvrdenia nazývať *sprievodná matica.*

Sprievodná matica úzko súvisí s charakteristickým polynómom $f(x)$ danej rekurencie. Po chvíli počítania sa dá ľahko overiť, že je to napríklad jej charakteristický polynóm.

Pomocou sprievodnej matice sa tiež dá iným spôsobom odvodiť explicitný vzorec pre n-tý člen postupnosti, uvedieme stručný návod. Z lineárnej algebry môžeme upraviť

$$\mathbf{s}_n = \mathbf{s}_0 A^n = \mathbf{s}_0 M J^n M^{-1},$$

kde J je Jordanov tvar matice A. Na jeho diagonále sa nachádzajú korene charakteristického polynómu $\lambda_0, \ldots, \lambda_{k-1}$. Ak sú rôzne, tak je J diagonálna a tým pádom aj J^n, ktorá má na diagonále n-té mocniny týchto koreňov.

Matica MJ^nM^{-1} má ako svoje prvky ich lineárne kombinácie, teda po vynásobení zľava vektorom $\mathbf{s}_0$ bude mať výsledok v každej zložke lineárnu kombináciu $\lambda_0^n, \ldots, \lambda_{k-1}^n$. Teraz stačí porovnať prvé zložky vektorov na oboch stranách a zistíme, že s_n sa dá napísať ako lineárna kombinácia $\lambda_0^n, \ldots, \lambda_{k-1}^n$.

V pôvodnom postupe na odvodenie sme potrebovali uhádnuť, že postupnosti tvaru λ^n pre vhodné λ spĺňajú daný rekurentný vzťah. Tento spôsob odvodenia ukazuje, ako sa na to dalo prísť. Zároveň zovšeobecnením postupu pre viacnásobné korene sa dá odvodiť všeobecný vzorec.

Vráťme sa ale naspäť k perióde postupnosti.

Lema 3.20. *Nech k je rád minimálnej rekurencie. Potom vektory $\mathbf{s}_0, \ldots, \mathbf{s}_{k-1}$ sú lineárne nezávislé.*

Dôkaz. Pre spor predpokladajme, že existujú čísla $b_0, \ldots, b_{k-1} \in \mathbb{F}_q$, aspoň jedno z nich nenulové, také, že

$$b_0\mathbf{s}_0 + \cdots + b_{k-1}\mathbf{s}_{k-1} = 0$$

Potom pre asociovanú maticu A minimálnej rekurencie platí

$$\begin{aligned} 0 &= (b_0\mathbf{s}_0 + \cdots + b_{k-1}\mathbf{s}_{k-1})A^n \\ &= b_0\mathbf{s}_0A^n + \cdots + b_{k-1}\mathbf{s}_{k-1}A^n \\ &= b_0\mathbf{s}_n + \cdots + b_{k-1}\mathbf{s}_{n+k-1}. \end{aligned}$$

Porovnaním prvých zložiek vektorov dostávame

$$0 = b_0 s_n + \cdots + b_{k-1} s_{n+k-1}.$$

Keď najvyšší člen s nenulovým b_i prevedieme na druhú stranu a podelíme, získame lineárnu rekurenciu menšieho rádu než k, čo je spor s minimalitou.

□

Veta 3.21. *Minimálna perióda postupnosti sa rovná rádu sprievodnej matice minimálnej rekurencie.*

Dôkaz. Označme p minimálnu periódu, k dĺžku minimálnej rekurencie a A jej sprievodnú maticu. Potom

$$\mathbf{s}_0 A^p = \mathbf{s}_0, \quad \ldots, \quad \mathbf{s}_{k-1} A^p = \mathbf{s}_{k-1}.$$

To znamená, že zobrazenie A^p je identické na prvých k stavových vektoroch. Avšak podľa predošlej lemy sú tieto vektory lineárne nezávislé, takže A^p je jednotková matica.

Pre menší exponent r nemôže byť A^r jednotková matica, pretože by r bola menšia perióda než p. Takže p je rád matice A v $M_k(\mathbb{F}_q)$. □

Posledným nástrojom na skúmanie minimálnej periódy, ktorý si predstavíme, je rád polynómu.

Definícia 3.22. *Rád polynómu* $f \in \mathbb{F}_q[x]$ takého, že $x \nmid f(x)$, definujeme ako najmenšie prirodzené číslo d také, že $f(x) \mid x^d - 1$. Značíme $d = \mathrm{ord}(f)$.

Poznámka. Podľa Vety 2.9 vieme, že polynóm f má všetky svoje korene v nejakom rozkladovom nadtelese $\mathbb{F}_{q^k}$. Podľa Tvrdenia 2.3 všetky nenulové prvky tohto nadtelesa sú korene $x^{q^k} - 1$. Keďže však polynóm f nemá koreň 0, číslo d určite existuje a je nanajvýš q^k.

Tvrdenie 3.23. *Nech* $f \in \mathbb{F}_q[x]$ *stupňa* k *taký, že* $x \nmid f(x)$ *a navyše* f *má len jednoduché korene. Potom rád* f *sa rovná najmenšiemu spoločnému násobku rádov jeho koreňov v* $\mathbb{F}_{q^k}$.

Dôkaz. Keďže má f iba jednoduché korene, tak delí polynóm $x^d - 1$ práve vtedy, keď $\lambda^d - 1 = 0$ alebo ekvivalentne $\lambda^d = 1$ pre každý jeho koreň λ. Číslo d musí byť teda deliteľné rádom každého koreňa a najmenšie také d je práve ich najmenší spoločný násobok. □

Špeciálne, ak je f stupňa k ireducibilný, má rôzne korene a každý z nich má v $\mathbb{F}_{q^k}$ rovnaký rád. Preto môžeme formulovať nasledovný dôsledok:

Dôsledok 3.24. *Rád ireducibilného polynómu rôzneho od* x *je rovnaký, ako rád ľubovoľného jeho koreňa.*

Veta 3.25. *Minimálna perióda postupnosti sa rovná rádu jej minimálneho polynómu.*

Dôkaz. Označme p minimálnu periódu, f minimálny polynóm a d rád f. Keďže $f(x) \mid x^d - 1$, podľa Lemy 3.11 spĺňa postupnosť aj rekurenciu určenú polynómom $x^d - 1$. Tá je $s_{n+d} = s_n$, takže $d \geqslant p$.

Naopak, podľa Tvrdenia 3.13 musí minimálny polynóm deliť charakteristický polynóm určený rekurenciou $s_{n+p} = s_n$, takže $f(x) | x^p - 1$ a teda $d \leqslant p$. □

Dôsledok 3.26. *Minimálna perióda postupnosti $s \in \mathbb{F}_q^\infty$ s ireducibilným charakteristickým polynómom $f(x)$ stupňa k je rovná rádu ľubovoľného jeho koreňa v $\mathbb{F}_{q^k}$.*

Dôkaz. Keďže je $f(x)$ ireducibilný, podľa Dôsledku 3.15 je to minimálny polynóm postupnosti. Podľa predošlej vety je minimálna perióda jeho rád, avšak podľa Dôsledku 3.24 je to rád ľubovoľného jeho koreňa v rozkladovom nadtelese. □

Navyše ako vedľajší produkt dostávame nasledujúce zaujímavé tvrdenie:

Tvrdenie 3.27. *Nech f je monický polynóm stupňa k nad $\mathbb{F}_q$ taký, že $x \nmid f(x)$. Potom sprievodná matica rekurencie určenej f má rovnaký rád, ako polynóm f.*

Dôkaz. Označme r rekurentný vzťah, pre ktorý je f charakteristický polynóm. Zostrojme postupnosť s s týmto rekurentným vzťahom takú, že $\mathbf{s}_0 = (1, 0, \ldots, 0)$. Určite je to minimálna rekurencia tohto polynómu, pretože rekurencia menšieho rádu by pokračovala ako nulová postupnosť. Preto podľa predchádzajúcich dvoch viet je rád f rovnako ako rád sprievodnej matice r rovný minimálnej perióde tejto postupnosti, a teda sa rovnajú. □

Kapitola 4

Pseudonáhodné postupnosti

S rozmachom počítačov prišla potreba generovať náhodné čísla. Tie majú mnohé spôsoby využitia – používajú sa v hrách[1], fyzikálnych a štatistických simuláciách či v šifrovaní správ.

Z hľadiska programátora je potrebná nejaká metóda, ktorej opakované volania budú dávať náhodné čísla. Pre jednoduchosť si predstavme, že táto funkcia bude vracať náhodne 0 alebo 1 (náhodný *bit*), neskôr si ukážeme spôsob, ako pomocou takej generovať náhodné celé alebo reálne čísla.

Aké vlastnosti má mať takáto funkcia? Každé jej volanie by sa malo správať ako hod mincou, kde každá zo strán má pravdepodobnosť padnutia $\frac{1}{2}$. Veľa opakovaných volaní môžeme interpretovať ako postupnosť 0 a 1, pre ktorú dokážeme určiť nejaké kritéria:

- *(Distribučný test.)* V dlhom úseku postupnosti by sa relatívny pomer výskytu každého bitu mal blížiť k $\frac{1}{2}$.
- *(Sériový test.)* Všeobecne, relatívny pomer výskytu daného bloku dĺžky k medzi za sebou idúcimi blokmi dĺžky k by sa mal blížiť k 2^{-k}.
- *(Korelačný test.)* Keď vedľa vygenerovanej postupnosti napíšeme posunutú tú istú postupnosť, relatívny pomer zhôd a nezhôd by sa mal blížiť k $\frac{1}{2}$.

Samozrejme, kritérií by sme mohli vymyslieť omnoho viac. Existujú programy určené na testovanie náhodnosti postupností bitov, ktoré používajú desiatky kritérií[2]. Uvedomme si však, že neexistuje žiadne „absolútne“ kritérium na náhodnú

[1] Všetci si pamätáme napríklad hru míny.

[2] Napríklad programový balíček inštitútu *National Institute of Standards and Technology*: http://csrc.nist.gov/groups/ST/toolkit/rng/index.html (17.7.2010)

postupnosť, a to už len z toho dôvodu, že pri skutočne náhodnom generátore je postupnosť samých núl rovnako pravdepodobná, ako ľubovoľná iná postupnosť (a síce obe majú pravdepodobnosť 0). Na druhú stranu, často ani nechceme, aby vygenerovaná postupnosť bola úplne náhodná.[3]

Dostávame sa konečne ku konkrétnym implementáciám náhodnej metódy. Keďže počítače sú deterministické stroje, zaviesť do nich náhodu je problém. Ten sa rieši dvoma spôsobmi:

- Pripojiť snímač k nejakému náhodnému fyzikálnemu javu a vzorkovať z neho náhodné čísla. Napríklad známy server `random.org` sníma atmosférický šum ([4]).
- Generovať postupnosti čísel, ktoré sú síce deterministicky určené, ale vykazujú náhodné správanie. Keďže nie sú skutočne náhodné, nazývajú sa *pseudonáhodné postupnosti*.

Ako už názov kapitoly napovedá, my sa budeme zaoberať druhým variantom. Ako náhodnú postupnosť budeme brať *maximálnu rekurentnú postupnosť* nad $\mathbb{F}_2$. Tento pojem predstavíme v nadchádzajúcej podkapitole.

Naďalej budeme používať značenie zavedené v Definícii 3.1.

4.1 Maximálne rekurentné postupnosti

Definícia 4.1. Lineárnu rekurentnú postupnosť nad $\mathbb{F}_q$ rádu k nazveme *maximálnou rekurentnou postupnosťou*, ak má minimálnu periódu $q^k - 1$.

Pre pohodlie budeme tieto postupnosti nazývať jednoducho *maximálne postupnosti*, v literatúre sa niekedy tiež používa označenie m-postupnosti. Prívlastok „maximálne“ je namieste, pretože z Tvrdenia 3.17 vieme, že minimálna perióda nemôže byť dlhšia.

V nasledujúcej vete využijeme teoretický základ z minulej kapitoly a charakterizujeme všetky maximálne postupnosti.

Veta 4.2. *Lineárna rekurentná postupnosť nad $\mathbb{F}_q$ rádu k je maximálna práve vtedy, keď jej charakteristický polynóm je primitívny.*

[3] Uvažujme nasledujúci príklad. Školská inšpekcia chce na každej škole urobiť za rok 3 námatkové kontroly. Ak si pre každú školu vyberie z roka 3 náhodné dni, pravdepodobnosť, že dve kontroly nastanú ten istý mesiac, je cca 24%. Teda pri približne jednej zo štyroch škôl by kontroly boli blízko seba.

Dôkaz. Postupnosť je podľa Vety 3.25 maximálna práve vtedy, keď jej minimálny polynóm má rád $q^k - 1$. Označme tento polynóm f a predpokladajme, že tomu tak je, t.j. že $f(x)|x^{q^k-1} - 1$ a $q^k - 1$ je najmenší taký exponent. Potom f má len jednoduché korene, pretože delí polynóm $x^{q^k} - x$, ktorý má len jednoduché korene podľa Tvrdenia 2.3.

Ak f nie je ireducibilný, vďaka jednoduchým koreňom dá sa napísať ako súčin $2 \leqslant m \leqslant k$ rôznych ireducibilných polynómov $g_1, \ldots, g_m$. Použitím Tvrdenia 3.23 a jeho dôsledku

$$\begin{aligned} \operatorname{ord}(f) &= \operatorname{nsn}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_m)) \leqslant \operatorname{ord}(g_1) \cdots \operatorname{ord}(g_m) \\ &\leqslant (q^{\deg g_1} - 1) \cdots (q^{\deg g_m} - 1) < q^{\deg g_1 + \cdots + \deg g_m} - 1 \\ &= q^{\deg f} - 1 \leqslant q^k - 1, \end{aligned}$$

pričom druhá nerovnosť plynie z toho, že korene polynómu patria do rozkladového nadtelesa a posledná z toho, že f delí charakteristický polynóm a má teda stupeň nanajvýš k. Takže v tomto prípade postupnosť nie je maximálna.

Ak je f ireducibilný, jeho rád je rád ľubovoľného jeho koreňa. Takže má rád $q^k - 1$ práve vtedy, keď je primitívny rádu k. V tom prípade musí byť zároveň charakteristickým polynómom, čo sme chceli dokázať. □

Dôsledok 4.3. *Pre každé $k \in \mathbb{N}$ a ľubovoľné konečné teleso $\mathbb{F}_q$ existuje maximálna postupnosť rádu k.*

Dôkaz. Podľa Tvrdenia 2.14 pre každé $k \in \mathbb{N}$ existuje primitívny polynóm stupňa k nad $\mathbb{F}_q$. Ním určená rekurencia pri nenulovom počiatočnom stavovom vektore nageneruje hľadanú maximálnu postupnosť. □

4.2 Pseudonáhodný generátor bitov

Keďže to pre nás nebude znamenať prácu navyše, zostrojíme pseudonáhodný generátor, ktorý bude generovať prvky telesa $\mathbb{F}_q$.

Najprv zvolíme $k \in \mathbb{N}$ a nájdeme primitívny polynóm nad $\mathbb{F}_q$ stupňa k: $f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_0 \in \mathbb{F}_q[x]$. Na začiatku generátor inicializujeme nejakými hodnotami $s_0, \ldots, s_{k-1} \in \mathbb{F}_q$. Potom vždy, keď si užívateľ vypýta náhodné číslo, vrátime ďalšie číslo rekurentnej postupnosti $s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n$. Vďaka primitivite polynómu bude táto postupnosť maximálna.

V praxi sa volí $q = 2$, čo vedie na generátor bitov, pretože práca nad telesom $\mathbb{F}_2$ je vďaka bitovým operáciám na procesore rýchla a jednoduchá. Hodnotu

k volíme tak, aby dĺžka periódy $q^k - 1$ presiahla očakávaný počet dotazov na náhodné číslo, pretože ináč by sa postupnosť zacyklila počas behu programu.

Vo zvyšku podkapitoly budeme analyzovať pseudonáhodné vlastnosti takejto postupnosti.

4.2.1 Distribučný a sériový test

Definícia 4.4. Ako n-tý m-vektor budeme nazývať

$$\mathbf{s}_{n,m} = (s_n, \ldots, s_{n+m-1}).$$

Všimnime si, že n-tý stavový vektor $\mathbf{s}_n$ je n-tý k-vektor $\mathbf{s}_{n,k}$, a tiež z periodicity $\mathbf{s}_{n,m} = \mathbf{s}_{n+q^k-1,m}$. V ďalšom texte budeme používať označenie *perióda* ako množinu $q^k - 1$ za sebou idúcich m-vektorov $\mathbf{s}_{0,m}, \ldots, \mathbf{s}_{q^k-2,m}$. Z kontextu bude vždy jasné, o aké m sa jedná.

Nasledujúce triviálne pozorovanie plynúce z definície nám poslúži ako základ pre ďalšie tvrdenia (pozri Tvrdenie 3.17):

Pozorovanie 4.5. *Maximálna rekurentná postupnosť obsahuje v perióde všetky stavové vektory práve raz až na nulový, ktorý neobsahuje.*

Dôsledok 4.6. *Nech $s \in \mathbb{F}_q^\infty$ je maximálna rekurentná postupnosť rádu k, $m \in \mathbb{N}, m \leqslant k$. Potom platí:*

(i) Ľubovoľný nenulový m-vektor sa v perióde vyskytne q^{k-m} krát, nulový jedenkrát menej.

(ii) Nula sa v perióde vyskytne $q^{k-1} - 1$ krát, zvyšné prvky $\mathbb{F}_q$ sa vyskytnú q^{k-1} krát.

(iii) Majme danú nenulovú m-ticu $(a_0, \ldots, a_{m-1}) \in \mathbb{F}_q^m$ a $l \in \mathbb{N}$ také, že $m + l \leqslant k$. Potom pre l-tice $(b_0, \ldots, b_{l-1}) \in \mathbb{F}_q^l$, sa každý z $(m+l)$-vektorov $(a_0, \ldots, a_{m-1}, b_0, \ldots, b_{l-1})$ bude v perióde vyskytovať rovnako veľakrát. Pre nulovú m-ticu platí to isté tvrdenie s obmedzením, že nulová l-tica bude nasledovať jedenkrát menej.

Dôkaz.

(i) Každý nenulový k-vektor sa v perióde vyskytuje $q^k - 1$ krát, takže pre pevne daných prvých m zložiek ho môžeme vždy doplniť na k-vektor q^{k-m} spôsobmi. Tvrdenie o nulovom m-vektore plynie z toho, že nulový k-vektor sa nevyskytuje.

(ii) Plynie z (i) pre $m = 1$.

(iii) Stačí spraviť rovnakú úvahu ako v bode (i): Pre pevne daných prvých m zložiek stavového vektora bude nasledovať daná l-tica práve toľkokrát, koľkokrát dokážeme túto $(m+l)$-ticu doplniť na nenulovú k-ticu. Pre nenulové vektory tento počet závisí podľa (i) iba na $m + l$, a ak je m-tica nulová, tak nulová l-tica bude nasledovať jedenkrát menej.

□

Interpretujme tento dôsledok. Bod (ii) je analógia distribučného testu – pre $\mathbb{F}_2$ je pomer núl a jednotiek v perióde približne 1:1. To, že to nie je úplne presne, nevadí, pretože počas behu programu aj tak nechceme prekročiť periódu postupnosti, takže istá odchýlka je akceptovateľná.

Bod (i) je v podobnom zmysle analógiou sériového testu, avšak tvrdenie platí iba pre m-vektory dĺžky menšej alebo rovnej k.

Napokon bod (iii) hovorí, že za sebou idúce prvky maximálnej postupnosti sú v istom zmysle na sebe nezávislé – po ľubovoľnej m-tici bude s rovnakou pravdepodobnosťou nasledovať ľubovoľná l-tica (samozrejme s obmedzením zo znenia dôsledku).

Majme však na pamäti, že všetky tieto odhady platia pre celú periódu $q^k - 1$ a de facto nehovoria nič o častiach periódy. Dá sa ale tušiť, že aj pre ne budú platiť nejaké odhady. Na tie ale sú potrebné hlbšie vedomosti, ktoré sú nad rámec tejto práce.

4.2.2 Korelačný test

Tvrdenie 4.7. *Nech $s \in \mathbb{F}_q^\infty$ je maximálna postupnosť rádu k. Definujme $u_n = s_n - s_{n+d}$ pre $d \in \mathbb{N}$. Potom ak je d násobok $q^k - 1$, tak je u konštantná. V opačnom prípade je u tiež maximálna postupnosť.*

Dôkaz. Ak je d násobok periódy, tvrdenie je zrejmé. Ináč d určite nie je perióda, takže u je nenulová postupnosť. Navyše u spĺňa tú istú rekurenciu ako s. Podľa Pozorovania 4.5 s niekde v sebe obsahuje počiatočný stavový vektor u, takže u je iba posunutím s a teda je maximálna. □

Vysvetlime si, ako tvrdenie súvisí s korelačným testom. Ak od s_n odčítame posunutú postupnosť s_{n+d}, tak na miestach, kde sa zhodujú, bude 0. Špeciálne pre $\mathbb{F}_2$ bude na zvyšných miestach 1. Za podmienky, že d nie je násobok periódy, je podľa tvrdenia táto rozdielová postupnosť taktiež maximálna. Takže podľa

predošlej podkapitoly bude núl o jednu menej než jednotiek, a teda ich pomer – pomer zhôd a nezhôd – bude v celej perióde približne 1:1.

4.2.3 Decimačný test

Ďalším druhom testu náhodnosti je decimačný test. Je založený na myšlienke, že ak z náhodnej postupnosti vyberieme každý d-tý prvok, mali by sme znovu dostať náhodnú postupnosť.

Tvrdenie 4.8. *Nech s je maximálna postupnosť rádu k a $u_n = s_{h+dn}, h, d \in \mathbb{N}_0$. Potom u je maximálna postupnosť rádu k práve vtedy, keď* $\mathrm{NSD}(d, q^k - 1) = 1$.

Dôkaz. Označme $p = q^k - 1$ a $t_n = s_{h+n}$, potom t je tiež maximálna postupnosť a $u_n = t_{dn}$. Podľa Dôsledku 3.9 vieme t_n explicitne vyjadriť ako

$$t_n = c_0\lambda^n + c_1\lambda^{qn} + \cdots + c_{k-1}\lambda^{q^{k-1}n},$$

kde $\lambda \in \mathbb{F}_{q^k}$ je koreň spoločného charakteristického polynómu s aj t, a teda

$$\begin{aligned} u_n \;=\; t_{dn} \;&=\; c_0(\lambda^d)^n + c_1(\lambda^{qd})^n + \cdots + c_{k-1}(\lambda^{q^{k-1}d})^n \\ &=\; c_0\lambda^{dn} + c_1(\lambda^{dn})^q + \cdots + c_{k-1}(\lambda^{dn})^{q^{k-1}}. \end{aligned}$$

Ak $\mathrm{NSD}(d, p) \neq 1$, tak λ^{dn} z teórie čísel nenageneruje cyklickú multiplikatívnu grupu $\mathbb{F}_{q^k}$. Preto sa u zacyklí skôr než po p členoch, a teda u nebude maximálna postupnosť rádu k.

Ináč je λ^d primitívny prvok $\mathbb{F}_{q^k}$. Označme f príslušný primitívny polynóm, prvky $\lambda^d, \ldots, \lambda^{q^{k-1}d}$ sú podľa Tvrdenia 2.10 jeho korene. Navyše u spĺňa rekurenciu určenú týmto polynómom, pretože je to lineárna kombinácia postupností $(\lambda^{q^i d})^n$ pre $i \in \{0, \ldots, k-1\}$, ktoré túto rekurenciu spĺňajú. Takže podľa Vety 4.2 je u maximálna postupnosť. □

Z dôkazu dokonca plynie, že ak $d = q^i$ ($i \in \{0, \ldots, k-1\}$), tak vybraná podpostupnosť bude spĺňať tú istú rekurenciu ako s. Je to tým, že λ^d je v tomto prípade asociovaný s λ.

Na tomto mieste je vhodné uviesť vetu, ktorá prisudzuje maximálnym postupnostiam význačné postavenie – hovorí, že v danej maximálnej postupnosti sa ako vybraná podpostupnosť dá nájsť ľubovoľná rekurentná postupnosť, ktorá spĺňa iba podmienku pre rád a ireducibilitu minimálneho polynómu. Budeme ju dokazovať pomocou slabšieho tvrdenia s elegantným kombinatorickým dôkazom.

Tvrdenie 4.9. *Nech $s \in \mathbb{F}_q^\infty$ je maximálna postupnosť rádu k a $u \in \mathbb{F}_q^\infty$ lineárna rekurentná postupnosť s ireducibilným minimálnym polynómom f stupňa k. Potom existujú $h, d \in \mathbb{N}_0$ také, že $u_n = s_{h+dn}$.*

Dôkaz. Označme λ koreň charakteristického polynómu s a α koreň f. Z podmienky na jeho stupeň vieme, že $\alpha \in \mathbb{F}_{q^k}$, a teda z primitivity λ existuje $d \in \mathbb{N}_0$ také, že $\lambda^d = \alpha$.

Označme M množinu všetkých k-tic $(c_0, \ldots, c_{k-1})$ takých, že

$$t_n = c_0\lambda^n + \cdots + c_{k-1}\lambda^{q^{k-1}n}$$

je postupnosť prvkov $\mathbb{F}_q$. Vieme, že sú to všetky postupnosti z $\mathbb{F}_q^\infty$, ktoré spĺňajú rekurentný vzťah s. Množina M má q^k prvkov, pretože každej z týchto postupností, ktoré sú určené počiatočným stavovým vektorom, prislúcha práve jedna k-tica $(c_0, \ldots, c_{k-1})$ (pozri Kapitolu 3.2). Navyše všetky tieto postupnosti, okrem nulovej, sú vďaka Pozorovaniu 4.5 len posunuté postupnosti s.

Podobne označme N množinu všetkých k-tic $(c_0, \ldots, c_{k-1})$ takých, že

$$t_n = c_0\alpha^n + \cdots + c_{k-1}\alpha^{q^{k-1}n}$$

je postupnosť prvkov $\mathbb{F}_q$. Z rovnakého dôvodu má táto množina q^k prvkov, navyše sa v nej vyskytuje nenulová k-tica určujúca postupnosť u. Ak by totiž bola nulová, bola by aj postupnosť u nulová a f by nebol stupňa k.

Všimnime si ale, že každá k-tica z M sa musí vyskytovať v N, pretože

$$t_{dn} = c_0\lambda^{dn} + \cdots + c_{k-1}\lambda^{q^{k-1}dn} = c_0\alpha^n + \cdots + c_{k-1}\alpha^{q^{k-1}n}.$$

Porovnaním počtu prvkov zisťujeme, že $M = N$, a teda existuje postupnosť t taká, ktorá je posunutím s a vybraním každého jej d-tého prvku získame postupnosť u. Teda existuje $h \in \mathbb{N}_0$ také, že $u_n = s_{h+dn}$.

□

Lema 4.10. *Nech $f \in \mathbb{F}_q[x]$ je monický ireducibilný polynómom stupňa l deliaceho $k \in \mathbb{N}_0$ a α ľubovoľný jeho koreň. Potom postupnosť*

$$s_n = \alpha^n + \alpha^{qn} + \cdots + \alpha^{q^{k-1}n}$$

je postupnosť z $\mathbb{F}_q^\infty$ spĺňajúca rekurenciu určenú polynómom f.

Dôkaz. Čísla $\alpha^n, \alpha^{qn}, \ldots, \alpha^{q^{l-1}n}$ sú korene f, takže podľa Vietovych vzťahov ich súčet patrí do $\mathbb{F}_q$. Navyše vďaka $\alpha \in \mathbb{F}_{q^l}$ platí $\alpha^{q^l n} = \alpha^n$, a preto za podmienky $l \mid k$ sa v s_n tento súčet celočíselnekrát zopakuje. Teda $s_n \in \mathbb{F}_q$. To, že s spĺňa rekurenciu určenú f, je zrejmé. □

Veta 4.11. *Nech $s \in \mathbb{F}_q^\infty$ je maximálna postupnosť rádu k a $u \in \mathbb{F}_q^\infty$ lineárna rekurentná postupnosť, ktorá má ireducibilný minimálny polynóm f stupňa l deliaceho k. Potom existujú $h, d \in \mathbb{N}_0$ také, že $u_n = s_{h+dn}$.*

Dôkaz. Ukážeme, že existuje vybraná postupnosť $t_n = s_{h+dn}$, ktorá je maximálna rádu l. Potom podľa predošlého tvrdenia budeme z nej vedieť vybrať u, čím bude dôkaz hotový.

Označme λ koreň charakteristického polynómu s a zvoľme $\alpha \in \mathbb{F}_{q^k}$ primitívny prvok multiplikatívnej grupy podtelesa $\mathbb{F}_{q^l}$. Z predošlej lemy a z Pozorovania 4.5 vieme, že existuje $h \in \mathbb{N}_0$ také, že

$$s_{h+n} = \lambda^n + \lambda^{qn} + \cdots + \lambda^{q^{k-1}n}.$$

Teda pre $d \in \mathbb{N}_0$ také, že $\lambda^d = \alpha$, platí

$$t_n = s_{h+dn} = \alpha^n + \alpha^{qn} + \cdots + \alpha^{q^{k-1}n}.$$

Minimálny polynóm α je primitívny stupňa l. Postupnosť t spĺňa ním určenú rekurenciu a navyše je vďaka nenulovým koeficientom nenulová, takže je maximálna rádu l. □

Poznámka. Táto veta sa dá dokázať aj jednoduchším spôsobom, a síce za použitia tzv. *stopy* prvku. Tento pojem však my nezavádzame, dôkaz sa dá nájsť v knihe Lidla a Niederreitera [1] (str. 291).

4.2.4 Riešené cvičenia

Na tomto mieste uvedieme riešenia vybraných cvičení z knihy *Introduction to finite fields and their applications* od Lidla a Niederreitera [1]. Sú to cvičenia týkajúce sa kapitoly 7.4.

Cvičenie 7.34. Nech s je maximálna rekurentná postupnosť rádu k nad $\mathbb{F}_q$. Potom medzi jej ľubovoľnými $(q^k-1)/(q-1)$ za sebou idúcimi členmi je $(q^{k-1}-1)/(q-1)$ nulových.

Riešenie. V perióde dĺžky $q^k - 1$ je podľa Dôsledku 4.6 presne $q^{k-1} - 1$ núl. Podľa zadania máme dokázať, že v $(q-1)$-tine periódy bude práve $(q-1)$-tina z nich.

Označme $r = (q^k - 1)/(q - 1)$. Pomocou koreňa $\lambda \in \mathbb{F}_{q^k}$ charakteristického polynómu vieme explicitne vyjadriť

$$\begin{aligned} s_n &= c_0\lambda^n + c_1\lambda^{qn} + \cdots + c_{k-1}\lambda^{q^{k-1}n}, \\ s_{n+r} &= c_0\lambda^n\lambda^r + c_1\lambda^{qn}\lambda^{qr} + \cdots + c_{k-1}\lambda^{q^{k-1}n}\lambda^{q^{k-1}r}. \end{aligned}$$

Vďaka primitivite λ má prvok λ^r zrejme rád $q-1$, takže $\lambda^r = \lambda^{qr} = \cdots = \lambda^{q^{k-1}r}$ a môžeme upraviť

$$s_{n+r} = \lambda^r(c_0\lambda^n + c_1\lambda^{qn} + \cdots + c_{k-1}\lambda^{q^{k-1}n}) = \lambda^r s_n.$$

To znamená, že $s_n = 0$ práve vtedy, keď $s_{n+r} = 0$, a teda každý r-vektor $\mathbf{s}_{n,r}$ obsahuje rovnako veľa núl, ako ten nasledujúci $\mathbf{s}_{n+r,r}$. V perióde je presne $q-1$ za sebou idúcich r-vektorov. Každý z nich preto musí obsahovať $(q^{k-1}-1)/(q-1)$ núl. □

Cvičenie 7.36. Nech s je lineárna rekurentná postupnosť nad $\mathbb{F}_q$ s minimálnou periódou p. Pre dané $c \in \mathbb{F}_q$ povieme, že sa vyskytol *úsek* c dĺžky $m \in \mathbb{N}$, ak $s_n \neq c, s_{n+i} = c$ pre $i \in \{1, \ldots, m\}$ a $s_{n+m+1} \neq c$ pre nejaké $0 \leqslant n < p$.

Dokážte, že ak je s maximálna postupnosť rádu $k > 1$, vyskytujú sa len nasledovné úseky:

- Pre $1 \leqslant m \leqslant k-2$ a ľubovoľné $c \in \mathbb{F}_q$ sa vyskytne $(q-1)^2 q^{k-m-2}$ úsekov c dĺžky m,
- úsek c dĺžky $k-1$ sa pre $c \neq 0$ vyskytne $(q-2)$-krát, pre $c = 0$ jedenkrát viac,
- úsek c dĺžky k sa pre $c \neq 0$ vyskytne raz, pre $c = 0$ ani raz a úseky väčšej dĺžky sa nevyskytnú.

Riešenie. Využijeme Pozorovanie 4.5 ktoré hovorí, že každý stavový vektor sa vyskytuje v perióde práve raz okrem nulového, ktorý sa nevyskytuje.

- Na pozícii n sa vyskytne úsek c dĺžky $m < k-2$ práve vtedy, keď prvá zložka stavového vektora $\mathbf{s}_n$ je rôzna od c, na čo máme $q-1$ možností; ďalších m zložiek je jednoznačne určených; $(n+m+1)$-tá zložka je znovu rôzna od c, na čo máme znovu $q-1$ možností a zvyšných $k-m-2$ zložiek vieme doplniť q^{k-m-2} spôsobmi.
- Aby nastal úsek c dĺžky $k-1$, musí byť prvá zložka patričného stavového vektora rôzna od c, na čo máme $q-1$ možností, a zvyšné zložky musia byť rovné c. Ak by ďalší člen postupnosti bol tiež c, nasledujúci stavový vektor by bol $(c, c, \ldots, c)$. Ten sa vyskytne pre $c \neq 0$ práve raz, ináč bude ďalší člen rôzny od c a nastane úsek dĺžky $k-1$.

- Úsek c dĺžky $m > k$ sa nevyskytne, pretože potom by dva za sebou idúce stavové vektory museli byť rovnaké, čo je spor. Úsek dĺžky k preto nastane práve vtedy, keď je príslušný stavový vektor rovný $(c, c, \ldots, c)$. To nastane pre $c \neq 0$ raz a pre $c = 0$ ani raz.

□

Cvičenie 7.38. Dokážte nasledujúci opak Vety 4.11: Každá vybraná postupnosť $u_n = s_{h+dn}, h, d \in \mathbb{N}_0$ z maximálnej postupnosti $s \in \mathbb{F}_q^\infty$ rádu k je buď nulová postupnosť alebo postupnosť s ireducibilným minimálnym polynómom stupňa deliaceho k.

Riešenie. Používajúc značenie z Tvrdenia 4.8 vieme, že

$$\begin{aligned} u_n &= c_0(\lambda^d)^n + c_1(\lambda^{qd})^n + \cdots + c_{k-1}(\lambda^{q^{k-1}d})^n \\ &= c_0\alpha^n + c_1(\alpha^q)^n + \cdots + c_{k-1}(\alpha^{q^{k-1}})^n, \end{aligned}$$

kde λ je koreň charakteristického polynómu s a $\alpha = \lambda^d$. Označme f minimálny polynóm α nad $\mathbb{F}_q$ v algebraickom zmysle. Potom je ireducibilný a aj $\alpha^q, \ldots, \alpha^{q^{k-1}}$ sú jeho korene, pretože sú s α asociované. Navyše jeho stupeň delí k, pretože jeho korene ležia v rozšírení $\mathbb{F}_{q^k}$.

Postupnosť u spĺňa rekurenciu určenú týmto polynómom, pretože ju spĺňajú postupnosti $\alpha^{qn}, \ldots, \alpha^{q^{k-1}n}$, ktorých je lineárnou kombináciou. Preto ak je postupnosť u nenulová, z ireducibility musí byť f jej minimálnym polynómom. □

Cvičenie 7.39. Nech s je maximálna rekurentná postupnosť rádu k nad $\mathbb{F}_q$. Dokážte, že každá maximálna rekurentná postupnosť t rádu k nad $\mathbb{F}_q$ je len posunutou postupnosťou $u_n = s_{dn}$ pre vhodné $d \in \mathbb{N}_0$.

Riešenie. Z Vety 4.11 vieme, že existujú $h, d \in \mathbb{N}_0$ také, že $t_n = s_{h+dn}$. Rozpísaním explicitného vzorca pre postupnosť s zisťujeme, že postupnosti $u_n = s_{dn}$ a s_{h+dn} sú lineárnou kombináciou postupností spĺňajúcich ten istý rekurentný vzťah, a teda u spĺňa ten istý vzťah ako t. Navyše podľa Tvrdenia 4.8 je d nesúdeliteľné s periódou, takže u je nenulová a teda aj maximálna postupnosť. Napokon z Pozorovania 4.5 je t len posunutou postupnosťou u.

□

Cvičenie 7.40. Nech s je nenulová lineárna rekurentná postupnosť nad $\mathbb{F}_2$ s minimálnou periódou p. Pre $h \in \mathbb{N}_0$ označme $s^{(h)}$ posunutú postupnosť $s_n^{(h)} = s_{n+h}$. Dokážte, že ak pre každé $h \in \{1, \ldots, p-1\}$ je $s + s^{(h)}$ iba posunutá postupnosť s, potom s musí byť maximálna postupnosť.

Riešenie. Nech s spĺňa minimálnu rekurenciu rádu k. Potom je s maximálna práve vtedy, keď v perióde obsahuje každý stavový vektor až na nulový.

Dokážem, že stavové vektory v perióde spolu s nulovým vektorom tvoria lineárny priestor nad $\mathbb{F}_2$. Podmienka na násobenie skalárom je triviálne splnená. Majme teda dva vektory z periódy $\mathbf{s}_i$ a $\mathbf{s}_j$. Ak sú rovnaké, ich súčet je nulový vektor. Ináč vieme, že $s + s^{(j-i)} = s^{(m)}$ pre nejaké $m \in \mathbb{N}_0$, takže špeciálne i-té stavové vektory postupností na oboch stranách sa rovnajú, t.j.

$$\mathbf{s}_i + \mathbf{s}_j = \mathbf{s}_{m+i}.$$

Teda množina je uzavretá aj na sčítanie a tvorí lineárny priestor.

Na dokončenie dôkazu si stačí uvedomiť, že podľa Lemy 3.20 je prvých k stavových vektorov lineárne nezávislých. Potom spomínaný lineárny priestor obsahuje 2^k vektorov, takže okrem nulového je v perióde všetkých $2^k - 1$. □

Cvičenie 7.41. Dokážte, že pre ľubovoľnú maximálnu rekurentnú postupnosť nad $\mathbb{F}_q$ existuje jej posunutá verzia s taká, že $s_n = s_{qn}$.

Riešenie. Na základe Pozorovania 4.5 môžeme zadanie preformulovať tak, že pre rekurenciu pôvodnej postupnosti rádu k hľadáme nenulovú postupnosť s spĺňajúcu $s_n = s_{qn}$. Označme λ koreň príslušného primitívneho polynómu. Má platiť

$$\begin{aligned} s_n - s_{qn} &= c_0\lambda^n + c_1\lambda^{qn} + \cdots + c_{k-1}\lambda^{q^{k-1}n} - (c_0\lambda^{qn} + c_1\lambda^{q^2n} + \cdots + c_{k-1}\lambda^n) \\ &= (c_0 - c_{k-1})\lambda^n + (c_1 - c_0)\lambda^{qn} + \cdots + (c_{k-1} - c_{k-2})\lambda^{q^{k-1}n} \quad = \quad 0. \end{aligned}$$

Postačujúcou podmienkou je, aby všetky koeficienty c_i boli rovnaké a nenulové. To sa dá podľa Lemy 4.10 dosiahnuť napríklad voľbou $c_0 = \cdots = c_{k-1} = 1$. □

4.3 Pseudonáhodný generátor celých a reálnych čísel

V predchádzajúcej podkapitole sme si predstavili generátor náhodných bitov, ale v praxi málokedy treba vygenerovať náhodný bit. Väčšinou je potrebné náhodné číslo v nejakom rozsahu.

Základným východiskovým bodom je funkcia, ktorá vracia pseudonáhodné nezáporné celé číslo z rozsahu premennej. Dočasne označme maximálnu hodnotu, ktorá sa dá uložiť do takejto premennej, ako `max_int`.

Jeden zo spôsobov, ako túto funkciu implementovať, by bolo zvoliť prvočíslo $p > \texttt{max\_int}$ a generovať maximálnu rekurentnú postupnosť nad telesom $\mathbb{Z}_p$, pričom hodnoty, ktoré sa do premennej nezmestia, by sme zahadzovali. Tento spôsob sa v praxi nepoužíva, pretože okrem zahadzovania by sme museli implementovať aritmetiku v $\mathbb{Z}_p$ a generovanú postupnosť si pamätať v premenných väčšieho rozsahu, než aký generujeme.

Druhý, používaný spôsob, využíva generátor pseudonáhodných bitov z predošlej podkapitoly. V prípade, keď chceme náhodnú hodnotu m-bitovej premennej, jednoducho vygenerujeme m bitov a premennú nimi naplníme. Formálne môžeme postupnosť takýchto čísel charakterizovať ako m-vektory $\mathbf{s}_{nm,m}$, pričom každý m-vektor interpretujeme ako číslo v binárnom zápise.[4]

Tvrdenie 4.12. *Nech $s \in \mathbb{F}_q^\infty$ je maximálna postupnosť minimálnej periódy p. Potom postupnosť $\mathbf{u}$ definovaná $\mathbf{u}_n = \mathbf{s}_{nm,m}$ má minimálnu periódu $p/\mathrm{NSD}(m,p)$.*

Dôkaz. Z teórie čísel vieme, že $(nm \bmod p)$ má periódu $p/\mathrm{NSD}(m,p)$, takže aj $\mathbf{u}$ bude mať takú periódu a zostáva ukázať, že to je minimálna perióda.

Predpokladajme, že $\mathbf{u}$ má periódu $r \in \mathbb{N}$. Potom s má periódu rm, pretože $\mathbf{s}_{nm,m} = \mathbf{u}_n = \mathbf{u}_{n+r} = \mathbf{s}_{nm+rm,m}$ pre každé $n \in \mathbb{N}_0$. Lenže p je minimálna perióda s, takže

$$p \mid mr \quad \Rightarrow \quad \frac{p}{\mathrm{NSD}(m,p)} \mid r \quad \Rightarrow \quad \frac{p}{\mathrm{NSD}(m,p)} \leqslant r.$$

□

Určite chceme, aby náš generátor mohol vygenerovať každé číslo, preto budeme voliť rád rekurencie k väčší alebo rovný m – z Pozorovania 4.5 totiž vieme, že všetky možné nenulové k-vektory sa v perióde vyskytujú. Navyše podľa posledného tvrdenia je vhodná voľba taká, aby $\mathrm{NSD}(m, q^k - 1) = 1$, pretože potom postupnosť $\mathbf{u}$ bude nadobúdať všetky m-vektory z periódy.

Týmto spôsobom teda získame generátor náhodného m-bitového čísla. Pre $max \leqslant \texttt{max\_int}$ z neho potom vieme ľahko dostať ľubovoľné číslo v rozsahu $[0, max)$ tak, že vygenerované číslo vymodulíme max. Tento spôsob je však chybný – ak napríklad zvolíme $max = 3/4 \cdot \texttt{max\_int}$, potom čísla z intervalu $[0, \texttt{max\_int}/4)$ majú dvakrát väčšiu pravdepodobnosť vygenerovania. Táto chyba sa však ľahko napraví tak, že pred modulením budeme čísla väčšie alebo rovnaké ako najväčší násobok max, ktorý sa zmestí do premennej, zahadzovať.

[4] Laicky povedané, vezmeme náhodnú postupnosť 0 a 1, rozsekáme ju na úseky dĺžky m a každý úsek chápeme ako číslo v dvojkovej sústave.

Ľubovoľné celé číslo v rozsahu $[min, max)$ napokon dostaneme tak, že vygenerujeme náhodné celé číslo v rozsahu $[0, max - min)$ a pričítame min.

Zostáva vysvetliť spôsob, akým generovať reálne čísla. Tie sa generujú typicky v intervale $[0, 1]$, pretože ľubovoľný iný (uzavretý) interval dokážeme z neho dostať prenásobením a pričítaním. Náhodné číslo v spomenutom intervale vieme jednoducho vygenerovať tak, že vygenerujeme náhodné celé číslo v intervale $[0, \texttt{max\_int}]$ a predelíme ho `max_int`.

Niekto by mohol namietať, že takto nagenerujeme iba niektoré diskrétne hodnoty z intervalu $[0, 1]$. Treba si však uvedomiť, že v počítači neexistuje nekonečná presnosť, preto ani iná možnosť, než generovať „iba“ diskrétne hodnoty, nie je.

Kapitola 5

Záver

Ako sme už spomenuli v úvode práce, cieľom nášho snaženia bolo vytvoriť pseudonáhodný generátor čísel. Ten, na základe celej Kapitoly 4, je uvedený v Prílohe A ako program v jazyku C++.

Ešte raz pripomeňme, že sme si počas výkladu dovolili vynechať niektoré zložitejšie tvrdenia týkajúce sa odhadov na výskyt prvkov maximálnej postupnosti v častiach jej periódy. Táto medzera sa dá doplniť štúdiom knihy Lidla a Niederreitera [1], konkrétne kapitoly 6.7.

Na záver uveďme, nakoľko sa náhodné generátory založené na lineárnych rekurentných postupnostiach nad $\mathbb{F}_2$ používajú v praxi. V prvom rade, tieto náhodné generátory nie sú vhodné pre kryptografické účely, pretože odpozorovaním pár vygenerovaných hodnôt dokážeme predpovedať celú postupnosť.[1]

Na druhú stranu, pre aplikácie, kde toto nie je problém, sa takéto generátory naozaj používajú. Asi najznámejším z nich je tzv. Mersenne Twister predstavený v roku 1998 Japoncami Matsumoto a Nishimura, ktorý má neuveriteľne veľkú periódu $2^{19937} - 1$ ([5]). V súčasnosti je podľa [6] tento algoritmus implementovaný ako základný pseudonáhodný generátor v programoch R, Maple, MATLAB, Gretl, ako aj v skriptovacích jazykoch Python a Ruby.

[1] Presnejšie: ak poznáme rekurentný vzťah, stačí nám toľko hodnôt, aký je jeho rád. Ak ho nepoznáme, so znalosťou dvojnásobku hodnôt ho dokážeme pomocou Gaussovej eliminačnej metódy určiť.

Dodatok A

Prílohy

Aplikáciou teórie v práci je nasledujúci program. Generuje lineárnu rekurentnú postupnosť rádu 64 nad $\mathbb{F}_2$ určenú primitívnym polynómom

$$x^{64} + x^{61} + x^{34} + x^9 + 1.$$

Má periódu $2^{64} - 1 \approx 1.84 \times 10^{19}$.

Stavový vektor sa ukladá do 64-bitovej premennej. Ľubovoľné 64-bitové číslo s výnimkou nuly teda slúži ako iniciačná hodnota, v prípade nuly sa generátor inicializuje aktuálnym časom.

A.1 C++ program

```
#include <ctime>
#include <iostream>
using namespace std;

/*
    Generates stream of pseudorandom bits using maximal period
    linear recurring sequence of degree 64.
*/
class RandomNumberGenerator64
{
private:
    unsigned long long statevector;

public:
    // seed 0 (or unspecified) initializes with current time
    RandomNumberGenerator64(unsigned long long seed = 0) {
        if (seed == 0) statevector = time(NULL);
        else statevector = seed;
    }

```

```
21      unsigned long long NextBits(int cnt) {
22          unsigned long long nextbit, res = 0;
23          for (int i = 0; i < cnt; i++) {
24              // primitive polynomial x^64 + x^61 + x^34 + x^9 + 1
25              nextbit = ((statevector >> 61)&1)
26                  ^ ((statevector >> 34)&1)
27                  ^ ((statevector >> 9)&1)
28                  ^ (statevector & 1);
29              statevector = ((statevector >> 1) | (nextbit << 63));
30              res |= nextbit << i;
31          }
32          return res;
33      }
34
35      int NextInt() {
36          return (int)NextBits(31);
37      }
38
39      int NextInt(int upperbound) {
40          int i, bound = (0x7fffffff/upperbound)*upperbound;
41          do {
42              i = NextInt();
43          } while (i >= bound);
44          return i % upperbound;
45      }
46
47      double NextDouble() {
48          return (double) (NextBits(64)-1) / (double) 0xfffffffffffffffeULL;
49      }
50  };
51
52  int main()
53  {
54      RandomNumberGenerator64 r;
55
56      cout << "Random bit: " << r.NextBits(1) << endl;
57      cout << "Random nonnegative 32bit integer: " << r.NextInt() << endl;
58      cout << "Random real in [0,1]: " << r.NextDouble() << endl;
59      cout << "Random die roll: " << r.NextInt(6)+1 << endl;
60  }
```

Literatúra

[1] Rudolf Lidl, Harald Niederreiter: *Introduction to finite fields and their applications – Revised edition*, Cambridge University Press 1984, 1994. Kap. 6, 7.4.

[2] Libor Barto, Jiří Tůma: *Konečná tělesa*, `http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf` (17.7.2010)

[3] Dan Kalman: *The Generalized Vandermonde Matrix*, Mathematics Magazine, Vol. 57, No. 1 (Jan. 1984), pp. 15-21
`http://www.jstor.org/stable/2690290` (17.7.2010)

[4] Mads Haahr: *Introduction to Randomness and Random Numbers*,
`http://www.random.org/randomness/` (17.7.2010)

[5] Makoto Matsumoto, Takuji Nishimura: *Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator*, ACM Transactions on Modeling and Computer Simulation, Vol. 8, No. 1, (Jan. 1998), pp. 3–30

[6] *Mersenne Twister*,
`http://en.wikipedia.org/wiki/Mersenne_twister` (17.7.2010)