ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

HLEDÁNÍ CELOČÍSELNÝCH ZÁVISLOSTÍ MEZI REÁLNÝMI ČÍSLY

BAKALÁŘSKÁ PRÁCE

Pavla Filipovičová

Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

Plzeň, 2016

Prohlašuji, že jsem diplomovou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 1. června 2016

.....

vlastnoruční podpis

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu mé bakalářské práce,
doc. RNDr. Jaroslavu Horovi, CSc., za věcné připomínky a čas, který mi věnoval.

Místo tohoto listu bude originální zadání bakalářské práce.

1 OBSAH

ÚVOD

Cílem mé práce bude se seznámit s velkými osobnostmi matematiky, jakými byli Srinivasa Aaiyagnar Ramanujan, Jörgen Gram a Erhard Schmidt. Seznámit se s jejich prací a objevy.

Hlavním cílem bude čtenáře seznámit s dvěma algoritmy, které se využívají pro hledání celočíselných závislostí mezi reálnými čísly. Těmi jsou Gramův-Schmidtův ortogonalizační proces, který je používaný právě i v LLL algoritmu.

Je to téma, o kterém se obecně málo ví, protože je to vcelku nový objev. Zajímavé také je to, že se Gramův-Schmidtův ortogonalizační proces jmenuje právě po těchto dvou matematicích, protože s touto metodou přišel jako první Laplace. Takzvaný LLL algoritmus je pojmenovaný po svých objevitelích Lenstrovy, Lenstrovy a Lovászovy, kteří ho publikovali až v roce 1982, je to tedy teprve 34 let staré téma.

Po vysvětlení každého z algoritmů bych poté ráda udělala několik příkladů, ve kterých uvidíme, jak fungují. A nějaký si ověříme v počítačovém programu.

Pro znalost těchto algoritmů bude potřeba se seznámit s některými pojmy z lineární algebry, kterým budu věnovat poměrně velkou část práce.

Na závěr práce bych se ráda věnovala hledání celočíselných závislostí mezi reálnými čísly, pro něž je právě LLL algoritmus důležitý. Ale není jediný. Na hledání celočíselných závislostí existují různé algoritmy. Těmi nejznámějšími jsou například HJLS, který je poměrně mladý, publikován byl až v roce 1992 a v roce 1999 byl ještě zdokonalen. A dalším je například PSOS algoritmus. Více jich zmiňovat nebudu, protože je v práci nebudu blíže rozebírat.

1. PRVNÍ KAPITOLA: SRINIVASA AAIYAGNAR RAMANUJAN

1.1 ŽIVOTNÍ OSUDY

Velmi nadaný indický matematik, narozený 22. prosince 1887, byl jedním z nejgeniálnějších matematiků své doby. Na základní školu nastoupil, když mu bylo necelých pět let. Na střední školu nastoupil v lednu roku 1898, tedy když mu bylo necelých jedenáct let. Malý Ramanujan měl dobré výsledky ve všech předmětech, nejvíce ho ale bavila matematika.

V roce 1900 se začal sám zabývat problematikou aritmetických a geometrických řad. O další dva roky později se naučil řešit kubické rovnice, což ho tak bavilo, že chtěl najít svoji vlastní metodu jak řešit rovnice čtvrtého řádu, tedy kvartické rovnice. Následující rok se snažil najít řešení rovnic pátého řádu, to se mu nepodařilo.

Na střední škole studoval matematiku hlouběji samostudiem. V roce 1904 se hlouběji zabýval řadou $\sum \frac{1}{n}$ a vypočítal Eulerovu konstantu na patnáct desetinných míst.

Na základě dobrých studijních výsledků získal stipendium na univerzitu, na kterou nastoupil v roce 1904. Ovšem kvůli tomu, že se Ramanujan věnoval jen matematice a ostatní předměty zanedbával, další rok mu bylo stipendium odebráno. Uspět na vysoké škole se pokoušel ještě jednou, ale opět neúspěšně.

Pokračoval tedy v jeho matematických pracích, ve kterých studoval např. řetězové zlomky a divergentní řady. Poté naneštěstí na rok onemocněl a podstoupil i operaci. V roce 1909 se oženil s desetiletou dívkou, se kterou žil až o dva roky později.

Navzdory tomu, že neměl vysokoškolské vzdělání, byl Ramanujan dobře znám univerzitním matematikům v Madrasu, především pro jeho excelentní práce pro časopis Indická matematická společnost, kde odvodil vztahy mezi eliptickými modulárními rovnicemi. Dále pak v tomto časopise zveřejnil brilantní výzkum o Bernoulliho číslech. Na doporučení byl roku 1912 jmenován do funkce úředníka, kde potkal mnoho vlivných lidí. Například S. N. Aiyar publikoval svůj článek, který se zabýval rozložením prvočísel, v Ramanujanově práci. Profesor stavebního inženýrství na Univerzitě v Madrasu, C. L. T. Griffith si také všiml Ramanujanových výjimečných schopností, napsal dopis profesoru matematiky M. J. M. Hillovi o Ramanujanově práci na téma Bernoullieho čísel.

Hill odpověděl brzy, ale nepodařilo se mu pochopit výsledky divergentních řad, ke kterým S. Ramanujan dospěl. Ramanujan se nevzdal a poslal další dopis a to profesoru matematiky Hardymu. Ten už zájem o výsledky projevil, ale pár výsledků potřeboval doložit a objasnit. Tato odpověď Ramanujana velice potěšila a požádal Hardyho o pomoc při získání stipendia na Univerzitu v Madrasu. Stipendium poté opravdu získal, a to na dobu dvou let. Díky spolupráci s Hardym Ramanujan vystudoval Cambridge´s Bachelor of Science Research a získal tak titul Ph.D. Roku 1917 vážně onemocněl a jeho lékaři se obávali, že zemře.

Dne 18. února 1918 by Ramanujan zvolen kolegy do seznamu stipendistů na Royal Society of London, a to byla veliká čest. Dostal několik vyznamenání a zdálo se, že se jeho zdraví trochu zlepšuje. Roku 1919 se vrací zpět do Indie a náhle se jeho zdravotní stav zhoršil. I přes všechna lékařská ošetření následujícího roku bohužel umírá, a to přesně 26. dubna 1920 v pouhých 32 letech.

obr. 1: Srinivasa Aaiyagnar Ramanujan

1.2 RAMANUJANOVY VÝSLEDKY

1.2.1 JEHO ŘADY KONVERGUJÍCÍ K PŘEVRÁCENÉ HODNOTĚ ČÍSLA π

Tento geniální matematik, Srinivasa Ramanujan, objevil několik nekonečných řad konvergujících k hodnotě $\frac{1}{\pi}$. Jeho poznámky, týkajících se těchto řad, byly napsány

ještě v Indii, do Anglie si je vzal s sebou a dále je rozvíjel. Jednou z těchto řad je řada:

$$\frac{\sqrt{8}}{9801}\sum_{n=0}\frac{(4n)!}{(n!)^4}\cdot\frac{(1103+26390n)}{396^{4n}}=\frac{1}{\pi}$$

Na Ramanujanových řadách je zajímavá hlavně rychlost konvergence k $\frac{1}{\pi}$. Další ukázky řad konvergujících k této hodnotě jsou například:

$$\sum_{n=0}\frac{((2n)!)^3(42n+5)}{(n!)^6 16^{3n+1}}=\frac{1}{\pi}$$

$$\frac{1}{4}\sum_{n=0}\frac{(1)^n(4n)!(21460n+1123)}{(n!)^4 441^{2n+1}2^{10n+1}}=\frac{1}{\pi}$$

Dalším matematicky krásným vztahem, který Ramanujan vymyslel je vztah, který propojuje dvě důležité konstanty π a e:

$$\frac{1}{1+\dfrac{e^{-2\pi}}{1+\dfrac{e^{-4\pi}}{1+\dots}}}=\left(\sqrt{\frac{5+\sqrt{5}}{2}}-\frac{\sqrt{5}+1}{2}\right)e^{\frac{2}{5}\pi}$$

Ramanujan byl konstantami π a e okouzlen. Dalším tématem, kterým se Ramanujan zabýval, i když to o něm není tolik známé, je zlatý řez.

2 DRUHÁ KAPITOLA: GRAM – SCHMIDTŮV ORTOGONALIZAČNÍ PROCES

2.1 JÖRGEN GRAM

Narodil se 27. června 1850 v Dánsku. Po ukončení základního vzdělání nastoupil na střední školu, tu v roce 1868 dokončil a nastoupil na univerzitu. V roce 1873 Gram získal magisterský titul v matematice. Gram publikoval svou první práci ještě před tím, než absolvoval. Jednalo se o práci o moderní algebře a v roce 1874 ji publikoval ve větším vydání ve francouzštině.

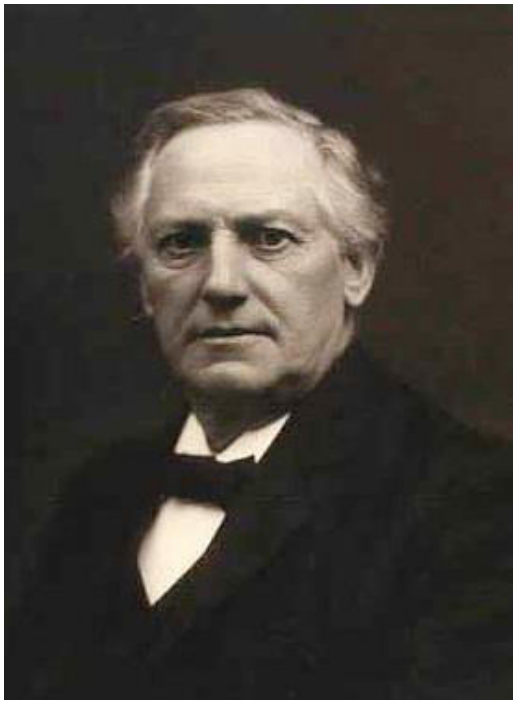
Roku 1875 získal svoje první zaměstnání jako asistent v pojišťovně Hafnia. V té době pracoval na matematickém modelu hospodaření v lesích. Jeho kariéra se vyvíjela dobře a brzy byl povýšen. Jeho práce pro pojišťovnu ho přivedla zpátky do matematického výzkumu. Pracoval na pravděpodobnosti a numerické analýze, protože tato dvě témata využíval denně prakticky i v zaměstnání. O těchto tématech dokonce i vydal knihu a díky ní mu byla udělena hodnost doktora věd roku 1879. Gram později tuto práci vydával v Journal für Mathematik a zásadně přispěla v rozvoji teorie integrálních rovnic. Dále zveřejnil druhý ze svých čtyř dokumentů v oblasti lesnictví. Jelikož tato práce byla psána v dánštině a nebyla nikdy otisknuta v jiných zemích, tak Gram nikdy nezískal mezinárodní uznání pro tuto práci, které si zasloužil. Němečtí výzkumníci, kteří Gramův výzkum neznali, publikovali práci týkající se stejných problémů. Jejich práci nebyla tak uspokojivá jako ta Gramova, ale i přes to získali právě ono mezinárodní uznání tito Němečtí výzkumníci. V letech 1883 a 1889 vydal další dva díly dokumentu o lesnictví.

Gramova práce na pravděpodobnost a numerickou analýzu ho dále vedla studovat abstraktní problémy v teorii čísel. V roce 1884 získal zlatou medaili Královské dánské akademie věd pro svou práci Výzkumy počtu prvočísla menší než dané číslo, kterou publikoval v časopise Společnost.

Ačkoli pokračoval v práci pro Hafnia pojišťovnu ve vysoké pozici, založil si vlastní pojišťovací společnost, Skjold pojišťovnu. Byl i jejím ředitelem a jednatelem od roku 1895 až do roku 1910. Díky jeho zaměstnání byl předsedou pojištění Dánské rady. Gram často přednášel v Dánské matematické společnosti a ovlivnil tak pozitivním způsobem příští generaci dánských matematiků. Navzdory tomu, že byl v podstatě amatérským matematikem, obdržel vyznamenání za jeho matematické příspěvky.

V roce 1888 byl poctěn s volbami do Společnosti. Často se účastnil zasedání Společnosti a publikoval v časopisech Bratrstva. Po mnoho let byl pokladníkem Dánské akademie.

Ovšem nejvíce se ho pamatujeme díky Gramově – Schmidtově ortogonalizačnímu procesu. Zemřel kvůli podivné a smutné nehodě. Stalo se tak 29. dubna 1916 v jeho 65 letech při cestě na setkání Dánské akademie, když ho srazil cyklista.



obr. 2: Jörgen Gram

2.2 ERHARD SCHMIDT

Narodil se 13. ledna 1876 v Estonsku. Navštěvoval místní univerzitu v Dorpatu před odchodem do Berlína, kde potom studoval. Doktorát získal na Univerzitě v Göttingenu roku 1905. Disertační práci psal na téma integrálních rovnic. Po získání doktorátu šel do Bonnu, kde byla oceněna jeho habilitační práce v roce 1906. V roce 1908 vydal důležitou práci na nekonečně mnoho rovnic o nekonečně mnoho neznámých. Po odchodu z Bonnu Schmidt získával různé pozice v Curychu, Erlangenu a ve Vratislavi, než byl jmenován profesorem na Univerzitě v Berlíně roku 1917. Když Schmidt dorazil do Berlína, snažil se o založení institutu aplikované matematiky, který univerzitě chyběl. Poté, co institut byl zřízen, Schmidt musel naplnit post ředitele Institutu aplikované matematiky. Jeho schopnosti byly uznány i mimo matematiku,

jelikož byl jmenován děkanem v akademickém roce 1921/1922 a vicekancléřem Univerzity v Berlíně v letech 1929-1930.

Třicátá léta byla pro Schmidta velice těžká. S nástupem nacistů k moci v roce 1933 byl život čím dál obtížnější pro Schmidtovy židovské kolegy, kteří byly nuceni opustit své posty.

V roce 1936, kdy problémy byly velmi obtížné, Schmidt se stal vedoucím německé delegace na mezinárodním kongresu matematiků, která se konala v Oslu. Schmidt zastával pozici autority na Univerzitě v Berlíně, a proto musel během těchto těžkých let prosadit rezoluce proti Židům, ale jeden z Bieberbachových asistentů prohlásil: „Myslím, že Schmidt vůbec nepochopil židovskou otázku."

Po skončení druhé světové války byl Schmidt jmenován ředitelem matematiky Výzkumného ústavu Německé akademie věd. V této funkci zůstal až do roku 1958, pak odešel do důchodu.

V jednom ze svých článků publikoval to, čemu se dnes říká Gram – Schmidtův ortogonalizační proces. **Měli bychom si však uvědomit, že Laplace tento proces představil ještě před Gramem a Schmidtem.**

Schmidt zemřel 16. prosince 1959 v Berlíně, bylo mu 83 let.

obr. 3: Erhard Schmidt

2.3 GRAMŮV – SCHMIDTŮV ORTOGONALIZAČNÍ PROCES

Nejprve si připomeneme pojmy jako skalární součin, vektorový prostor se skalárním součinem, ortogonální bázi a bázi ortonormální a další pojmy z lineární algebry.

2.3.1 VEKTOROVÉ PROSTORY SE SKALÁRNÍM SOUČINEM

Prvky $\mathbb{R}^n$, tj. vektory vektorového prostoru $\mathbb{R}^n$, budeme psát sloupcově. Matici se sloupci $\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_k \in \mathbb{R}^n$ budeme psát jako $\left(\vec{b}_1\middle|\vec{b}_2\middle|\ldots\middle|\vec{b}_k\right)$. Lineární obal vektorů $\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_k$ budeme značit $\left\langle\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_k\right\rangle$.

Máme-li báze $B=\left(\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_n\right)$ a $C=\left(\vec{c}_1,\vec{c}_2,\ldots,\vec{c}_n\right)$ prostoru $\mathbb{R}^n$, pak maticí přechodu od báze *B* k bázi *C* rozumíme (jednoznačně určenou) matici *X*, pro kterou $\bar{C}=\bar{B}X$, kde $\bar{B}=\left(\vec{b}_1\middle|\vec{b}_2\middle|\ldots\middle|\vec{b}_n\right)$ a $\bar{C}=\left(\vec{c}_1\middle|\vec{c}_2\middle|\ldots\middle|\vec{c}_n\right)$. Tedy *i*-tý sloupec matice *X* je roven vyjádření vektoru c_i v bázi *B*. Matice přechodu od báze *C* k bázi *B* je rovna X^{-1}.

Skalární součin vektorů $\vec{x}=\left(x_1,\mathrm{x}_2,\ldots,\mathrm{x}_\mathrm{n}\right)^T$ a $\vec{y}=\left(y_1,y_2,\ldots,y_n\right)^T$ je dán vztahem

$$\vec{x}\cdot\vec{y}=\vec{x}^T\vec{y}=x_1y_1+x_2y_2+\ldots+x_ny_n,$$

kde T v druhém výrazu značí transponování a součin chápeme maticově, tj. jako součin matice typu $1\times n$ s maticí typu $n\times 1$. Velikost vektoru x budeme značit

$$\left\|\vec{x}\right\|=\sqrt{\vec{x}\cdot\vec{x}}\,.$$

Dva nenulové vektory nazveme kolmé, pokud je jejich skalární součin roven 0.

Definice 1: Vektorovým prostorem nad tělesem *T* rozumíme neprázdnou množinu prvků *V*, na níž je definováno sčítání dvojic prvků (tedy $\forall\vec{u},\vec{v}\in V:\vec{u}+\vec{v}\in V$) a násobení prvků z *V* prvky z tělesa *T* (tedy $\forall\vec{u}\in V\wedge\forall r\in T:r\vec{u}\in V$). Uvedené operace musí splňovat tyto podmínky:

1. $\vec{u}+\vec{v}=\vec{v}+\vec{u}$ $\quad\vec{u},\vec{v}\in V$, neboli komutativita
2. $\left(\vec{u}+\vec{v}\right)+\vec{w}=\vec{u}+\left(\vec{v}+\vec{w}\right)$ $\quad\vec{u},\vec{v},\vec{w}\in V$, neboli asociativita
3. $\exists\vec{o}\in V:0\cdot\vec{u}=\vec{o}$ $\quad\vec{u}\in V$
4. $r\left(\vec{u}+\vec{v}\right)=r\vec{u}+r\vec{v}$ $\quad\vec{u},\vec{v}\in V,r\in T$, neboli distributivita

5. $(r+s)\vec{u} = r\vec{u} + s\vec{u}$ $\vec{u} \in V; r, s \in T$, neboli distributivita sčítání čísel
6. $r(s\vec{u}) = (rs)\vec{u}$ $\vec{u} \in V; r, s, \in T$, neboli asociativní zákon násobení
7. $1 \cdot \vec{u} = \vec{u}$ $\vec{u} \in V$

Příklady vektorových prostorů:

- Těleso T spolu s operacemi sčítání a násobení definovanými na T je V (vektorový prostor) nad T.
- Speciálně těleso reálných čísel je V nad R.
- Množina všech polynomů s koeficienty v T je spolu s obvyklými operacemi sčítání a násobení prvkem z T vektorový prostor nad T.

Definice 2: Neprázdnou podmnožinu W vektorového prostoru nazveme *podprostorem* prostoru V, jestliže W je vektorovým prostorem vzhledem k operacím sčítání a násobení prvky z T definovanými na V. Značíme $W \subseteq V$.

Definice 3: Buď M podmnožina vektorového prostoru V. Průnik všech podprostorů prostoru V, obsahujících množinu M, nazýváme *lineárním obalem* množiny M a značíme $[M]$. Je-li množina M konečná, $M = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$, pak místo $[\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}]$ budeme psát $[\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n]$.

Definice 4: Podmnožina M vektorového prostoru V se nazývá *bází*, jestliže je lineárně nezávislá a generuje V.

Definice 5: Neprázdná podmnožina M vektorového prostoru V nad tělesem T se nazývá *lineárně nezávislá*, jestliže pro každou vlastní podmnožinu $N \subset M$ je $[N] \subset [M]$. V opačném případě, tj. když existuje vlastní podmnožina N množiny M taková, že $[N] = [M]$, se množina M nazývá *lineárně závislá*.

Definice 6: Podmnožina M vektorového prostoru V se nazývá *množivou generátorů* prostoru V, jestliže $[M] = V$. Můžeme též říkat, že množina M *generuje* V. Nebo-li: Podmnožina M vektorového prostoru V je množinou generátorů prostoru V, právě tehdy když každý vektor z V je lineární kombinací vektorů z množiny M.

Definice 7: Buďte $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n$ vektory z vektorového prostoru *V*. *Lineární kombinací* vektorů $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n$ nazveme každý vektor

$$\vec{u} = r_1\vec{u}_1 + r_2\vec{u}_2 + \ldots + r_n\vec{u}_n = \sum_{i=1}^{n} r_i\vec{u}_i ,$$

kde $r_1, r_2, \ldots, r_n \in T$. Prvky $r_1, r_2, \ldots, r_n$ nazýváme *koeficienty lineární kombinace*. Lineární kombinace se nazývá *triviální*, pokud jsou všechny její koeficienty rovny nule. Pokud je alespoň jeden různý od nuly, říkáme, že je *netriviální*.

Příklad 1: Zjistěte, které z těchto množin generují R^4:

a) {(1,1,1,1),(2,1,3,2),(-2,3,-1,0),(-1,0,1,1)},

b) {(2,1,0,2),(-5,-3,2,4),(1,1,1,2)},

c) {(1,2,1,2),(2,1,2,1),(1,1,1,1),(-2,0,-1,-3),(-1,1,0,-2)},

d) {(-1,1,0,-1),(2,0,1,3),(1,2,3,4),(2,3,4,6),(1,-3,5,-7)}.

Řešení:

a) nejprve si rozepíšeme vektory do matice a zjistíme, zda jsou LZ nebo LN:

$$\left(\begin{array}{cccc|c} 1 & 2 & 2 & 1 & a \\ 1 & 1 & 3 & 0 & b \\ 1 & 3 & 1 & 1 & c \\ 1 & 2 & 0 & 1 & d \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & -2 & -1 & a \\ 0 & -1 & 5 & 1 & b-a \\ 0 & 2 & -4 & 1 & c-b \\ 0 & 0 & 2 & 2 & d-a \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1 & 2 & -2 & -1 & a \\ 0 & -1 & 5 & 1 & b-a \\ 0 & 0 & 6 & 3 & c-2a+b \\ 0 & 0 & 2 & 2 & d-a \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & -2 & -1 & a \\ 0 & -1 & 5 & 1 & b-a \\ 0 & 0 & 6 & 3 & c-2a+b \\ 0 & 0 & 0 & 3 & -a+b-c+3d \end{array}\right)$$

Vektory jsou lineárně nezávislé a dokážeme najít pro libovolné *a, b, c, d* dokážeme najít řešení.
Tato množina generuje R^4.

b) Negeneruje R^4, jsou dány jen 3 vektory.

c) také nejprve rozepíšeme do matice:

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & -2 & -1 & a \\ 2 & 1 & 1 & 0 & 1 & b \\ 1 & 2 & 1 & -1 & 0 & c \\ 2 & 1 & 1 & -3 & -2 & d \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 2 & 1 & -2 & -1 & a \\ 2 & 1 & 1 & 0 & 1 & b \\ 0 & 0 & 0 & 1 & 1 & c-a \\ 0 & 0 & 0 & -3 & -3 & d-b \end{array}\right) \sim$$

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & -2 & -1 & a \\ 2 & 1 & 1 & 0 & 1 & b \\ 0 & 0 & 0 & 1 & 1 & c-a \\ 0 & 0 & 0 & 0 & 0 & d-b+3c-3a \end{array}\right)$$

Negeneruje R^4.

d) opět rozepíšeme do matice:

$$\left(\begin{array}{ccccc|c} -1 & 2 & 1 & 2 & 1 & a \\ 1 & 0 & 2 & 3 & -3 & b \\ 0 & 1 & 3 & 4 & 5 & c \\ -1 & 3 & 4 & 6 & -7 & d \end{array}\right) \sim \left(\begin{array}{ccccc|c} -1 & 2 & 1 & 2 & 1 & a \\ 0 & 2 & 3 & 5 & -2 & a+b \\ 0 & 1 & 3 & 4 & 5 & c \\ 0 & 3 & 6 & 9 & -10 & b+d \end{array}\right) \sim$$

$$\left(\begin{array}{ccccc|c} -1 & 2 & 1 & 2 & 1 & a \\ 0 & 0 & -3 & -3 & -12 & a+b-2c \\ 0 & 1 & 3 & 4 & 5 & c \\ 0 & 0 & -3 & -3 & -25 & b+d-3c \end{array}\right) \sim \left(\begin{array}{ccccc|c} -1 & 2 & 1 & 2 & 1 & a \\ 0 & 1 & 3 & 4 & 5 & c \\ 0 & 0 & -3 & -3 & -12 & a+b-2c \\ 0 & 0 & 0 & 0 & -13 & -a-c+d \end{array}\right)$$

Vektory jsou lineárně nezávislé a dokážeme najít pro libovolné *a, b, c, d* dokážeme najít řešení.

Tato množina generuje R^4.

Definice 8: Řekneme, že vektorový prostor *V* nad *T* má *konečnou dimenzi*, jestliže ve *V* existuje konečná množina generátorů.

Definice 9: Buď $V \neq 0$ vektorový prostor konečné dimenze. *Dimenzí* prostoru *V* rozumíme počet prvků libovolné jeho báze. Triviální vektorový prostor $V = 0$ má dimenzi 0. Vektorový prostor dimenze *n* budeme značit V_n, nebo budeme psát *dim V = n*.

Příklad 2: Určete dimenzi podprostoru [(1,2,1,3,-2,4),(1,2,2,3,-6,8),(1,3,4,1,-7,11), (3,7,7,7,-15,23),(2,3,0,8,-3,5)] prostoru R^6.

Řešení: $\begin{pmatrix} 1 & 2 & 1 & 3 & -2 & 4 \\ 1 & 2 & 2 & 3 & -6 & 8 \\ 1 & 3 & 4 & 1 & -7 & 11 \\ 3 & 7 & 7 & 7 & -15 & 23 \\ 2 & 3 & 0 & 8 & -3 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 3 & -2 & 4 \\ 0 & 0 & 1 & 0 & -4 & 4 \\ 0 & 1 & 3 & -2 & -5 & 7 \\ 0 & 1 & 4 & -2 & -9 & 11 \\ 0 & -1 & -2 & 2 & 1 & -3 \end{pmatrix} \sim$

$\begin{pmatrix} 1 & 2 & 1 & 3 & -2 & 4 \\ 0 & 1 & 3 & -2 & -5 & 7 \\ 0 & 0 & 1 & 0 & -4 & 4 \\ 0 & 1 & 4 & -2 & -9 & 11 \\ 0 & -1 & -2 & 2 & 1 & -3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 3 & 2 & 4 \\ 0 & 1 & 3 & -2 & -5 & 7 \\ 0 & 0 & 1 & 0 & -4 & 4 \\ 0 & 0 & 1 & 0 & -4 & 4 \\ 0 & 0 & 1 & 0 & -4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 3 & -2 & 4 \\ 0 & 1 & 3 & -2 & -5 & 7 \\ 0 & 0 & 1 & 0 & -4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

Takže *dim W = 3.*

Definice 10: Buďte V a V' vektorové prostory nad tělesem T. Zobrazení f množiny V do množiny V' se nazývá *homomorfismus*, jestliže pro všechna $\vec{u}, \vec{v} \in V$, $r \in T$ platí:

$$f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$$
$$f(r\vec{u}) = r \cdot f(\vec{u})$$

Homomorfismus f, který je *prostým* zobrazením, se nazývá *monomorfismus*. Homomorfismus f, který je zobrazením V *na* V′, se nazývá *epimorfismus*. Homomorfismus, který je současně monomorfismem a epimorfismem, se nazývá *izomorfismus*. Řekneme, že vektorové prostory V a V' jsou izomorfní, $V \cong V'$, jestliže existuje izomorfismus prostoru V na V'. Pro homomorfismus vektorového prostoru V do vektorového prostoru V' budeme používat označení $f : V \to V'$.

Definice 11: Buďte V, V' vektorové prostory a $f : V \to V'$ homomorfismus. Množinu $Ker\, f = \{\vec{u} \in V \,|\, f(\vec{u}) = 0\}$ nazýváme *jádrem homomorfismu f*. Množinu $\mathrm{Im}\, f = \{f(\vec{u}) \,|\, \vec{u} \in V\}$ nazýváme *obrazem homomorfismu f.*

Věta: Buď f homomorfismus vektorového prostoru V do vektorového prostoru V'. Pak:

a) f je monomorfismus, právě když Ker f = 0,

b) f je epimorfismus, právě když Im f = V',

c) f je izomorfismus, právě když Ker f = 0 a Im f = V'.

Důkaz

a) Pokud je *f* monomorfismus, je zřejmě Ker *f* = 0. Obráceně předpokládejme, že existují vektory $\vec{u},\vec{v} \in V, \vec{u} \neq \vec{v}$, takové, že $f(\vec{u}) = f(\vec{v})$. Pak $0 = f(\vec{u}) - f(\vec{v}) = f(\vec{u} - \vec{v})$, takže $0 \neq \vec{u} - \vec{v} \in Ker\ f$, což je ve sporu. Tvrzení b) je jasné a tvrzení c) vyplývá z a) a b).■

Definice 12: Buďte $f, h: V \to V', g: V' \to V''$ homomorfismy. Homomorfismus $gf: \mathrm{V} \to \mathrm{V}''$ definovaný vztahem $(gf)(\vec{\mathrm{u}}) = \mathrm{g}(f(\vec{\mathrm{u}}))$ nazýváme *složením* (nebo součinem) homomorfismů *f* a *g*. Součet homomorfismů *f* a *h* je definovaný vztahem $(f+h)(\vec{u}) = f(\vec{u}) + h(\vec{u})$.Násobení homomorfismů *f* prvkem *r*∈*T* je definováno vztahem $(rf)(\vec{u}) = r \cdot f(\vec{u})$.

2.3.2 ORTOGONÁLNÍ A ORTONORMÁLNÍ BÁZE

Definice 13: Nechť *V* je vektorový prostor nad tělesem *T*, pak *skalárním součinem* na prostoru *V* nazveme každé zobrazení *f* množiny $V \times V$ do tělesa *T*, které má následující vlastnosti:

1) $\forall x, y \in V$ $\quad f(x,y) = \overline{f(y,x)}$,

2) $\forall x, y, z \in V$ $\quad f(x+y,z) = f(x,z) + f(y,z)$,

3) $\forall x, y \in V, \forall a \in T$ $\quad f(ax,y) = a \cdot f(x,y)$,

4) $\forall x \in V, x \neq 0$ $\quad f(x,x) > 0$.

Když máme definovaný skalární součin dvou vektorů $\vec{u}\ a\ \vec{v}$, který zapisujeme jako $\vec{u} \cdot \vec{v}$, můžeme rozepsat axiomy, které jsou:

$(S_1)(\forall \vec{u} \in V)$ $\quad \vec{u} \cdot \vec{u} \geq 0 \wedge \vec{u} \cdot \vec{u} = 0 \leftrightarrow \vec{u} = \vec{o}$,

$(S_2)(\forall \vec{\mathrm{u}}, \vec{\mathrm{v}} \in \mathrm{V})$ $\quad \vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$, neboli: platí komutativita,

$(S_3)(\forall \vec{\mathrm{u}}, \vec{\mathrm{v}}, \vec{\mathrm{w}} \in \mathrm{V})$ $\quad \vec{u} \cdot (\vec{v} + \vec{w}) = \vec{u}\vec{v} + \vec{u}\vec{w}$, neboli: platí distributivita sčítání vektorů,

$(S_4)(\forall \vec{\mathrm{u}}, \vec{\mathrm{v}} \in \mathrm{V}), (\lambda \in \mathrm{R})$ $\quad (\lambda \cdot \vec{u}) \cdot \vec{v} = \lambda \cdot (\vec{u} \cdot \vec{v})$.

Definice 14: *Velikostí (normou) vektoru* $\vec{v}$, kterou značíme $|\vec{v}|$, rozumíme reálné číslo $\|\vec{v}\|$ definované rovností:

$$|\vec{v}| = \sqrt{\vec{v} \cdot \vec{v}}\,.$$

Jestliže se $\|\vec{v}\| = 1$, pak se vektor $\vec{v}$ nazývá *normovaný (jednotkový).*

Definice 15: Odchylkou φ dvou nenulových vektorů $\vec{u}\ a\ \vec{v}$, rozumíme úhel $\varphi \in \langle 0, \pi \rangle$. Tento úhel je definovaný takto:

$$\cos\varphi = \frac{\vec{u} \cdot \vec{v}}{|\vec{u}| \cdot |\vec{v}|}\,.$$

Příklad 3: Máme dané tři body: A=[1,5,1], B=[5,6,0], C=[2,5,2]. Určete úhel α.

Řešení:

$\vec{v} = B - A = (4,1,-1)$
$\vec{u} = C - A = (1,0,1)$
$|\vec{v}| = \sqrt{4^2 + 1^2 + (-1)^2} = \sqrt{18}$
$|\vec{u}| = \sqrt{1^2 + 1^2} = \sqrt{2}$

$$\cos\alpha = \frac{4 \cdot 1 + 0 + (-1) \cdot 1}{\sqrt{18} \cdot \sqrt{2}} = \frac{3}{6} = 0,5$$

$\alpha = 60^\circ$

Definice 16: Řekneme, že vektory $x, y \in V$ jsou *navzájem ortogonální*, tedy kolmé, jestliže je jejich skalární součin roven nule. Podmnožina *M* prostoru *V* se nazývá *ortogonální*, jestliže jsou každé dva její různé vektory navzájem ortogonální. Podmnožina *M* prostoru *V* se nazývá *ortonormální*, jestliže je ortogonální a každý její vektor je normovaný. *Ortogonální*, resp. *ortonormální bází* prostoru V budeme rozumět každou bázi tohoto prostoru, která je ortogonální, resp. ortonormální množinou.

Příklad 4: Dva jednotkové vektory v rovině, které jsou na sebe kolmé, tvoří ortonormální bázi.

Pozn.: Zatímco ortogonální množina může obsahovat nulový vektor, množina ortonormální ho obsahovat nemůže. Každá ortonormální množina je tedy lineárně

nezávislá. Poznamenejme ještě, že z každé ortogonální podmnožiny neobsahující nulový vektor můžeme normováním vektorů utvořit množinu ortonormální.

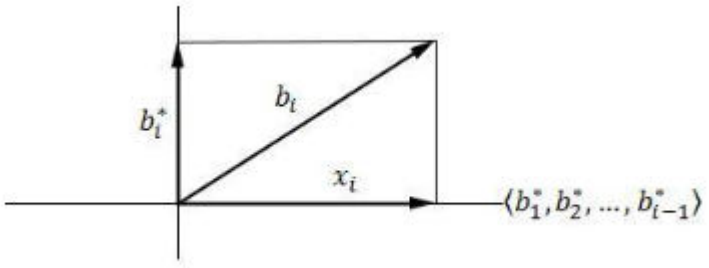
Definice 17: Nechť *M* je podmnožina vektorového prostoru *V*. Řekneme, že vektor $\vec{v} \in V$ je *ortogonální k podmnožině M*, jestliže je ortogonální ke každému vektoru této podmnožiny. Množinu všech vektorů prostoru *V*, které jsou ortogonální k podmnožině *M*, značíme symbolem $M^{\perp}$. Jestliže *W* je podprostor prostoru *V*, potom množinu $W^{\perp}$ nazýváme *ortogonální doplněk podprostoru W* v prostoru *V*.

2.3.3 GRAMŮV – SCHMIDTŮV ORTOGONALIZAČNÍ PROCES

Tento proces pro danou bázi $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ prostoru $\mathbb{R}^n$ nalezne bázi $\vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_n^*$ takovou, že: $\vec{b}_i^* \cdot \vec{b}_j^* = 0$ pro všechna $1 \le i < j \le n$,

$\vec{b}_i^* = \vec{b}_i - \vec{x}_i$, kde $\vec{x}_i \in \langle \vec{b}_1, \ldots, \vec{b}_{i-1} \rangle$ pro všechna $1 \le i \le n$.

Tedy: z první vlastnosti je patrné, že výsledné vektory $\vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_n^*$ jsou vzájemně kolmé. A z druhé vlastnosti plyne, že $\langle \vec{b}_1, \vec{b}_2, \ldots, \vec{b}_i \rangle = \langle \vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_i^* \rangle$ pro všechna *i*. Vektor $\vec{x}_i$ z druhé vlastnosti je ortogonální projekcí vektoru $\vec{b}_i$ na podprostor $\langle \vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{i-1} \rangle$, neboli nejlepší aproximace vektoru $\vec{x}_i$ v tomto prostoru. Vektor $\vec{b}_i^*$ je potom kolmicí na tento podprostor, neboli ortogonální projekcí vektoru $\vec{b}_i$ na ortogonální doplněk $\langle \vec{b}_1, \ldots, \vec{b}_{i-1} \rangle^{\perp}$.



obr. 4

Gramův – Schmidtův ortogonalizační proces si můžeme představit tak, že vstupní vektory postupně narovnáváme do kolmé polohy, *i* - tým vektorem posouváme

v podprostoru určeném prvními i vektory tak, aby se neměnil objem rovnoběžnostěnu, který tyto vektory určují.

Protože jsou na sebe vektory vystupující na pravé straně kolmé, tak platí $\left\|\vec{b}_i\right\|^2 = \left\|\vec{b}_i^*\right\|^2 + \left\|\vec{x}_i\right\|^2$. A speciálně $\left\|\vec{b}_i^*\right\| \leq \left\|\vec{b}_i\right\|$.

Jak spočítat vektory $\vec{b}_i^*$? Vektor $\vec{x}_i$ leží v podprostoru $\left\langle \vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_{i-1}^* \right\rangle$, tedy

$$\vec{x}_i = \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*$$

pro jistá reálná čísla μ_{ij}. Tyto koeficienty budeme počítat tak, že roznásobíme vztah $\vec{b}_i^* \cdot \vec{b}_j^* = (\vec{b}_i - \vec{x}_i) \cdot \vec{b}_j^* = 0$ a dosadíme vyjádření vektoru x_i. Dostaneme vztah:

$$\mu_{ij} = \frac{\vec{b}_i \vec{b}_j^*}{\vec{b}_j^* \vec{b}_j^*} = \frac{\vec{b}_i \vec{b}_j^*}{\left\|\vec{b}_j^*\right\|^2}.$$

Vektory $\vec{b}_1^*, \ldots, \vec{b}_n^*$ jsou tedy vektory $\vec{b}_1, \ldots, \vec{b}_n$ jednoznačně určeny takto:

$\vec{b}_1^* = \vec{b}_1$

$\vec{b}_2^* = \vec{b}_2 - \mu_{21} \vec{b}_1^*$, $kde\ \mu_{21} = \dfrac{\vec{b}_2 \cdot \vec{b}_1^*}{\left\|\vec{b}_1^*\right\|^2}$,

…

$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*$, $kde\ \mu_{ij} = \dfrac{\vec{b}_i \cdot \vec{b}_j^*}{\left\|\vec{b}_j^*\right\|^2}$

Vyjádřením vektorů $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ získáme maticový zápis

$$\left(\vec{b}_1 \middle| \vec{b}_2 \middle| \ldots \middle| \vec{b}_n\right) = \left(\vec{b}_1^* \middle| \vec{b}_2^* \middle| \ldots \middle| \vec{b}_n^*\right) \begin{pmatrix} 1 & \mu_{21} & \mu_{31} & \ldots & \mu_{n1} \\ 0 & 1 & \mu_{32} & \ldots & \mu_{n2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

Teď ukážeme alternativní způsob výpočtu ortogonální projekce $\vec{x}_i$ vektoru $\vec{b}_i$ na podprostor $\langle \vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{i-1} \rangle$. Hledáme vektor $\vec{x}_i = x_1\vec{b}_1 + x_2\vec{b}_2 + \ldots + x_{i-1}\vec{b}_{i-1}$, vektor $\vec{b}_i - \vec{x}_i$ je kolmý na všechny vektory $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{i-1}$. A vyjde soustava rovnic:

$$G_{\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_{i-1}} \cdot (x_1, x_2, \ldots, x_{i-1})^T = (\vec{b}_i \cdot \vec{b}_1, \vec{b}_i \cdot \vec{b}_2, \ldots, \vec{b}_i \cdot \vec{b}_{i-1})^T$$

kde $G_{\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_{i-1}}$ je tzv. Gramova matice vzhledem k vektorům $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{i-1}$, je dána předpisem

$$G_{\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_{i-1}} = (\vec{b}_k \cdot \vec{b}_l)_{k,l=1}^{i-1} = \left(\vec{b}_1 \middle| \ldots \middle| \vec{b}_{i-1}\right)^T \left(\vec{b}_1 \middle| \ldots \middle| \vec{b}_{i-1}\right).$$

Rozdíl těchto dvou postupů je v tom, zda vyjadřujeme vektor $\vec{x}_i$ v nové bázi $\vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_{i-1}^*$, nebo ve staré bázi $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{i-1}$. Výhoda prvního postupu je ta, že vzniká soustava rovnic na diagonální matici, takže můžeme její řešení (μ_{ij}) přímo vyjádřit.

Ještě si připomeňme, že absolutní hodnota determinantu udává *n*-rozměrný objem rovnoběžnostěnu určeného sloupcovými (řádkovými) vektory dané matice. Geometrický význam determinantu Gramovy matice udává druhou mocninu *k*-rozměrného objemu rovnoběžnostěnu určeného bázovými vektory $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k$.

Definice 18: Nechť V je reálný nebo komplexní unitární prostor. *Gramovou maticí* vektorů $\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_m \in V$ nazýváme matici

$$G(\vec{w}_1, \ldots, \vec{w}_m) = \begin{pmatrix} (w_1|w_1) & \ldots & (w_1|w_m) \\ (w_2|w_1) & \ldots & (w_2|w_m) \\ \ldots & \ldots & \ldots \\ (w_m|w_1) & \ldots & (w_m|w_m) \end{pmatrix}.$$

Determinant této matice se nazývá *Gramův determinant* vektorů $\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_m$.

Gramova matice vektorů $\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_m$ je tedy sestavena ze skalárních součinů těchto vektorů tak, že na místě *ij* je skalární součin $(\vec{w}_i|\vec{w}_j)$.

Jestliže je $M = \{\vec{v}_1, \ldots, \vec{v}_n\}$ báze prostoru *V*, potom je $G(\vec{v}_1, \ldots, \vec{v}_n)$ „maticí skalárního součinu“ vzhledem k bázi *M*.

Ještě si upřesníme pojem použitý v předchozí definici, a to komplexní unitární prostor:

Prostorem se skalárním součinem, resp. *unitárním prostorem* budeme rozumět každý vektorový prostor s pevně zvoleným skalárním součinem. *Reálným*, resp. *komplexním* unitárním prostorem budeme rozumět unitární prostor nad tělesem reálných, resp. komplexních čísel.

Příklad 5: Uvažujeme množinu vektorů $\vec{v}_1 = (1,1,0), \vec{v}_2 = (2,0,1), \vec{v}_3 = (0,1,1)$. Proveďte Gramův-Schmidtův ortogonalizační proces.

Musíme tedy najít takové vektory, které mají jednotkovou velikost, jsou navzájem kolmé a každý z vektorů $\vec{v}_i$ lze zapsat jako lineární kombinaci vektorů $\vec{u}_j$.

Ještě před tím, než začneme počítat, si ověříme lineární nezávislost. Ta je patrná už „letmým“ pohledem, ale pro jistotu si vektory přepíšeme do matice:

$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \square \begin{pmatrix} 1 & 2 & 0 \\ 0 & -2 & 1 \\ 0 & 1 & 1 \end{pmatrix} \square \begin{pmatrix} 1 & 2 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$$

a vidíme, že jsou skutečně lineárně nezávislé. Teď se budeme věnovat ortogonalizaci. Gramův-Schmidtův ortogonalizační proces se dá provádět různými postupy. My si nyní ukážeme dva z nich.

Řešení 1:

$\vec{v}_1 = \vec{v}_1^* = (1,1,0)$

$\vec{v}_2 = (2,0,1)$

$\vec{v}_3 = (0,1,1)$

$$\mu_{21} = \frac{\vec{v}_2 \cdot \vec{v}_1^*}{\left\|\vec{v}_1^*\right\|^2} = \frac{(2+0+0)}{1^2+1^2} = 1$$

$$\mu_{31} = \frac{\vec{v}_3 \cdot \vec{v}_1^*}{\left\|\vec{v}_1^*\right\|^2} = \frac{(0+1+0)}{2} = \frac{1}{2}$$

$$\vec{v}_2^* = \vec{v}_2 - \mu_{21} \cdot \vec{v}_1^* = (2,0,1) - 1(1,1,0) = (1,-1,1)$$

$$\mu_{32} = \frac{\vec{v}_3 \cdot \vec{v}_2^*}{\left\|\vec{v}_2^*\right\|^2} = \frac{(0-1+1)}{1^2+(-1)^2+1^2} = 0$$

$$\vec{v}_3^* = \vec{v}_3 - \mu_{31} \cdot \vec{v}_1^* - \mu_{32} \cdot \vec{v}_2^* = (0,1,1) - \frac{1}{2}(1,1,0) - 0(1,-1,1) =$$

$$= (0,1,1) - \left(\frac{1}{2},\frac{1}{2},0\right) = \left(-\frac{1}{2},\frac{1}{2},1\right)$$

A získáváme tedy trojici vektorů: $\vec{v}_1^* = (1,1,0), \vec{v}_2^* = (1,-1,1), \vec{v}_3^* = \left(-\frac{1}{2},\frac{1}{2},1\right)$

Řešení 2:

Za první vektor $\vec{u}_i$ dosadíme normovaný vektor $\vec{v}_1$, požadujeme, ale velikost vektorů $\vec{u}_i$ byla rovna jedné. Tedy

$$\vec{u}_1 = \frac{\vec{v}_1}{\left\|\vec{v}_1\right\|} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{pmatrix}$$

Za druhý vektor zvolíme takto:

$$\vec{u}_2 = \frac{\vec{v}_2 - \vec{u}_1(\vec{u}_1 \cdot \vec{v}_2)}{\left\|\vec{v}_2 - \vec{u}_1(\vec{u}_1 \cdot \vec{v}_2)\right\|} = \frac{(2,0,1) - \left[\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right) \cdot \left(\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right) \cdot (2,0,1)\right)\right]}{\left\|(2,0,1) - \left[\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right) \cdot \left(\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right) \cdot (2,0,1)\right)\right]\right\|} =$$

$$= \frac{(2,0,1) - \left[\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right) \cdot \left(\frac{2}{\sqrt{2}}+0+0\right)\right]}{\left\|(2,0,1) - (1,1,0)\right\|} = \frac{(2,0,1) - (1,1,0)}{\left\|(2,0,1) - (1,1,0)\right\|} =$$

$$= \frac{(1,-1,1)}{\left\|(1,-1,1)\right\|} = \frac{(1,-1,1)}{\sqrt{(1^2+(-1)^2+1^2}} = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$$

Tento vektor má jednotkovou velikost, protože:

$$\left\|\vec{u}_2\right\| = \sqrt{\left(\frac{1}{\sqrt{3}}\right)^2 + \left(-\frac{1}{\sqrt{3}}\right)^2 + \left(\frac{1}{\sqrt{3}}\right)^2} = \sqrt{1} = 1$$

a také je $\vec{u}_1 \cdot \vec{u}_2 = 0$ o čemž se můžeme přesvědčit, tak, že vektory vynásobíme:

$$\vec{u}_1 \cdot \vec{u}_2 = \frac{\vec{u}_1 \cdot \vec{v}_2 - (\vec{u}_1 \cdot \vec{u}_1)(\vec{u}_1 \cdot \vec{v}_2)}{\left\|\vec{v}_2 - \vec{u}_1(\vec{u}_1 \cdot \vec{v}_2)\right\|} = \frac{(\vec{u}_1 \cdot \vec{v}_2) - (\vec{u}_1 \cdot \vec{v}_2)}{\left\|\vec{v}_2 - \vec{u}_1(\vec{u}_1 \cdot \vec{v}_2)\right\|} = 0$$

Zbývá poslední vektor: $\vec{u}_3 = \frac{\vec{v}_3 - \vec{u}_2(\vec{u}_2 \cdot \vec{v}_3) - \vec{u}_1(\vec{u}_1 \cdot \vec{v}_3)}{\left\|\vec{v}_3 - \vec{u}_2(\vec{u}_2 \cdot \vec{v}_3) - \vec{u}_1(\vec{u}_1 \cdot \vec{v}_3)\right\|} =$

$$= \frac{(0,1,1) - \left(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right) \cdot \left(0 - \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{3}}\right) - \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right) \cdot \left(0 + \frac{1}{\sqrt{2}} + 0\right)}{\left\|(0,1,1) - \left(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right) \cdot \left(0 - \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{3}}\right) - \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right) \cdot \left(0 + \frac{1}{\sqrt{2}} + 0\right)\right\|} =$$

$$= \frac{(0,1,1) - (0,0,0) - \left(\frac{1}{2}, \frac{1}{2}, 0\right)}{\left\|(0,1,1) - (0,0,0) - \left(\frac{1}{2}, \frac{1}{2}, 0\right)\right\|} = \frac{\left(-\frac{1}{2}, \frac{1}{2}, 1\right)}{\left\|-\frac{1}{2}, \frac{1}{2}, 1\right\|} = \frac{\left(-\frac{1}{2}, \frac{1}{2}, 1\right)}{\sqrt{\frac{1}{4} + \frac{1}{4} + 1}} =$$

$$= \frac{\left(-\frac{1}{2}, \frac{1}{2}, 1\right)}{\sqrt{\frac{3}{2}}} = \frac{\left(-\frac{1}{2}, \frac{1}{2}, 1\right)}{\frac{\sqrt{6}}{2}} = \frac{2 \cdot \left(-\frac{1}{2}, \frac{1}{2}, 1\right)}{\sqrt{6}} = \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$$

A teď už jsme vypočítali jednu z nekonečně mnoha možných ortonormálních bází, která tedy je:

$$\left\{\vec{u}_1, \vec{u}_2, \vec{u}_3\right\} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix} \right\}. \textit{ (konec příkladu)}$$

2.3.4 MŘÍŽKY

Nyní se seznámíme s pojmem mřížky a uvedeme si jejich vlastnosti. Blíže se budeme věnovat mřížkám v dimenzi 2 a probereme problém hledání krátkého vektoru v dané mřížce.

Budeme se zejména zajímat o mřížky celočíselné. Každá mřížka má pro $n \geq 2$ nekonečně mnoho bází, jako např. dvojice vektorů (1,0),(0,1) a (123,124),(124,125) jsou bázemi jedné stejné mřížky $L = \mathbb{Z}^2$. Budeme se snažit najít relativně krátkou bázi dané celočíselné mřížky. Nejlepší bude, když najdeme bázi složenou z co nejkratších vektorů, jako je to ve výše uvedeném příkladě pro $L = \mathbb{Z}^2$ zřejmě kanonická báze

(1,0),(0,1). Nejkratší bázi je však kromě malých hodnot *n* těžké najít. Neznáme totiž žádný algoritmus pro nalezení nejkratšího nenulového vektoru v dané mřížce.

Nejkratší bázi dané mřížky je tedy složité najít. LLL (Lenstra-Lenstra-Lovászův) algoritmus je schopen v polynomiálním čase najít bázi, která není o mnoho horší než je ta nejlepší. Nejkratší vektor nalezené báze bude nejvýše $\left(2^{\frac{n-1}{2}}\right)$-krát delší než nejkratší nenulový vektor mřížky.

Definice 19: Podmnožina $L \subseteq \mathbb{R}^n$ se nazývá *mřížka*, pokud existuje báze $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ vektorového prostoru $\mathbb{R}^n$ taková, že

$$L = \sum_{i=1}^{n} \mathbb{Z}\, \vec{b}_i = \left\{ \sum_{i=1}^{n} x_i \vec{b}_i : x_1, \ldots, x_n \in \mathbb{Z} \right\}.$$

Vektory $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ nazýváme *bází* této mřížky. Mřížku *L* nazveme *celočíselnou*, pokud $L \subseteq \mathbb{Z}^n$.

Tvrzení 1: Dvě báze prostoru $\mathbb{R}^n$ jsou *bází stejné mřížky* právě tehdy, když je matice přechodu od jedné ke druhé celočíselná s determinantem ± 1.

Důkaz:

$B = \left(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\right)$ a $C = \left(\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_n\right)$ jsou báze prostoru $\mathbb{R}^n$. Označme $\bar{B}, \bar{C}$ příslušné matice a označme *X* (resp. *Y*) matici přechodu od *B* do *C* (resp. od *C* do *B*). Takže $\bar{C} = \bar{B}X$ a $\bar{B} = \bar{C}Y$ a platí $Y = X^{-1}$.

Právě tehdy když:

a) $\Rightarrow$

Předpoklad: *B* a *C* jsou báze stejné mřížky. Protože každý vektor z báze *C* je celočíselnou lineární kombinací vektorů z báze *B*, je *X* celočíselná. Podobně *Y* je celočíselná. Navíc je *XY* jednotková matice a podle věty o součinu determinantu je $\det X \det Y = 1$, takže $\det X = \pm 1$.

b) $\Leftarrow$

Předpoklad: *X* je celočíselná a $\left|\det X\right| = 1$. Pak také *Y* je celočíselná. Tedy každý

vektor z *B* je celočíselnou lineární kombinací vektorů z *C* a naopak, takže *B* a *C* jsou bází stejné mřížky.■

Definice 20: *Determinantem mřížky* L s bází $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ rozumíme číslo

$$d(L) = \left|\det(\vec{b}_1 \left| \vec{b}_2 \right| \ldots \left| \vec{b}_n)\right|.$$

Determinant je důležitým parametrem mřížky a udává *n*-rozměrný objem rovnoběžnostěnu určeného bázovými vektory. Snadným důsledkem předchozího tvrzení je, že determinant na volbě báze nezávisí.

Mřížky v dimenzi 2

Definice 21: Bázi $(\vec{b}_1, \vec{b}_2)$ celočíselné mřížky $L \subseteq \mathbb{Z}^2$ nazveme nejkratší, pokud

a) $\vec{b}_1$ je nejkratší nenulový vektor z L a

b) $\vec{b}_2$ je nejkratší vektor $\mathrm{L} \setminus \left\langle \vec{b}_1 \right\rangle$.

Algoritmus 1: (Gaussova redukce mřížky)

vstup: báze $\left(\vec{b}_1, \vec{b}_2\right)$ mřížky $L \subseteq \mathbb{Z}^2$

výstup: nejkratší báze mřížky *L*

1. **opakuj** v případě $\left\|\vec{b}_1\right\| > \left\|\vec{b}_2\right\|$, **potom** prohoď $\vec{b}_1, \vec{b}_2$

   $$x := [\mu_{21}] = \left[\frac{\vec{b}_1 \cdot \vec{b}_2}{\left\|\vec{b}_1\right\|^2}\right]$$

   $\vec{b}_2 := \vec{b}_2 - x\vec{b}_1$

   dokud $x = 0$

2. **vrať se** $(\vec{b}_1, \vec{b}_2)$

Po proběhnutí každého cyklu je $(\vec{b}_1, \vec{b}_2)$ bází mřížky *L*. Při každém průběhu cyklu se delší vektory zkrátí a mřížka tedy obsahuje konečně mnoho bodů s velikostí menší než předem dané číslo.

Příklad 6: Mějme tří báze mřížky L: (12,2),(13,4); (1,2),(11,0) a (1,2),(9,-4). Která je nejkratší?

Řešení:

Uvědomme si, že kolmé vektory jsou nejkratší bází.

$$\cos\alpha = \frac{(12,2)\cdot(13,4)}{\|(12,2)\|\cdot\|(13,4)\|} = \frac{(156+8)}{\sqrt{12^2+2^2}\cdot\sqrt{13^2+4^2}} = \frac{164}{\sqrt{148}\cdot\sqrt{185}} = \frac{164}{74\sqrt{5}}$$

$\alpha = 7°38'$ .... tento úhel se kolmosti ani nepřibližuje

$$\cos\beta = \frac{(1,2)\cdot(11,0)}{\|(1,2)\|\cdot\|(11,0)\|} = \frac{11}{\sqrt{5}\cdot\sqrt{121}} = \frac{11}{11\sqrt{5}} = \frac{\sqrt{5}}{5}$$

$\beta = 63°26'$ ... tento úhel je větší, ale pořád není kolmý

$$\cos\gamma = \frac{(1,2)\cdot(9,-4)}{\|(1,2)\|\cdot\|(9,-4)\|} = \frac{9-8}{\sqrt{5}\cdot\sqrt{97}} = \frac{1}{\sqrt{485}}$$

$\gamma = 87°24'$ ... Tento úhel je téměř kolmý, takže tato báze je nejkratší.

Příklad 7: Mějme bázové vektory $\vec{b}_1 = (1,5)$ a $\vec{b}_2 = (6,21)$. Najdeme nejkratší bázi mřížky.

Řešení:

Nyní už nebudeme počítat úhly, protože máme zadány jen bázové vektory. Použijeme algoritmus Gaussovy redukce mřížky.

1. $x = \left\lceil \frac{(1,5)\cdot(6,21)}{\|(1,5)\|^2} \right\rfloor = \left\lceil \frac{6+105}{\sqrt{26}^2} \right\rfloor = \left\lceil \frac{111}{26} \right\rfloor = 4$,

   tzn., že položíme $\vec{b}_2 = (6,21) - 4(1,5) = (6,21) - (4,20) = (2,1)$ a protože $x \neq 0$ pokračujeme od začátku. Ale musíme prohodit vektory, podle první podmínky.

2. $x_2 = \left\lceil \frac{(2,1)\cdot(1,5)}{\|(2,1)\|^2} \right\rfloor = \left\lceil \frac{2+5}{\sqrt{5}^2} \right\rfloor = \left\lceil \frac{7}{5} \right\rfloor = 1,$

tzn., že položíme $\vec{b}_2 = (1,5) - (2,1) = (-1,4)$, a protože je už $\|\vec{b}_2\| > \|\vec{b}_1\|$, tak víme, že ve třetím kroku vyjde *x=0.*

Řešením je tedy dvojice vektorů (2,1),(-1,4).

Nyní si dokážeme funkčnost algoritmu Gaussovy redukce mřížky.

Důkaz:

Nechť $\vec{b}_1, \vec{b}_2$ je báze mřížky *L* vrácená v algoritmu. Uvažujeme libovolný nenulový vektor $\vec{v}$ v mřížce *L* takový, že:

$$\vec{v} = x\vec{b}_1 + y\vec{b}_2 \qquad x, y \in \mathbb{Z}, \quad xy \neq 0.$$

A tedy druhá mocnina normy $\vec{v}$ je:

$\|\vec{v}\|^2 = \sqrt{(x\vec{b}_1 + y\vec{b}_2)\cdot(x\vec{b}_1 + y\vec{b}_2)}^2 = x^2\|\vec{b}_1\|^2 + 2xy(\vec{b}_1\cdot\vec{b}_2) + y^2\|\vec{b}_2\|^2$ a protože $|\mu_{21}| \leq \frac{1}{2}$, tak platí $|\vec{b}_1\cdot\vec{b}_2| \leq \frac{1}{2}\|\vec{b}_1\|$ a tedy $\|\vec{v}\|^2 \geq x^2\|\vec{b}_1\|^2 - xy\|\vec{b}_1\|^2 + y^2\|\vec{b}_2\|^2$.

Pokud *x=0*, tak je tento výraz alespoň $\|\vec{b}_2\|^2$, pokud je *y=0*, tak je alespoň $\|\vec{b}_1\|^2$.

Pokud je $0<|y| \leq |x|$, potom $x^2 - xy \geq 0,$ takže součet dvou prvních výrazů je kladný a dostáváme alespoň $\|\vec{b}_2\|^2$ a pokud $0<|x|<|y|$, pak $y^2 - xy \geq 1$ a už součet druhého a třetího členu je alespoň $\|\vec{b}_2\|^2$ takže $\vec{b}_1$ je opravdu nejkratším nenulovým vektorem mřížky a vektory z $L \setminus \langle \vec{b}_1 \rangle$ mají délku alespoň $\|\vec{b}_2\|$.■

Na závěr tématu mřížek uvedeme jednu aplikaci mřížek v dimenzi 2 v teorii čísel a pár příkladů.

Tvrzení 2: Každé prvočíslo *p* takové, že $p \equiv 1 (\mathrm{mod}\, 4)$, je součtem dvou čtverců, tj. lze ho zapsat ve tvaru $p = a^2 + b^2$, kde $a, b \in \mathbb{Z}$.

Příklad 8: Najděte nejkratší bázi mřížky $L \subseteq \mathbb{Z}^2$ dané bázovými vektory (3,8),(5,14).

Řešení:

$\|\vec{b}_1\| < \|\vec{b}_2\|$, takže vektory nechám v tomto pořadí

$$x = \left\lceil \frac{(3,8)\cdot(5,14)}{\|(3,8)\|^2} \right\rfloor = \left\lceil \frac{127}{73} \right\rfloor = 1$$

$$\vec{b}_2 = \vec{b}_2 - x\vec{b}_1 = (5,14) - (3,8) = (2,6)$$

$\|\vec{b}_2\| = \sqrt{4+36} = \sqrt{40}$ takže to znamená, že $\|\vec{b}_1\| > \|\vec{b}_2\|$ a musím je prohodit.

$$x = \left\lceil \frac{(2,6)\cdot(3,8)}{\|(2,6)\|^2} \right\rfloor = \left\lceil \frac{54}{40} \right\rfloor = 1$$

$$\vec{b}_2 = \vec{b}_2 - x\vec{b}_1 = (3,8) - (2,6) = (1,2)$$

$\|\vec{b}_2\| = \sqrt{5} < \|\vec{b}_1\| = \sqrt{40}$, takže opět prohodíme

$x = \left\lceil \frac{(2,6)\cdot(1,2)}{\|(2,6)\|^2} \right\rfloor = \left\lceil \frac{14}{40} \right\rfloor = 0$, teď algoritmus skončil a můžeme říct, že nejkratší báze mřížky L je dvojice vektorů (2,6),(1,2).

Příklad 9: Najděte nejkratší bázi mřížky $L \subseteq \mathbb{Z}^2$ dané bázovými vektory (9,5),(5,3).

Řešení:

$\|\vec{b}_1\| = \sqrt{106} > \|\vec{b}_2\| = \sqrt{34}$, takže musíme prohodit vektory.

$$x = \left\lceil \frac{(5,3)\cdot(9,5)}{\|(5,3)\|^2} \right\rfloor = \left\lceil \frac{60}{34} \right\rfloor = 1$$

$\vec{b}_2 = \vec{b}_2 - x\vec{b}_1 = (9,5) - (5,3) = (4,2)$ a tedy

$\left\|\vec{b}_1\right\| = \sqrt{34} > \left\|\vec{b}_2\right\| = \sqrt{20}$, takže opět prohodíme vektory

$$x = \left\lceil \frac{(4,2)\cdot(5,3)}{\left\|(4,2)\right\|^2} \right\rfloor = \left\lceil \frac{26}{20} \right\rfloor = 1$$

$\vec{b}_2 = \vec{b}_2 - x\vec{b}_1 = (5,3) - (4,2) = (1,1)$ a tedy

$\left\|\vec{b}_1\right\| = \sqrt{20} > \left\|\vec{b}_2\right\| = \sqrt{2}$ to je v pořádku, nemusíme prohazovat vektory

$$x = \left\lceil \frac{(4,2)\cdot(1,1)}{\left\|(4,2)\right\|^2} \right\rfloor = \left\lceil \frac{6}{20} \right\rfloor = 0$$ teď algoritmus skončil a můžeme říct, že nejkratší báze mřížky L je dvojice vektorů (4,2),(1,1).

2.4 LLL-REDUKOVANÁ BÁZE A LLL ALGORITMUS

Nyní už víme, že když chceme najít nejlépe co nejkratší bázi mřížky, snažíme se docílit toho, aby na sebe byly její vektory dostatečně kolmé. Bázi, u níž jsme celočíselnou aproximací Gramovy-Schmidtovy ortogonalizace docílili toho, že koeficienty $\left|\mu_{ij}\right| < \frac{1}{2}$, se říká redukovaná vzhledem k velikosti. Redukovanost vzhledem k velikosti, ale zaručuje kolmost pouze v případě, že velikosti vektorů příliš neklesají.

Bylo by tedy dobré najít podmínku dostatečně silnou, aby bylo možné takovou bázi najít v rozumném (polynomiálním) čase.

To se podařilo Arjenovi Lenstrovi, Heindrikovi Lenstrovi a Lászlóvi Lovászovi v roce 1982 v jejich slavném článku *Factoring Polynomials with Rational Coefficents*, což v překladu znamená faktorizace polynomů s racionálními koeficienty.

Zavedeme pojem LLL-redukované báze mřížky a poté LLL algoritmus.

Definice 22: Báze $\vec{b}_1,\ldots,\vec{b}_n$ mřížky $L \subseteq \mathbb{R}^n$ se nazývá *LLL-redukovaná*, pokud:

(R1) $\left|\mu_{ij}\right| \le \frac{1}{2}$ pro všechna $1 \le j < i \le n$

(R2) $\left\|\vec{b}_i^*\right\|^2 \ge \left(\frac{3}{4} - \mu_{i\ i-1}^2\right)\left\|\vec{b}_{i-1}^*\right\|^2$ pro všechna $1 < i \le n$.

Podmínku (R2) můžeme chápat jako zeslabení podmínky $\left\|\vec{b}_2^*\right\|^2 \geq \frac{3}{4}\left\|\vec{b}_1^*\right\|^2$, kterou máme zaručenou, když skončí algoritmus Gaussovy redukce mřížky v dimenzi 2. Po úpravě podmínky (R2) dostaneme

$$\left\|\vec{b}_i^*\right\|^2 + \mu_{i\,i-1}^2 \left\|\vec{b}_{i-1}^*\right\|^2 \geq \frac{3}{4}\left\|\vec{b}_{i-1}^*\right\|^2$$

a když využijeme kolmost vektorů $\vec{b}_i^*$ *a* $\vec{b}_{i+1}^*$ dostáváme podmínku ekvivalentní k podmínce (R2), tedy podmínku

(R2´) $\left\|\vec{b}_i^* + \mu_{i\,i-1}\vec{b}_{i-1}^*\right\|^2 \geq \frac{3}{4}\left\|\vec{b}_{i-1}^*\right\|^2$ pro všechna $1 < i \leq n$.

Vektory $\vec{b}_i^* + \mu_{i\,i-1}\vec{b}_{i-1}^*$ *a* $\vec{b}_{i-1}^*$ jsou kolmice vektorů $\vec{b}_i$ *a* $\vec{b}_{i-1}$ na podprostor $\left\langle \vec{b}_1,\ldots,\vec{b}_{i-2}\right\rangle$. Podmínce (R2´) lze tedy rozumět tak, že jestli promítneme mřížku o dimenzi 2 generovanou vektory $\vec{b}_i$ a $\vec{b}_{i-1}$ na ortogonální doplněk prostoru $\left\langle \vec{b}_1,\ldots,\vec{b}_{i-2}\right\rangle$, pak je splněna podmínka algoritmu Gaussovy redukce mřížky na uspořádání vektorů podle velikosti až na faktor $\frac{3}{4}$

Konstanta $\frac{3}{4}$ v (R2) může být nahrazena nějakým jiným libovolným reálným číslem z intervalu $\left(\frac{1}{4},1\right)$.

Lemma 1: Pro libovolnou LLL-redukovanou bázi a každé $1 \leq i \leq j \leq n$ platí:

$$\left\|\vec{b}_i\right\|^2 \leq 2^{j-1}\left\|\vec{b}_i^*\right\|^2$$

Důkaz:

Kvůli tomu, že $\vec{b}_i = \vec{b}_i^* + \sum_{k=1}^{i-1}\mu_{ik}\vec{b}_k^*$ a vektory $\vec{b}_1^*,\vec{b}_2^*,\ldots,\vec{b}_i^*$ jsou vzájemně kolmé, dostaneme

$$\left\|\vec{b}_i\right\|^2 = \left\|\vec{b}_i^*\right\|^2 + \sum_{k=1}^{i-1}\mu_{ik}^2\left\|\vec{b}_k^*\right\|^2.$$

Použitím podmínky (R1) a nerovností mezi vektory $\vec{b}_1^*, \vec{b}_2^*, \ldots$ dostaneme

$$\left\|\vec{b}_i\right\|^2 \le \left\|\vec{b}_i^*\right\|^2 + \sum_{k=1}^{i-1} \frac{1}{4} 2^{i-k} \left\|\vec{b}_i^*\right\|^2 = \left\|\vec{b}_i^*\right\|^2 \left(1 + \frac{1}{4}(2^i - 2)\right) \le$$

$$\le 2^{i-1} \left\|\vec{b}_i^*\right\|^2 \le 2^{i-1} 2^{j-1} \left\|\vec{b}_j^*\right\|^2 = 2^{j-1} \left\|\vec{b}_j^*\right\|^2 .$$

A získáváme tak odhad součinu velikostí vektorů LLL-redukované báze a velikosti prvního vektoru v této bázi, v závislosti na determinantu mřížky.

Tvrzení 3: Pro libovolnou LLL-redukovanou bázi $\vec{b}_1, \ldots, \vec{b}_n$ mřížky *L* platí

$$d(L) \le \left\|\vec{b}_1\right\| \left\|\vec{b}_2\right\| \ldots \left\|\vec{b}_n\right\| \le 2^{\frac{n(n-1)}{4}} d(L) \qquad \text{a} \qquad \left\|\vec{b}_1\right\| \le 2^{\frac{n-1}{4}} \sqrt[n]{d(L)}.$$

Důkaz:

Nerovnost $d(L) \le \left\|\vec{b}_1\right\| \left\|\vec{b}_2\right\| \ldots \left\|\vec{b}_n\right\|$ již byla dokázána v důkazu tvrzení 2. Z Lemmatu odvodíme další nerovnost:

$$\prod_{i=1}^{n} \left\|\vec{b}_i\right\| \le \prod_{i=1}^{n} 2^{\frac{i-1}{2}} \left\|\vec{b}_i^*\right\| = 2^{\frac{n(n-1)}{4}} d(L)$$

vynásobíme-li nerovností $\left\|\vec{b}_1\right\|^2 \le 2^{\frac{i-1}{2}} \left\|\vec{b}_i^*\right\|^2$ přes všechna $1 \le i \le n$, tak dostaneme

$$\left\|\vec{b}_1\right\|^{2n} \le \prod_{i=1}^{n} 2^{i-1} \left\|\vec{b}_i^*\right\|^2 = 2^{\frac{n(n-1)}{2}} d(L)^2$$

a konečný výsledek získáme odmocněním.■

Číslu $\frac{\left\|\vec{b}_1\right\| \left\|\vec{b}_2\right\| \ldots \left\|\vec{b}_n\right\|}{d(L)}$ se říká defekt kolmosti báze $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$. Dokázali jsme, že LLL-redukovaná báze má defekt kolmosti nanejvýš $2^{\frac{n(n-1)}{4}}$. Jako poslední nerovnost, kterou odvodíme je dolní odhad velikosti nejkratšího nenulového vektoru mřížky pomocí velikosti vektroru LLL-redukované báze.

Tvrzení 4: Pro libovolnou *LLL*-redukovanou bázi $\vec{b}_1, \ldots, \vec{b}_n$ mřížky *L* a libovolný nenulový vektor $\vec{v} \in L$ platí:

$$\left\|\vec{b}_1\right\| \le 2^{\frac{n-1}{2}} \left\|\vec{v}\right\|$$

Důkaz:

Pro $\vec{v} \in L$ existují celá čísla $x_1, x_2, \ldots, x_n$ taková, že $\vec{v} = \sum_{i=1}^{n} x_i \vec{b}_i$. Označíme k index takový, že $x_k \neq 0$, tedy $\vec{v} = \sum_{i=1}^{k} x_i \vec{b}_i, x_{\ k} \neq 0$. Protože $\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*$, tak platí $\vec{v} = x_k \vec{b}_k^* + \sum_{j=1}^{k-1} v_j \vec{b}_j^*$ pro jistá reálná čísla v_j. Takže

$\left\|\vec{v}\right\|^2 = x_k^2 \left\|\vec{b}_k^*\right\|^2 + \sum_{j=1}^{k-1} v_j^2 \left\|\vec{b}_j^*\right\|^2 \ge \left\|\vec{b}_k^*\right\|^2$ pak už stačí použít Lemmat 1.■

Kostra *LLL* algoritmu je jednoduchá. Nejprve provedeme Gramův-Schmidtův ortogonalizační proces, potom celočíselnou aproximací tohoto procesu získáme novou bázi splňující podmínku (R1) a otestujeme podmínku (R2), není-li pro nějaké kroky *i* splněna, prohodíme vektory $\vec{b}_i$ a $\vec{b}_{i-1}$ a vrátíme se na začátek algoritmu.

Algoritmus 2: (LLL algoritmus)

vstup: báze $\vec{b}_1, \ldots, \vec{b}_n$ mřížky $L \subseteq \mathbb{Z}^n$

výstup: *LLL*-redukovaná báze mřížky *L*

1. Gramovou-Schmidtovou ortogonalizací spočítej $\vec{b}_1^*, \ldots, \vec{b}_n^*$ a $\mu_{ij}, 1 \le j < i \le n$
2. **pro** $i = 2, \ldots, n$ **udělej**

   pro $j = i-1, \ldots, 1$ **udělej**

   $x := \lceil \mu_{ij} \rfloor$

   $\vec{b}_i := \vec{b}_i - x\vec{b}_j$

   $\mu_{ij} := \mu_{ij} - x$

   pro $l = 1, \ldots, j-1$ **udělej** $\mu_{il} := \mu_{il} - x\mu_{jl}$
3. **pro** $i = 2, \ldots, n$ **udělej**

jestli $\left\|\vec{b}_i^*\right\|^2 < \left(\frac{3}{4} - \mu_{i\,i-1}^2\right)\left\|\vec{b}_{i-1}^*\right\|^2$, tak **potom**

prohoď $\vec{b}_i$ a $\vec{b}_{i-1}$

jdi na 1.

4. **vrať** $\vec{b}_1,...,\vec{b}_n$

Po provedení kroku 2. bude splněna podmínka (R1), pokud ukážeme, že hodnoty μ_{ij} jsou správně aktualizovány.

Lemma 2: Po provedení kroku 2. bude splněna podmínka (R1).

Důkaz:

Označíme $\vec{c}_k^*, \vec{c}_k, v_{kl}$ nové hodnoty pro $\vec{b}_k^*, \vec{b}_k, \mu_{kl}$ po odečtení $x\vec{b}_j$ od vektoru $\vec{b}_i$. Tedy $\vec{c}_i = \vec{b}_i - x\vec{b}_j$ a $\vec{c}_k = \vec{b}_k$ pro $k \neq i$. Protože $\vec{c}_i$ vznikl z $\vec{b}_i$ přičtením vektoru z podprostoru $\left\langle \vec{b}_1,...,\vec{b}_{i-1} \right\rangle$, platí $\vec{c}_k^* = \vec{b}_k^*$ pro každé $1 \leq k \leq n$. Pro k,l taková, že $l < k \neq i$, je

$$v_{kl} = \frac{\vec{c}_k \vec{c}_l^*}{\left\|\vec{c}_l\right\|^2} = \frac{\vec{b}_k \vec{b}_l^*}{\left\|\vec{b}_l^*\right\|} = \mu_{kl}$$

Pro l takové, že $j < l < i$, je vektor $\vec{b}_l^*$ kolmý na $\vec{b}_j$, takže

$$v_{il} = \frac{\vec{c}_i \vec{c}_l^*}{\left\|\vec{c}_l^*\right\|^2} = \frac{(\vec{b}_i - x\vec{b}_j)\vec{b}_l^*}{\left\|\vec{b}_l^*\right\|^2} = \frac{\vec{b}_i \vec{b}_l^*}{\left\|\vec{b}_l^*\right\|^2} = \mu_{il}$$

Protože $\vec{b}_j \vec{b}_j^* = \vec{b}_j^* \vec{b}_j^*$, tak platí

$$v_{il} = \frac{\vec{c}_i \vec{c}_j^*}{\left\|\vec{c}_j^*\right\|^2} = \frac{(\vec{b}_i - x\vec{b}_j)\vec{b}_j^*}{\left\|\vec{b}_j^*\right\|^2} = \mu_{ij} - x$$

A konečně, pro $l < j$ máme

$$v_{il} = \frac{\vec{c}_i \vec{c}_l^*}{\left\|\vec{c}_l^*\right\|^2} = \frac{(\vec{b}_i - x\vec{b}_j)\vec{b}_l^*}{\left\|\vec{b}_l^*\right\|^2} = \mu_{il} - x\mu_{jl}\,.$$

Ukázali jsme, že po provedení vnitřku cyklů pro *i* a *j* jsou hodnoty μ_{kl} aktualizovány správně a nová hodnota pro μ_{ij} je nejvýše $\frac{1}{2}$. Navíc jiné hodnoty než $\mu_{il}, l \leq j$ se nemění, takže díky pořadí vykonávání cyklů máme zaručeno, že po provedení kroku 2. jsou μ_{kl} aktualizovány správně.■

Výsledná báze po skončení algoritmu splňuje podmínky (R1) a (R2).

Teď už je jasné, že algoritmus končí a nyní se provedeme důkaz, že algoritmus skončí v polynomiálním čase vzhledem k velikosti vstupu.

K tomu budeme potřebovat následující hodnoty *D* a d_i, $1 \leq i \leq n$:

$$D = \prod_{i=1}^{n} d_i \text{, kde } d_i = \prod_{j=1}^{i} \left\| \vec{b}_j^* \right\|^2 .$$

Číslo d_i je tedy rovno čtverci objemu rovnoběžnostěnu určeného prvními *i* vektory báze, $d_n = d(\mathrm{L})^2$ a platí, že: $d_i = \det(G_{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_i})$.

Ukážeme, že hodnota *D* není příliš velká vzhledem ke vstupu. V kroku 2. se nemění a ve 3. kroku prohozením vektorů se alespoň $\frac{3}{4}$ krát zmenší. Proto se do kroku 1. mnohokrát nevrátíme.

Lemma 3: Velikost *D* i počet návratů do 1. kroku je polynomiální vzhledem k velikosti vstupu.

Důkaz:

Velikost vstupu můžeme odhadnout hodnotou

$$M = \max(n, \log(\max_j \left\| \vec{b}_j \right\|))$$

Na každý vektor je třeba alespoň jeden bit a vektor normy *r* vyžaduje alespoň $\log r$ bitů. Číslo d_i je zřejmě menší než $(\max_j \left\| \vec{b}_j \right\|)^i$, číslo *D* tedy na začátku splňuje

$$D \leq (\max_j \left\| \vec{b}_j \right\|)^{n(n-1)} .$$

Krok 2. nemění hodnoty $\vec{b}_i^*$, tedy ani *D* (jak jsme ukázaly v důkazu Lemmatu 2). Po prohození vektorů $\vec{b}_i$ a $\vec{b}_{i-1}$ se vektory $\vec{b}*_i,\ldots,\vec{b}*_{i-2}$ nezmění, nezmění se ani hodnoty $d_1,\ldots,d_{i-2}$. Z vyjádření $d_j = \det(G_{\vec{b}_1,\ldots,\vec{b}_j})$ je vidět, že se nezmění ani čísla $d_i,\ldots,d_n$. Místo $\vec{b}_{i-1}^*$ označíme novou hodnotu $\vec{c}_{i-1}^*$, jenž je kolmicí $\vec{b}_i$ k podprostoru $\langle \vec{b}_1,\ldots,\vec{b}_{i-2} \rangle$, takže $\vec{c}_{i-1}^* = \vec{b}_i^* + \mu_{i\,i-1}\vec{b}_{i-1}^*$. Z rovnocennosti (R2) a (R2´) vidíme, že norma tohoto vektoru je $\leq \frac{3}{4}\left\|\vec{b}_{i-1}^*\right\|$. Číslo d_i se tedy zmenší alespoň $\frac{3}{4}$ krát a s ním i hodnota *D*. *D* je zdola omezeno jedničkou, a proto je podmínka z kroku 3. splněna nejvýše kolikrát:

$\log_{\frac{4}{3}} D \leq n(n-1)\log_{\frac{4}{3}}(\max\left\|\vec{b}_j\right\|)$ a to je jistě menší než CM^3 pro jistou konstantu *C*.■

Během jednoho průběhu kroků 1., 2., 3. probíhá polynomiálně mnoho operací sčítání, odčítání, násobení a dělení čísel μ_{ij} a složek vektorů $\vec{b}_i \;\; a \;\; \vec{b}_i^*$. K důkazu, že algoritmus pracuje v polynomiálním času chybí odhad velikosti čitatelů a jmenovatelů zúčastněných čísel.

Lemma 4: Pro každé $1 \leq j \leq i \leq n$ je

$d_{i-1}\vec{b}_i^* \in \mathbb{Z}^n$ $\qquad\qquad$ $\left\|\vec{b}_i^*\right\| \leq D$ $\qquad$ a $\qquad$ $d_j\mu_{ij} \in \mathbb{Z}$.

Důkaz:

Zvolíme se tedy libovolné $1 \leq i \leq n$. Vektor $\vec{b}_i^*$ lze napsat jako $\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} a_j\vec{b}_j$, kde $(a_1,\ldots,a_{i-1})$ je řešením soustavy lineárních rovnic

$$G_{\vec{b}_1,\ldots,\vec{b}_{i-1}}(a_1,\ldots,a_{i-1})^T = (\vec{b}_i\cdot\vec{b}_1, \vec{b}_i\cdot\vec{b}_2,\ldots,\vec{b}_i\cdot\vec{b}_{i-1})^T .$$

Podle Cramerova pravidla je každé a_j podílem determinantu jisté celočíselné matice a determinantu matice $G_{\vec{b}_1,\ldots,\vec{b}_{i-1}}$, který je roven d_{i-1} Takže

$$d_{i-1}\vec{b}_i^* = d_{i-1}\vec{b}_i - \sum_{j=1}^{i-1} d_{i-1}a_j\vec{b}_j \in \mathbb{Z}^n$$

Pro libovolné j je $d_{j-1}\vec{b}_j^* \in \mathbb{Z}^n$, proto platí $\left\|d_{j-1}\vec{b}_j^*\right\| \geq 1$ tedy $\left\|\vec{b}_j^*\right\| \geq \frac{1}{d_{j-1}}$. Definice čísel d_j této nerovnosti dostáváme

$$\left\|\vec{b}_i^*\right\|^2 \frac{d_{i+1}}{d_i} = \frac{d_{i+1}}{\left\|\vec{b}_1^*\right\|^2 \left\|\vec{b}_2^*\right\|^2 \ldots \left\|\vec{b}_i^*\right\|^2} \leq d_{i+1} d_1^2 \ldots d_i^2 \leq D^2$$

a konečně

$$d_j \mu_{ij} = d_j \frac{\vec{b}_i \cdot \vec{b}_j^*}{\left\|\vec{b}_j^*\right\|^2} = d_j \frac{\vec{b}_i \cdot \vec{b}_j^*}{\frac{d_j}{d_{j-1}}} = d_{j-1}\left(\vec{b}_i \cdot \vec{b}_j^*\right) = \vec{b}_i \cdot \left(d_{j-1}\vec{b}_j^*\right) \in \mathbb{Z} \quad \blacksquare$$

Lemma 5: Po provedení 2. kroku platí $\left\|\vec{b}_i\right\|^2 \leq nD^2$ pro každé $1 \leq i \leq n$.

Důkaz:

Protože $\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*$ a vektory $\vec{b}_i^*$ jsou na sebe kolmé, platí

$\left\|\vec{b}_i\right\|^2 = \left\|\vec{b}_i^*\right\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \left\|\vec{b}_j^*\right\|^2$. Užitím Lemmatu 4 a nerovnosti $\mu_{ij} \leq \frac{1}{2}$ dostáváme

$$\left\|\vec{b}_i\right\|^2 \leq D^2 + \sum_{j=1}^{i-1} \frac{1}{4} D^2 \leq D^2 + \frac{n}{4} D^2 \leq nD^2 \quad \blacksquare$$

Nyní po shrnutí poznatků dostáváme polynomiální mez pro časovou složitost LLL algoritmu.

Tvrzení 5: *LLL*-algoritmus pracuje v polynomiálním čase v závislosti na velikosti vstupu.

Důkaz:

V lemmatu 3 jsme dokázali, že počet návratů do 1. kroku je shora omezený polynomiálně. Všechny operace (kterých je polynomiálně mnoho) se provádí s racionálními čísly, jejichž jmenovatel je rovněž polynomiálně omezen (dokázáno v Lemmatu 4) a jejichž velikost je také polynomiálně omezená (dokázáno v Lemmatu 4 a 5).■

LLL algoritmus byl formulován ve své zjednodušené podobě, provádí řadu zbytečných operací. Například test ve 3. kroku je lepší provádět průběžně, ne počítat celou Gramovu-Schmidtovu ortogonalizace a její celočíselnou aproximaci znovu.

Příklad 10: Najděte LLL redukovanou bázi mřížky dané bází:

$\vec{b}_1 = (1,1,1), \vec{b}_2 = (-1,0,2), \vec{b}_3 = (3,5,6)$

Řešení:

Nejprve provedeme Gramovu-Schmidtovu ortogonalizaci:

$\vec{b}_1^* = \vec{b}_1 = (1,1,1)$,

$$\mu_{21} = \frac{\vec{b}_2 \cdot \vec{b}_1^*}{\left\|\vec{b}_1\right\|^2}$$

$$\vec{b}_2^* = \vec{b}_2 - \mu_{21}\vec{b}_1^* = (-1,0,2) - \frac{(-1,0,2)\cdot(1,1,1)}{\left\|(1,1,1)\right\|^2}\cdot(1,1,1) = (-1,0,2) - \frac{1}{3}\cdot(1,1,1) = \left(-\frac{1}{4},-\frac{1}{3},\frac{5}{3}\right)$$

$$\mu_{31} = \frac{\vec{b}_3 \cdot \vec{b}_1^*}{\left\|\vec{b}_1^*\right\|^2}, \mu_{32} = \frac{\vec{b}_3 \cdot \vec{b}_2^*}{\left\|\vec{b}_2^*\right\|^2}$$

$$\vec{b}_3^* = \vec{b}_3 - \mu_{31}\vec{b}_1^* - \mu_{32}\vec{b}_2^* = (3,5,6) - \frac{(3,5,6)\cdot(1,1,1)}{\left\|(1,1,1)\right\|^2}\cdot(1,1,1) - \frac{(3,5,6)\cdot\left(-\frac{4}{3},-\frac{1}{3},\frac{5}{3}\right)}{\left\|\left(-\frac{4}{3},-\frac{1}{3},\frac{5}{3}\right)\right\|^2}\cdot\left(-\frac{4}{3},-\frac{1}{3},\frac{5}{3}\right) =$$

$$= (3,5,6) - \frac{14}{3}\cdot(1,1,1) - \frac{13}{14}\cdot\left(-\frac{4}{3},-\frac{1}{3},\frac{5}{3}\right) = \left(-\frac{3}{7},\frac{9}{14},-\frac{3}{14}\right)$$

Takhle je dokončena Gramova-Schmidtova ortogonalizace. V kroku 2. když dosadíme za $i=2, j=1$, tak se nic nestane. Dosadíme $i=3, j=2$ a vyjde:

$x = \left[\mu_{ij}\right] = \left[\mu_{32}\right] = \left[\frac{13}{14}\right] = 1$, $\vec{b}_3 = \vec{b}_3 - x\vec{b}_2 = (3,5,6) - (-1,0,2) = (4,5,4)$

Pro $i=3, j=1$ vyjde:

$x = \left[\mu_{31}\right] = \left[\frac{14}{3}\right] = 4$, $\vec{b}_3 = \vec{b}_3 - x\vec{b}_1 = (4,5,4) - 4(1,1,1) = (0,1,0)$

Pro přehlednost: na konci kroku 2. máme:

$\vec{b}_1 = (1,1,1), \vec{b}_2 = (-1,0,2), \vec{b}_3 = (0,1,0)$

$\vec{b}_1 = (1,1,1), \vec{b}_2 = (-1,0,2), \vec{b}_3 = (0,1,0)$

$$\mu_{21} = \frac{1}{3}, \mu_{31} = \frac{(0,1,0)\cdot(1,1,1)}{\|(1,1,1)\|^2} = \frac{1}{3}, \mu_{32} = \frac{(0,1,0)\cdot\left(-\frac{4}{3},-\frac{1}{3},\frac{5}{3}\right)}{\left\|\left(-\frac{4}{3},-\frac{1}{3},\frac{5}{3}\right)\right\|^2} = -\frac{1}{14}$$

Ve 3. zkontrolujeme nerovnost, jestli není potřeba prohodit vektory.

$\|\vec{b}_2^{\,*}\|^2 = \frac{14}{3}, \|\vec{b}_3^{\,*}\|^2 = \frac{9}{14}, \|\vec{b}_2^{\,*}\|^2 > \|\vec{b}_3^{\,*}\|^2$, takže prohodíme.

Tedy: $\vec{b}_1 = (1,1,1), \vec{b}_2 = (0,1,0), \vec{b}_3 = (-1,0,2)$. Teď se vrátíme na začátek a zopakujeme Gramovu-Schmidtovu ortogonalizaci:

$$\vec{b}_1^{\,*} = \vec{b}_1 = (1,1,1)$$
$$\vec{b}_2^{\,*} = \vec{b}_2 - \mu_{21}\vec{b}_1^{\,*} = (0,1,0) - \frac{1}{3}(1,1,1) = \left(-\frac{1}{3},\frac{2}{3},-\frac{1}{3}\right)$$
$$\vec{b}_3^{\,*} = \vec{b}_3 - \mu_{31}\vec{b}_1^{\,*} - \mu_{32}\vec{b}_2^{\,*} = (-1,0,2) - \frac{1}{3}(1,1,1) + \frac{1}{2}\left(-\frac{1}{3},\frac{2}{3},-\frac{1}{3}\right) = \left(-\frac{3}{2},0,\frac{3}{2}\right)$$

Krok 2.: beze změny; zkontrolujeme, zda není třeba prohodit vektory.

$\|\vec{b}_1^{\,*}\|^2 = 3, \|\vec{b}_2^{\,*}\| = 1, \|\vec{b}_3^{\,*}\| = 5$, první je větší než druhý, takže prohodíme a opět provedeme ortogonalizaci.

$\vec{b}_1 = (0,1,0), \vec{b}_2 = (1,1,1), \vec{b}_3 = (-1,0,2)$

$$\vec{b}_1^{\,*} = \vec{b}_1 = (0,1,0)$$
$$\vec{b}_2^{\,*} = \vec{b}_2 - \mu_{21}\vec{b}_1^{\,*} = (1,1,1) - (1,0,1) = (0,1,0)$$
$$\vec{b}_3^{\,*} = \vec{b}_3 - \mu_{31}\vec{b}_1^{\,*} - \mu_{32}\vec{b}_2^{\,*} = (-1,0,2) - 0 - \frac{1}{2}(1,0,1) = \left(-\frac{3}{2},0,\frac{3}{2}\right)$$

3. krok: LLL algoritmus je dokončen, našli jsme LLL-redukovanou bázi.

Pro jistotu si ukážeme ještě jeden příklad a náš výsledek porovnáme s výsledkem, který zpracuje počítačový program.

Příklad 11: Najděte LLL-redukovanou bázi mřížky dané bázovými vektory

$\vec{b}_1 = (0,3,4), \vec{b}_2 = (-1,3,3), \vec{b}_3 = (5,4,7)$.

Řešení:

První krok: Gramova-Schmidtova ortogonalizace:

$$\vec{b}_1 = \vec{b}_1^* = (0,3,4)$$

$$\mu_{21} = \frac{\vec{b}_2 \cdot \vec{b}_1^*}{\left\|\vec{b}_1^*\right\|^2} = \frac{21}{25}$$

$$\mu_{31} = \frac{\vec{b}_3 \cdot \vec{b}_1^*}{\left\|\vec{b}_1^*\right\|^2} = -\frac{16}{25}$$

$$\vec{b}_2^* = \vec{b}_2 - \mu_{21} \cdot \vec{b}_1^* = (-1,3,3) - \frac{21}{25}(0,3,4) = (-1,3,3) - \left(0, \frac{63}{25}, \frac{84}{25}\right) = \left(-1, \frac{12}{25}, -\frac{9}{25}\right)$$

$$\mu_{32} = \frac{\vec{b}_3 \cdot \vec{b}_2^*}{\left\|\vec{b}_2^*\right\|^2} = \frac{-\frac{14}{25}}{\frac{34}{25}} = \frac{-14}{34} = -\frac{7}{17}$$

$$\vec{b}_3^* = \vec{b}_3 - \mu_{31} \cdot \vec{b}_1^* - \mu_{32} \cdot \vec{b}_2^* = (5,4,-7) - \frac{-16}{25}(0,3,4) - \frac{-7}{17}\left(-1, \frac{12}{25}, -\frac{9}{25}\right) =$$

$$= (5,4,-7) - \left(0, \frac{-48}{25}, \frac{-64}{25}\right) - \left(\frac{7}{17}, \frac{-84}{425}, \frac{63}{425}\right) = \left(\frac{-78}{17}, \frac{2432}{425}, -\frac{78}{17}\right)$$

Druhý krok:

$$i = 2, j = 1: \quad x = \left[\mu_{21}\right] = \left[\frac{21}{25}\right] = 0$$

$$i = 3, j = 2: \quad x = \left[\mu_{32}\right] = \left[-\frac{7}{17}\right] = -1 \Rightarrow \vec{b}_3 = \vec{b}_3 - x\vec{b}_2 = (4,7,-4)$$

Třetí krok: porovnáme

$$\left\|\vec{b}_1^*\right\| = 25, \left\|\vec{b}_2^*\right\| = \frac{34}{25}$$

$\left\|\vec{b}_2^*\right\| < \left\|\vec{b}_1^*\right\|$ *takže prohodíme*

Před opakováním algoritmu, rekapitulace:

$$\vec{b}_1 = (-1,3,3), \vec{b}_2 = (0,3,4), \vec{b}_3 = (4,-7,4)$$
$$\vec{b}_1 = \vec{b}_1^{\,*}, \mu_{21} = \frac{21}{19}, \mu_{31} = \frac{5}{19}$$

První krok: Gramova-Schmidtova ortogonalizace:

$$\vec{b}_2^{\,*} = \vec{b}_2 - \mu_{21} \cdot \vec{b}_1^{\,*} = (0,3,4) - \frac{21}{19}(-1,3,3) = (0,3,4) - \left(-\frac{21}{19}, \frac{63}{19}, \frac{63}{19}\right) = \left(\frac{21}{19}, -\frac{6}{19}, \frac{13}{19}\right)$$

$$\mu_{32} = \frac{\vec{b}_3 \cdot \vec{b}_2^{\,*}}{\left\|\vec{b}_2^{\,*}\right\|^2} = \frac{-\frac{10}{19}}{\frac{34}{19}} = \frac{-10}{34} = -\frac{5}{17}$$

$$\vec{b}_3^{\,*} = \vec{b}_3 - \mu_{31} \cdot \vec{b}_1^{\,*} - \mu_{32} \cdot \vec{b}_2^{\,*} = (4,7,-4) - \frac{5}{19}(-1,3,3) - \frac{-5}{17}\left(\frac{21}{19}, -\frac{6}{19}, \frac{13}{19}\right) =$$
$$= (4,7,-4) - \left(-\frac{5}{19}, \frac{15}{19}, \frac{15}{19}\right) - \left(-\frac{105}{323}, \frac{30}{323}, -\frac{65}{323}\right) = \left(\frac{78}{17}, \frac{104}{17}, -\frac{78}{17}\right)$$

Druhý krok:

$$i = 2, j = 1: \quad x = [\mu_{21}] = \left[\frac{21}{19}\right] = 1 \Rightarrow \vec{b}_2 = \vec{b}_2 - x\vec{b}_1 = (1,0,1)$$
$$i = 3, j = 2: \quad x = [\mu_{32}] = \left[-\frac{5}{17}\right] = 0$$

Třetí krok: porovnáme

$$\left\|\vec{b}_1^{\,*}\right\| = 19, \left\|\vec{b}_2^{\,*}\right\| = \frac{34}{19}$$
$$\left\|\vec{b}_2^{\,*}\right\| < \left\|\vec{b}_1^{\,*}\right\| \quad \textit{takže prohodíme}$$

Před opakováním algoritmu, opět pro pořádek provedeme rekapitulaci:

$$\vec{b}_1 = (1,0,1), \vec{b}_2 = (-1,3,3), \vec{b}_3 = (4,-7,4)$$
$$\vec{b}_1 = \vec{b}_1^{\,*}, \mu_{21} = \frac{2}{2} = 1, \mu_{31} = 0$$

První krok: Gramova-Schmidtova ortogonalizace:

$$\vec{b}_2^{\,*} = \vec{b}_2 - \mu_{21} \cdot \vec{b}_1^{\,*} = (-1,3,3) - (1,0,1) = (-2,3,2)$$

$$\mu_{32} = \frac{\vec{b}_3 \cdot \vec{b}_2^*}{\left\|\vec{b}_2^*\right\|^2} = \frac{5}{17}$$

$$\vec{b}_3^* = \vec{b}_3 - \mu_{31} \cdot \vec{b}_1^* - \mu_{32} \cdot \vec{b}_2^* = (4,7,-4) - 0(1,0,1) - \frac{5}{17}(-2,3,2) =$$
$$= (4,7,-4) - 0 - \left(-\frac{10}{17}, \frac{15}{17}, \frac{10}{17}\right) = \left(\frac{78}{17}, \frac{104}{17}, -\frac{78}{17}\right)$$

Druhý krok:

$$i = 2, j = 1: \quad x = \left[\mu_{21}\right] = \left[1\right] = 1 \Rightarrow \vec{b}_2 = \vec{b}_2 - x\vec{b}_1 = (-2,3,2)$$
$$i = 3, j = 2: \quad x = \left[\mu_{32}\right] = \left[\frac{5}{17}\right] = 0$$

Třetí krok: porovnáme

$$\left\|\vec{b}_1^*\right\| = 2, \left\|\vec{b}_2^*\right\| = 17, \left\|\vec{b}_3^*\right\| = \frac{1352}{17} \approx 79,53$$
$$\left\|\vec{b}_1^*\right\| < \left\|\vec{b}_2^*\right\|, \left\|\vec{b}_2^*\right\| < \left\|\vec{b}_3^*\right\|$$

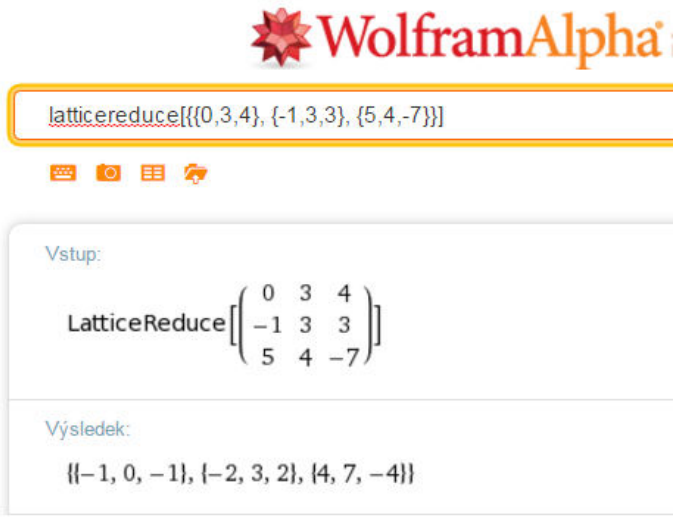
Tedy nic neprohazujeme.

Před opakováním algoritmu, opět rekapitulujeme:

$$\vec{b}_1 = (1,0,1), \vec{b}_2 = (-2,3,2), \vec{b}_3 = (4,7,-4)$$
$$\vec{b}_1 = \vec{b}_1^*, \mu_{21} = 0, \mu_{31} = 0$$

Z rekapitulace je jasné, že další opakování je zbytečné provádět. Našli jsme tedy LLL-redukovanou bázi mřížky

Stejné zadání vložíme do online matematického programu Wolfram Alfa zavoláním příkazu „latticereduce“:


WolframAlpha
latticereduce[{{0,3,4}, {-1,3,3}, {5,4,-7}}]
Vstup:
LatticeReduce[(0 3 4 ; −1 3 3 ; 5 4 −7)]
Výsledek:
{{−1, 0, −1}, {−2, 3, 2}, {4, 7, −4}}

3 OBJEVOVÁNÍ CELOČÍSELNÝCH ZÁVISLOSTÍ

Hledání celočíselných vztahů mezi čísly je jedna z aplikací LLL redukce. Několik těchto aplikací si nyní ukážeme. Bude se jednat dále o diofantické aproximace a polynomiálně rychlou závěrečnou fázi Berlekamp-Henselova algoritmu.

3.1 CELOČÍSELNÉ VZTAHY MEZI ČÍSLY

Celočíselnou závislostí mezi reálnými čísly $\alpha_1,\ldots,\alpha_n$ rozumíme rovnost

$$m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n = 0,$$

kde $m_1,\ldots,m_n$ jsou celá čísla. K nalezení takového vztahu můžeme zkusit najít krátký vektor $\vec{b}$ v mřížce $L \subseteq \mathbb{R}^{n+1}$ dané bází

$$(1,0,\ldots,0,\lfloor N\alpha_1 \rceil),(0,1,0,\ldots,0,\lfloor N\alpha_2 \rceil),\ldots,(0,1,\ldots,0,1,\lfloor N\alpha_n \rceil),$$

kde N je dostatečně velké číslo. Vektor $\vec{b}$ leží v mřížce *L*:

$$\vec{b} = m_1(1,0,\ldots,0,\lfloor N\alpha_1 \rceil) + \ldots + m_n(0,1,\ldots,0,1,\lfloor N\alpha_n \rceil) \in$$
$$\in (m_1, m_2, \ldots, m_n, N(\alpha_1 m_1 + \ldots + \alpha_n m_n))$$

Protože vektor $\vec{b}$ je krátký, tak čísla $m_1,\ldots,m_n$ nebudou příliš velká a číslo $\alpha_1 m_1 + \ldots + \alpha_n m_n$ bude celkem malé. V nejlepším případě to bude nula.

Výše popsaným způsobem lze najít řadu zajímavých vztahů, jako je například *Machinův vzorec*, pro který stačí hodnota N kolem 10 000:

$$-\pi + 16\ arctg\left(\frac{1}{5}\right) - 4\ arctg\left(\frac{1}{239}\right) = 0$$

Jiným příkladem je hledání minimálních polynomů algebraických čísel, tak že pro dané číslo β položíme $\alpha_i = \beta^i$, tak pokud takový polynom existuje a najdeme celočíselný polynom, jehož kořenem je β.

Na hledání celočíselných závislostí existují speciální algoritmy.

Jimiž jsou např. *HJLS* (Johan Håstad, Bettina Just, Jeffrey Lagarias, Claus-Peter Schnorr), r. 1896; *PSOS* (Ferguson), r. 1988; *PSLQ* (Ferguso a Bailey), r. 1992. Významným výsledkem algoritmu PSQL byla například tato rovnost:

$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k}\left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6}\right)$, která umožňuje rychle nalézt *n*-tou cifru čísla π v hexadecimální (šestnáctkové) soustavě, aniž bychom znali předchozí cifru.

Ráda bych ukázala, že se v této řadě blížíme číslu π již při malých *n* hodnotách. Využiji online matematického programu Wolfram Alfa pro výpočet:

Součet:

$$\sum_{n=0}^{1} \frac{-\frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} + \frac{4}{8n+1}}{16^n} = \frac{102\,913}{32\,760}$$

Desetinné aproximace:

3.14142246642246642246642246642246642246642246642246642246642246...

Součet:

$$\sum_{n=0}^{2} \frac{-\frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} + \frac{4}{8n+1}}{16^n} = \frac{615\,863\,723}{196\,035\,840}$$

Desetinné aproximace:

3.14158739034658152305211128740540505246387599328775799364 0...

Součet:

$$\sum_{n=0}^{3} \frac{-\frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} + \frac{4}{8n+1}}{16^n} = \frac{357\,201\,535\,487}{113\,700\,787\,200}$$

Desetinné aproximace:

3.14159245756743538183700455505729339400738995059481874897 6...

Pro číslo π je mnoho známých celočíselných vztahů, jako například zlomek $\frac{355}{113} = 3{,}14159292$, dalším zajímavým celočíselným vyjádřením čísla π je tento řetězový zlomek s pravidelnou strukturou: $\pi = 3 + \cfrac{1^2}{6 + \cfrac{3^2}{6 + \cfrac{5^2}{6 + \cfrac{7^2}{6 + \cfrac{9^2}{6 + \cfrac{11^2}{6 + \ddots}}}}}}$

3.2 DIOFANTICKÁ APROXIMACE

Pro libovolná reálná čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ a $\varepsilon \in (0,1)$ existují celá čísla $z_1, z_2, \ldots, z_n, q$ splňující:

$$\left| \frac{z_i}{q} - \alpha_i \right| \leq \frac{\varepsilon}{q} \qquad \text{pro } i = 1, \ldots, n \qquad \text{a} \qquad 1 \leq q \leq \varepsilon^{-n}.$$

Pomocí LLL algoritmu lze najít jen o něco málo horší aproximaci v polynomiálním čase.

Tvrzení 6: Existuje polynomiální algoritmus, který pro zadaná racionální čísla $r_1, r_2, \ldots, r_n$ a $0 < \varepsilon < 1$ najde celá čísla $z_1, z_2, \ldots, z_n, q$ splňující:

$$\left| \frac{z_i}{q} - \alpha_i \right| \leq \frac{\varepsilon}{q} \qquad \text{pro } i = 1, \ldots, n \qquad \text{a} \qquad 1 \leq q \leq 2^{\frac{n(n+1)}{4}} \varepsilon^{-n}$$

Důkaz:

Uvažujme mřížku $L \subseteq \mathbb{R}^{n+1}$ s bází

$$= (z_1 - \alpha_1 q, \ldots, z_n - \alpha_n q, 2^{-\frac{n(n+1)}{4}} \varepsilon^{n+1})$$

$$(1,0,\ldots,0), (0,1,\ldots,0), \ldots, (0,\ldots,0,1,0), (-\alpha_1, -\alpha_2, \ldots, -\alpha_n, 2^{-\frac{n(n+1)}{4}} \varepsilon^{n+1})$$

Pokud by poslední složka nebyla racionální, tak ji s dostatečnou přesností zaokrouhlíme na racionální číslo. Označme $\vec{b}$ aproximaci nejkratšího nenulového vektoru mřížky *L* nalezenou LLL algoritmem, tedy:

$$\vec{b} = z_1(1,0,\ldots,0) + \ldots + z_n(0,\ldots,0,1,0) + q(-\alpha_1,-\alpha_2,\ldots,-\alpha_n,2^{-\frac{n(n+1)}{4}}\varepsilon^{n+1}) =$$
$$= (z_1 - \alpha_1 q,\ldots,z_n - \alpha_n q,2^{-\frac{n(n+1)}{4}}\varepsilon^{n+1})$$

pro celá čísla $z_1, z_2,\ldots,z_n,q$, která se dají v polynomiálním čase spočítat z vektoru $\vec{b}$ jako řešení soustavy lineárních rovnic. Z tvrzení 4 dostáváme

$$\left\|\vec{b}\right\| \le 2^{\frac{n}{4}}\sqrt[n+1]{d(L)} = 2^{\frac{n}{4}}\sqrt[n+1]{2^{-\frac{n(n+1)}{4}}\varepsilon^{n+1}} = \varepsilon$$

Velikost vektoru $\vec{b}$ je nejvýše ε, takže absolutní hodnoty všech složek jsou menší než ε, což po úpravě dává nerovnosti z tvrzení.■

3.3 FAKTORIZACE CELOČÍSELNÝCH POLYNOMŮ

Nyní se dostáváme k tématu, které bylo původní motivací pro vynález LLL algoritmu. Ukážeme si, jak lze pomocí LLL algoritmu rozložit primitivní celočíselný polynom na ireducibilní faktory v polynomiálním čase.

Připomeneme princip Belekamp-Henselova algoritmu:

vstup: $f \in \mathbb{Z}[x]$ primitivní bezčtvercový polynom stupně *n*

zvolíme vhodné prvočíslo *p* a najdeme pomocí algoritmu rozklad polynomu $f \bmod p$ v oboru $\mathbb{Z}_p[x]$. Tento rozklad zdvihneme na rozklad $f \bmod m$ v oboru $\mathbb{Z}_m[x]$, kde *m* je mocnina *p*. Nyní je potřeba nalezené faktory zkombinovat tak, aby vznikl rozklad f v oboru $\mathbb{Z}[x]$, což je nejtěžší část. Pomocí LLL algoritmu lze tento krok „zpolynomiálnět“ tak, že pro daný faktor $\bmod m$ spočítáme odpovídající faktor polynomu f.

Ukážeme si myšlenku původního algoritmu z článku Lenstry, Lenstry, Lovásze, v praxi je ale algoritmus založený na této myšlence pomalý.

V roce 2002 přišel Mark van Hoeij s jiným algoritmem založeným na LLL-redukci, který je velmi rychlý a jeho varianta je aplikovaná ve většině počítačových systémů.

Nyní si zavedeme značení:

Uvažujme libovolný ireducibilní faktor $u \in \mathbb{Z}_m[x]$ polynomu $f \bmod m$ a označme d stupněm polynomu u. Následující tvrzení říká, že když najdeme *krátký* (tzn. $\|g\|^n \le m\|f\|^{-d}$) polynom $g \in \mathbb{Z}[x]$, který je modulo m dělitelný u, pak *největší společný dělitel (f, g)* je nekonstantní polynom.

Tvrzení 7: Nechť $f, g \in \mathbb{Z}[x]$ jsou polynomy stupně *n, k*, a m je přirozené číslo a $u \in \mathbb{Z}_m[x]$ je monický nekonstantní polynom, který dělí $f \bmod m$ i $g \bmod m$. Pokud $\|f\|^k \|g\|^n < m$, pak *největší společný dělitel (f, g)* je nekonstantní.

Důkaz:

Existují celočíselné polynomy s, t takové, že $res(f,g) = sf + tg$ a podíváme-li se na tento vztah modulo *m* a vezmeme v potaz, že $f \bmod m$ i $g \bmod m$ jsou dělitelné u, zjistíme, že $res(f,g) \bmod m$ je číslo dělitelné polynomem u. Protože u je nekonstantní a monický (m má typicky netriviální dělitele nuly, mocninu prvočísla), platí $res(f,g) \bmod m = 0$. Absolutní hodnotu determinantu můžeme shora odhadnout součinem velikostí řádků, tedy podle definice rezultantu

$$|res(f,g)| \le \|f\|^k \|g\|^n < m$$

Z toho plyne, že $res(\mathrm{f,g}) = 0$ a podle Sylvesterova kritéria je největší společný dělitel (f, g) nekonstantní.■

Tvrzení 8: Množina polynomů $P = \{g \in \mathbb{Z}[x] : \deg \mathrm{g} < \mathrm{j}, \mathrm{u} \mid (g \bmod m)\}$ je mřížka s bází $B = \{u, ux, \ldots, ux^{j-d-1}, m, mx, \ldots, mx^{d-1}\}$.

Důkaz:

Je jasné, že $B \subseteq P$. Ale, mějme libovolný polynom $g \in P$. Protože $u \mid (g \bmod m)$, existují polynomy $q, r \in \mathbb{Z}[x]$ takové, že $g = qu + mr$.

Dělením polynomu r polynomem u se zbytkem dostaneme $q', r' \in \mathbb{Z}[x]$ takové, že $r = q'u + r'$, $\deg r' < d$. Nyní lze psát $g = qu + m(q'u + r') = (q + mq')u + mr'$.

Srovnáním stupňů obou stran získáme $\deg(q + mq') < j - d$.■

ZÁVĚR

Cílem mé práce bylo hledání celočíselných závislostí mezi reálnými čísly. Bohužel jsem této kapitole nevěnovala tolik prostoru, jako jsem chtěla.

I přes to jsem ráda, že jsem tuto práci psala, protože jsem se seznámila s jedním matematickým velikánem, a to se Srinavasa Ramanujanem. Nikdy před tím jsem o něm neslyšela a po bádání po informacích o něm si myslím, že to byl naprosto geniální člověk. Dokázal vymyslet různé složité vzorce a měl k tomu jenom tužku a svůj proslulý zápisník.

Dále jsem se seznámila s LLL algoritmem, o kterém jsem také dříve neslyšela. K němu byla zapotřebí znalost Gramova-Schmidtova ortogonalizačního procesu, kterým jsem se také v práci zabývala. Na oba algoritmy jsem zpracovala několik příkladů.

RESUMÉ

In this thesis, I wrote three biographies of three mathematicians. Srinivasa Ramanujan, Gram and Schmidt.

I also introduced a few concepts from linear algebra that are needed to explain the Gram -Schmidt algorithm and LLL algorithm. Chapter searching integer dependencies between real numbers I unfortunately did not manage to devote as much time as I wanted.

SEZNAM LITERATURY

1) David Stanovský a Libor Barto: Počítačová algebra, Matfyzpress, ISBN: 978-80-7378-167-5
2) Ladislav Bican: Lineární algebra, Matematický seminář SNTL
3) Jindřich Bečvář: Lineární algebra, Matfyzpress, ISBN: 80-85863-92-8
4) RNDr. Ladislav Bican: Lineární algebra v úlohách, Vydala Univerzita Karlova v Praze

Internetové zdroje:

5) Biografie byly přeloženy ze stránek Mac Tutor – History of Mathematics
6) Příklady Ramanujanových řad jdoucích k $\frac{1}{\pi}$ jsou ze stránek wikipedia.org
7) Zadání jednoho příkladu na Gramův-Schmidtův ortogonalizační proces ze stránek: kolej.mff.cuni.cz