Využití pojmu Hilbertovy báze pro ověření hypotézy o shodnosti strukturálních a kombinatorických imsetů*

Petr Šimeček, Milan Studený

2. září 2004

Abstrakt

Klíčovým problémem v metodě popisu struktur podmíněné nezávislosti (mezi N náhodnými veličinami) pomocí tzv. imsetů je otevřená otázka shodnosti dvou množin celočíselných vektorů, tzv. strukturálních a kombinatorických imsetů. Tato otázka svoji povahou spadá do oblasti celočíselného programování a souvisí úzce s úlohou nalezení tzv. minimální celočíselné Hilbertovy báze pro jistý racionální konvexní kužel. Tématem tohoto příspěvku jsou počítačové experimenty, jejichž cílem je potvrdit či vyvrátit hypotézu o shodnosti těchto dvou množin vektorů. S pomocí počítače se podařilo hypotézu ověřit pro $N \leq 4$, navíc byly dosaženy částečné výsledky pro $N = 5$ a nastíněny další možné směry postupu.

Tento příspěvek se věnuje řešení klíčového problému z oblasti popisu struktur podmíněné nezávislosti (mezi N náhodnými veličinami) pomocí tzv. imsetů a to ověření hypotézy o shodnosti množin strukturálních a kombinatorických imsetů. Základní definice a většinu značení nalezne čtenář toužící po hlubším vhledu do problematiky v [1] a [2]. Zde se také nacházejí důkazy tvrzení, jež se nám zdály příliš zřejmé či naopak příliš obtížné na to, abychom je prezentovali v tomto příspěvku.

1 Základní pojmy

Zde si připomeňme alespoň základní pojmy. Nechť N je přirozené číslo (odpovídající počtu náhodných veličin).

Definice. *Imsetem rozumíme zobrazení potenční množiny $\mathcal{P}(\{1, 2, \ldots, N\})$ do množiny celých čísel $\mathbb{Z}$. Hodnotu imsetu v pro $A \subseteq \{1, 2, \ldots, N\}$ značíme $v(A)$.*

Imset lze chápat také jako celočíselný vektor v $\mathbb{R}^{2^N}$, jehož složky jsou indexovány podmnožinami $\{1, 2, \ldots, N\}$.

Definice. *Elementárním imsetem odpovídajícím nezávislosti (nezávislostnímu vztahu) mezi náhodnými veličinami X_i a X_j dáno $\{X_k; k \in C\}$, kde $\{i\}$, $\{j\}$ a C jsou po dvou disjunktní podmožiny $\{1, 2, \ldots, N\}$, budeme rozumět imset*

*Práci na tomto příspěvku byla poskytnuta podpora z grantu GA ČR 201/04/0393.

$u_{\langle i,j|C\rangle}$ *takový, že* $u_{\langle i,j|C\rangle}(\{i,j\} \cup C) = u_{\langle i,j|C\rangle}(C) = 1$, $u_{\langle i,j|C\rangle}(\{i\} \cup C) = u_{\langle i,j|C\rangle}(\{j\} \cup C) = -1$ *a zbylým prvkům potenční množiny přiřadí* $u_{\langle i,j|C\rangle}$ *nulu.*

Množinu všech elementárních imsetů budeme značit $\mathcal{E}_N$*.*

Povšimněme si, že $|\mathcal{E}_N| = \binom{N}{2} \cdot 2^{N-2}$.

Například pro $N = 3$ množinu všech elementárních imsetů $\mathcal{E}_3$ znázorňuje následující tabulka:

	$\emptyset$	**{1}**	**{2}**	**{3}**	**{1,2}**	**{1,3}**	**{2,3}**	**{1,2,3}**
$u_{\langle 1,2\|\emptyset\rangle}$	1	-1	-1	0	1	0	0	0
$u_{\langle 1,3\|\emptyset\rangle}$	1	-1	0	-1	0	1	0	0
$u_{\langle 2,3\|\emptyset\rangle}$	1	0	-1	-1	0	0	1	0
$u_{\langle 2,3\|\{1\}\rangle}$	0	1	0	0	-1	-1	0	1
$u_{\langle 1,3\|\{2\}\rangle}$	0	0	1	0	-1	0	-1	1
$u_{\langle 1,2\|\{3\}\rangle}$	0	0	0	1	0	-1	-1	1

Definice. *Množinou kombinatorických imsetů* $\mathcal{C}_N$ *budeme rozumět všechny možné součty konečně mnoha elementárních imsetů, neboli*

$$\mathcal{C}_N = \left\{ \sum_{i=1}^{k} \alpha_i u_i;\ \alpha_i \in \mathbb{N}, u_i \in \mathcal{E}_N, k \in \mathbb{N}_0 \right\}.$$

Rozklad kombinatorického imsetu na součet elementárních imsetů není jednoznačný, například platí

$$u_{\langle 1,2|\{3\}\rangle} + u_{\langle 1,3|\emptyset\rangle} = u_{\langle 1,3|\{2\}\rangle} + u_{\langle 1,2|\emptyset\rangle}.$$

Jednoznačný je však stupeň kombinatorického imsetu $v = \sum_{i=1}^{k} \alpha_i u_i$, který je definován jako $deg(v) = \sum_{i=1}^{k} \alpha_i$, neboť toto číslo – jak pozorný čtenář snadno nahlédne[1] – je rovno výrazu

$$deg(v) = \frac{1}{2} \sum_{A \subseteq \{1,\ldots,N\}} |A| \cdot (|A| - 1) \cdot v(A). \tag{1}$$

Povšimněme si, že stupeň kombinatorického imsetu je lineární forma. Navíc pomocí formule (1) můžeme rozšířit definici stupně $deg(v)$ na libovolný (nejen kombinatorický) imset v.

Dále můžeme nahlédnout, že jediný kombinatorický imset stupně nula je nulový imset a kombinatorické imsety stupně jedna jsou právě elementární imsety.

Definice. *Množinou strukturálních imsetů* $\mathcal{S}_N$ *budeme rozumět všechny imsety, jež lze vyjádřit jako nezápornou reálnou*[2] *kombinaci konečně mnoha elementárních imsetů, neboli*

$$\mathcal{S}_N = \left\{ \sum_{i=1}^{k} \alpha_i u_i \in \mathbb{Z}^{\mathcal{P}(\{1,2,\ldots,N\})};\ \alpha_i \in \mathbb{R}^+, u_i \in \mathcal{E}_N, k \in \mathbb{N}_0 \right\}.$$

[1] Stačí dokázat, rovnost (1) platí pro všechny elementární imsety, a ukázat, že takto definovaný stupeň je lineární forma.

[2] Lze ukázat, že pokud slovo „reálnou“ nahradíme slovem „racionální“, dostaneme ekvivalentní definici.

Stupeň strukturálního imsetu je celé číslo, jak je možno snadno nahlédnout z formule (1).

Povšimněme si, že u imsetu nízkého stupně je poměrně snadné rozhodnout, zda je kombinatorický. Na druhé straně otázka, zda-li je či není strukturální, je mnohem obtížnější. I z tohoto, avšak nejen z tohoto důvodu[3] je zajímavá otázka, zda náhodou neplatí, že pro všechna N nastává rovnost $\mathcal{C}_N = \mathcal{S}_N$.

Tento příspěvek si neklade za cíl tuto otázku teoreticky rozřešit. Pouze ji zodpovíme pro dostatečně nízká N a formulujeme tvrzení, jež mohou být základem dalšího bádání. Úhelným kamenem dalšího postupu bude pojem minimální celočíselné Hilbertovy báze.

2 Pojem minimální celočíselné Hilbertovy báze

Definice. *Každý konvexní kužel K v $\mathbb{R}^n$ kónicky generovaný konečnou množinou celočíselných vektorů obsahuje tzv. minimální celočíselnou Hilbertovu bázi, což je množina celočíselných vektorů $w_1, \ldots, w_m$ z K taková, že*

$$\forall x \in K \cap \mathbb{Z}^n \ \exists(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m : \quad x = \sum_{i=1}^{m} \alpha_i w_i.$$

Tento pojem jsme přejali z knihy [4], kde je dokázáno, že tato definice je konzistentní, a tamtéž je na straně 233 v důkazu věty 16.4 ukázáno, že pokud $e_1, \ldots, e_l$ jsou generátorem výše zmíněného kužele, pak minimální celočíselnou Hilbertovu bázi stačí hledat v mnohostěnu $\mathcal{M}$ tvořeném body

$$\mathcal{M} = \left\{ \sum_{i=1}^{l} \lambda_i e_i; \ \lambda_i \in [0, 1] \right\}.$$

Pakliže výše zmíněnou metodu aplikujeme na náš případ, zjistíme, že otázka, zda $\mathcal{C}_N = \mathcal{S}_N$, je ekvivalentní s otázkou, zda minimální celočíselná Hilbertova báze kužele generovaného $\mathcal{E}_N$ (jeho celočíselné body jsou $\mathcal{S}_N$) je rovna $\mathcal{E}_N$ (přičemž zjevně $\mathcal{E}_N$ obsahuje).

Protože rozhodnout, zda daný bod patří či nepatří do mnohostěnu $\mathcal{M}$ a tedy i nalézt všech body mnohostěnu $\mathcal{M}$ je v praxi obtížné, volíme postup pro nalezení Hilbertovy báze pro dané N následovně:

1. Zavedeme „vhodný“ obal $\mathcal{O}$ mnohostěnu $\mathcal{M}$. Vhodný v tomto kontextu znamená, že počítač dokáže rychle rozhodnout, zda daný imset do $\mathcal{O}$ patří či nikoli, a že dokáže v reálném čase prohledat všechny imsety v $\mathcal{O}$ obsažené.

2. Postupně volíme n od jedné do $|\mathcal{E}_N| = \binom{N}{2} \cdot 2^{N-2}$. Procházíme všechny imsety z $\mathcal{O}$ mající stupeň n, u každého z nich rozhodneme, zda jej lze zapsat jako součet nějakého imsetu stupně $n-1$ (ty už máme vyhledané v minulém kroku a uložené v paměti) a nějakého elementárního imsetu. Pokud ano, pokračujeme, pokud ne, nalezli jsme prvek $\mathcal{O}$, jehož zápis ve tvaru nezáporné celočíselné kombinace prvků $\mathcal{E}_N$ je „problematický“.

[3]Ověření této hypotézy má zásadní vliv na počítačovou implementaci inferenčního mechanismu.

3. Pokud algoritmus skončí a žádný „problematický“ imset nenalezne, můžeme učinit závěr, že $\mathcal{C}_N = \mathcal{S}_N$. Pokud jej nalezne, nemusí být závěr jednoznačný, záleží na „obalení“ mnohostěnu $\mathcal{M}$ pomocí $\mathcal{O}$.

Obtíže nastanou již u prvního bodu výše uvedeného scénáře. Pokud jako obal použijeme kužel generovaný prvky $\mathcal{E}_N$, můžeme tento popsat jako průnik jistých poloprostorů[4]. Postup jejich hledání s využitím Fourier-Motzkinovy transformace za pomoci programu PORTA je popsán v [3]. Tento postup však díky jeho obrovské výpočetní složitosti můžeme použít jen pro $N \leq 5$, kdy pro N rovno třem, čtyřem a pěti potřebujeme po řadě 5, 37 a 117 978 nadrovin udávajících výše zmíněné poloprostory. Proto se nadále budeme soustředit pouze na případ $N \leq 5$.

Tento kužel zcela jistě obsahuje mnohostěn $\mathcal{M}$, přičemž můžeme jistě jako obal $\mathcal{O}$ brát pouze takové jeho imsety v, že $\forall A \subseteq \{1, \ldots, N\} : \ |v(A)| \leq deg(v)$.

3 Výsledky počítačových experimentů

Dále rozebereme výsledky našeho výzkumu pro různá N:

$N = 3$:

Použili jsme výše zmíněný postup a v několika málo sekundách sekundách se podařilo ověřit, že $\mathcal{C}_3 = \mathcal{S}_3$.

$N = 4$:

Zde již bylo nutné postupovat mnohem opatrněji. Za prvé si lze všimnout, že pro libovolný strukturální imset v platí

$$\sum_{A \subseteq \{1,\ldots,N\}} v(A) = 0,$$

a také že pro každé $i \in \{1, \ldots, N\}$ platí

$$\sum_{A \subseteq \{1,\ldots,N\},\ i \in A} v(A) = 0.$$

Díky těmto dvěma vlastnostem stačí strukturální imset reprezentovat pomocí jeho hodnot pro $A \subseteq \{1, \ldots, N\} : |A| \geq 2$, neboť hodnoty pro $A \subseteq \{1, \ldots, N\} : |A| \leq 1$ jsou již těmito jednoznačně určeny. Tím se nám dimenze problému snižuje o $N + 1$, přičemž se nijak nekomplikuje výpočet stupně.

Užitečné je též uvědomit si, že imsety z mnohostěnu $\mathcal{M}$ nabývají pro $A \subseteq \{1, \ldots, N\} : |A| = 2$ hodnot od -4 do 2, pro $|A| = 3$ hodnot od -3 do 3 a pro $|A| = 4$ hodnot od 0 do 6. Stačí se tedy omezit se na takovéto imsety. Tato změna je o to významnější, že nám umožní změnit meze do sebe vnořených $11 = 2^4 - (4 + 1)$ for–cyklů.

Dále je důležité vhodně zvolit datové typy, aby výpočet nebyl příliš náročný na paměť, a v bodě 2 výše zmíněného scénáře šikovně implementovat vyhledávání v imsetech stupně $n - 1$ za pomoci jejich setřízení a hašovací tabulky, jinak

[4] odvozených od jeho stěn nebo chcete-li od extremálních paprsků duálního kužele neboli tzv. „skeletonu“.

úloha neskončí v reálném čase. Zdrojový kód pro GNU Pascal je možné nalézt na adrese:

`http://5r.matfyz.cz/ctyri.pas.`

Výpočet na stroji Artax s procesorem Intel Pentium 4 HT 2800 MHz a 1 GB paměti trval 12 minut, přičemž bylo využito 530 MB operační paměti.

$N = 5$:

Zde jsme sice využili další zmenšení obalu $\mathcal{O}$ založené na tom, že každý strukturální imset v musí zjevně splňovat

$$\sum_{A\subseteq\{1,\ldots,N\}} (v(A))^+ \leq 2\, deg(v), \qquad \sum_{A\subseteq\{1,\ldots,N\}} (v(A))^- \leq 2\, deg(v).$$

A také, že pro libovolnou $B \subset \{1,\ldots,N\}$ musí platit

$$\sum_{A:\ B\subseteq A\subseteq\{1,\ldots,N\}} v(A) \geq 0,$$

nicméně i při této redukci jsme byli schopni vyšetřit jen imsety stupně nejvýše čtyři, přičemž výpočet trval necelé tři dny. Program je k nahlédnutí na adrese

`http://5r.matfyz.cz/pet.tar.gz.`

4 Myšlenka fixovaného stupně

Nadějným směrem dalšího možného postupu je namísto „obalování" celého mnohostěnu $\mathcal{M}$ aproximovat průniky $\mathcal{M}$ s množinou imsetů daného stupně n. Lze totiž ukázat:

Věta. *Nechť v je strukturální imset stupně $deg(v) = n$ z mnohostěnu*

$$\mathcal{M} = \left\{ \sum_{e_i\in\mathcal{E}_N} \lambda_i e_i;\ \lambda_i \in [0,1] \right\},$$

potom tento imset náleží i do mnohostěnu, jenž je konvexním obalem množiny všech součtů n různých elementárních imsetů neboli množiny

$$\mathcal{B}_n = \left\{ v = \sum_{e_i\in D}^{n} e_i;\ D \subseteq \mathcal{E}_N, |D| = n \right\}.$$

Důkaz. Dokážeme nejprve pomocné tvrzení, že každý bod r–rozměrné jednotkové krychle, jehož součet souřadnic je $n \in \mathbb{N}_0$, je konvexní kombinací bodů z krychle o souřadnicích $(s_1,\ldots,s_r)$ takových, že $\forall i : s_i \in \{0,1\}$ a $s_1 + s_2 + \cdots + s_r = n$. Pokud toto tvrzení platí, pak po dosazení $r = |\mathcal{E}_N|$, koeficienty λ_i použité v $\mathcal{M}$ definují příslušný bod krychle a prohozením příslušných sum snadno nahlédneme požadovaný závěr.

Pomocné tvrzení dokážeme indukcí podle r zároveň pro všechna přípustná n: pro $r \leq 2$ tvrzení evidentně platí. Předpokládáme-li platnost tvrzení pro všechna $r' < r$, pak jeho platnost pro r (a libovolné n) dokážeme nejprve pro body na stěnách krychle. Vezměme si tedy libovolnou stěnu krychle, bez újmy na obecnosti tedy třeba tu s pevnou první souřadnicí $s_1 = 0$, respektive $s_1 = 1$. Tedy má-li mít bod na této stěně součet souřadnic n, musí být součet druhé až r–té souřadnice roven n, respektive $n-1$, a indukční předpoklad nám zaručuje, že takovýto bod již bude požadovanou konvexní kombinací.

Zbývá totéž dokázat o bodech uvnitř krychle. Ale každý takový bod je konvexní kombinací dvou bodů, pro něž platnost tvrzení již byla nahlédnuta. Vskutku ke každému bodu uvnitř krychle můžeme přičíst i odečíst vhodný násobek vektoru $\left(1, \frac{1}{r-1}, \ldots, \frac{1}{r-1}\right)$ tak, že dostaneme body ležící na stěnách krychle, z kterých lze tento bod nakombinovat. $\square$

Problémem, na který opět narážíme, je obrovská výpočetní složitost. Ukazuje se, že asi nebude možné najít přesný popis konvexního uzávěru $\mathcal{B}_n$ ve tvaru průniku poloprostorů, ale spíše nějakou jeho vnější aproximaci.

5 Závěr

Podařilo se nám hypotézu, že $\mathcal{C}_N = \mathcal{S}_N$ ověřit pro $N \leq 4$.

Problém pro $N = 5$ nadále zůstává otevřený a uvítáme náměty či rady, jak postupovat při jeho řešení. Zatím je známo pouze to, že pakliže existuje prvek minimální celočíselné Hilbertovy báze $\mathcal{S}_5$ neobsažený v $\mathcal{E}_5$, pak má tento prvek stupeň ostře vyšší než 4.

Nadějné se zdá být hledání imsetů v mnohostěnech pro jednotlivé stupně, které však zatím naráží na příliš vysokou časovou náročnost.

Reference

[1] Studený M. (2001): *On mathematical description of probabilistic conditional independence structures*, doktorská práce, ÚTIA AV ČR.

[2] Studený M. (2005): *On Probabilistic Conditional Independence Structures*, Springer.

[3] Studený M., Bouckaert R.R., Kočka T. (2000): *Extreme supermodular set functions over five variables*, výzkumná zpráva číslo 1977, ÚTIA AV ČR.

[4] Schrijver A., (1998): *Theory of Linear and Integer Programming*, John Wiley.