Peanovské součiny a deskriptivní analýza lineárních teorií

Petr Glivický

petrglivicky@gmail.com

Výjezdní zasedání KTIML 2012

Content

Co děláme

- Zabýváme se modely Peanovy aritmetiky (PA) zejména s ohledem na možnosti jejich „konstrukce“.
- Cíl (vzdálený): metoda prokazování konzistencí v aritmetice.

Co děláme

- Zabýváme se modely Peanovy aritmetiky (PA) zejména s ohledem na možnosti jejich „konstrukce“.
- Cíl (vzdálený): metoda prokazování konzistencí v aritmetice.
- Žádný nestandardní model PA nelze zkonstruovat v pravém slova smyslu.
- Tennenbaumova věta: V každém spočetném nestandardním modelu PA jsou součet i součin nerekurzivní.

Náš přístup

Principy:

- fixovaná aditivní část:
  - Na saturovaném modelu $\mathcal{M}_+$ Presburgerovy aritmetiky (Pr) existuje pro každou kompletní extenzi $S \supset$PA součin $\cdot_S$ s $\langle \mathcal{M}_+, \cdot_S \rangle \models S$.
  - Namísto celých modelů PA konstruujeme pouze „peanovské součiny“ na jednom pevně zvoleném saturovaném modelu Pr.

Náš přístup

Principy:

- fixovaná aditivní část:
  - Na saturovaném modelu $\mathcal{M}_+$ Presburgerovy aritmetiky (Pr) existuje pro každou kompletní extenzi $S \supset$PA součin $\cdot_S$ s $\langle \mathcal{M}_+, \cdot_S \rangle \models S$.
  - Namísto celých modelů PA konstruujeme pouze „peanovské součiny“ na jednom pevně zvoleném saturovaném modelu Pr.
- lokální pohled:
  - Předepíšeme-li hodnoty součinu v nějakých bodech, jaká omezení na možné hodnoty v jiných bodech si vynutí požadavek peanovskosti?

Peanovská nezávislost

Mějme $\langle \mathcal{M}_+, \cdot \rangle \models \mathrm{PA}$ saturovaný a $X = \{(x_i, y_i); i \in I\} \subseteq M^2$.

Otázka

Pro jaké body $(a, b) \in M^2$ existuje peanovský součin $\circ$ shodující se s $\cdot$ na X a lišící se v (a, b)?

Peanovská nezávislost

Mějme $\langle \mathcal{M}_+, \cdot \rangle \models \mathrm{PA}$ saturovaný a $X = \{(x_i, y_i); i \in I\} \subseteq M^2$.

Otázka

Pro jaké body $(a, b) \in M^2$ existuje peanovský součin $\circ$ shodující se s $\cdot$ na X a lišící se v (a, b)?

Takový bod (a, b) pak nazýváme peanovsky nezávislý na X (vzhledem k $\cdot$). Definujeme i jiné druhy nezávislosti než peanovskou.

Peanovská nezávislost

Je-li $|X| < |M|$ není těžké dokázat následující:

Tvrzení (o nezávislosti)

(a, b) je $\cdot$-izomorfně nezávislý na $X \Leftrightarrow a \cdot b$ není skorouniformně definovatelný v $\mathcal{M}_+$ z parametrů $a, b, x_i, y_i, x_i \cdot y_i$, $i \in I$.

Peanovská nezávislost

Je-li $|X| < |M|$ není těžké dokázat následující:

Tvrzení (o nezávislosti)

(a, b) je $\cdot$-izomorfně nezávislý na $X \Leftrightarrow a \cdot b$ není skorouniformně definovatelný v $\mathcal{M}_+$ z parametrů $a, b, x_i, y_i, x_i \cdot y_i$, $i \in I$.

Odtud plyne kritérium: Nechť alespoň jeden z prvků a, b není tvaru $L(\overline{z})$, kde L je lineární forma s koeficienty v $\mathbb{Q}$ a každé z_j je mezi $a, b, x_i, y_i, x_i \cdot y_i$, $i \in I$. Pak (a, b) je peanovsky nezávislý na X.

Peanovská nezávislost

Je-li $|X| < |M|$ není těžké dokázat následující:

Tvrzení (o nezávislosti)

(a, b) je $\cdot$-izomorfně nezávislý na $X \Leftrightarrow a \cdot b$ není skorouniformně definovatelný v $\mathcal{M}_+$ z parametrů $a, b, x_i, y_i, x_i \cdot y_i$, $i \in I$.

Odtud plyne kritérium: Nechť alespoň jeden z prvků a, b není tvaru $L(\overline{z})$, kde L je lineární forma s koeficienty v $\mathbb{Q}$ a každé z_j je mezi $a, b, x_i, y_i, x_i \cdot y_i$, $i \in I$. Pak (a, b) je peanovsky nezávislý na X.

Podstatnou roli při jakékoli aplikaci tvrzení hraje znalost eliminační množiny v $Pr \models \mathcal{M}_+$.

Peanovská nezávislost

Pokud $|X| = |M|$, je v některých případech možné rozdělit X na $X = Y \cup Z$, $Z = \{(x_i, y_i); i \in I'\}$ tak, že $|Z| < |M|$ a $\cdot \restriction Y$ lze „zakódovat“ do struktury $\mathcal{F} = \langle \mathcal{M}_+, \ldots \rangle$ (fixátor $\cdot$ na Y).

Peanovská nezávislost

Pokud $|X| = |M|$, je v některých případech možné rozdělit X na $X = Y \cup Z$, $Z = \{(x_i, y_i); i \in I'\}$ tak, že $|Z| < |M|$ a $\cdot \restriction Y$ lze „zakódovat“ do struktury $\mathcal{F} = \langle \mathcal{M}_+, \ldots \rangle$ (fixátor $\cdot$ na Y). Pak platí:

Tvrzení (druhé o nezávislosti)

(a, b) je $\cdot$-izomorfně nezávislý na $X \Leftrightarrow a \cdot b$ není skorouniformně definovatelný v $\mathcal{F}$ z parametrů $a, b, x_i, y_i, x_i \cdot y_i$, $i \in I'$.

Pro aplikaci tvrzení je nutné znát eliminační množinu $\mathcal{F}$.

Potkavší se dvojice

Definice

Nechť $\mathcal{M}_+ \models \mathrm{Pr}\ a\ (\cdot, \circ)$ *je dvojice peanovských se součinů na* M. *Říkáme, že* $(\cdot, \circ)$ *je potkavší se dvojice s bodem setkání* $a \in M$, *pokud v* $\langle \mathcal{M}_+, \cdot, \circ \rangle$ *platí* $(\forall x)(a \cdot x = a \circ x)$ a $(\exists c, d < a)(c \cdot d \neq c \circ d)$.

Potkavší se dvojice

Definice

Nechť $\mathcal{M}_+ \models \mathrm{Pr}$ *a* $(\cdot, \circ)$ *je dvojice peanovských se součinů na* M. *Říkáme, že* $(\cdot, \circ)$ *je potkavší se dvojice s bodem setkání* $a \in M$, *pokud v* $\langle \mathcal{M}_+, \cdot, \circ \rangle$ *platí* $(\forall x)(a \cdot x = a \circ x)$ *a* $(\exists c, d < a)(c \cdot d \neq c \circ d)$.

Potkavší se dvojice umožňují konstrukci nových součinů s jistou mírou indukce.

Konkrétně indukce pro (ko)omezeně lineární formule, tj. formule $\psi(x)$ takové, že v každém součinu je jeden z činitelů x a všechny kvantifikace jsou (ko)omezené do x.

Potkavší se dvojice

Věta

Nechť $\mathcal{M} = \langle \mathcal{M}_+, \cdot \rangle$ je saturovaný model PA, $a \in M \setminus \mathbb{N}$. Pak existuje peanovský součin $\circ$ na $\mathcal{M}_+$ takový, že $(\cdot\,, \circ)$ je potkavší se dvojice s bodem setkání a.

Potkavší se dvojice

Věta

Nechť $\mathcal{M} = \langle \mathcal{M}_+, \cdot \rangle$ je saturovaný model PA*, $a \in M \setminus \mathbb{N}$. Pak existuje peanovský součin $\circ$ na $\mathcal{M}_+$ takový, že $(\cdot\,, \circ)$ je potkavší se dvojice s bodem setkání a.*

Problém je ekvivalentní s otázkou, zda existují $c, d < a$ taková, že (c, d) je peanovsky nezávislý na $X_a = \{(a, m); m \in M\}$. Je $|X_a| = |M|$ a $\mathcal{F} = \langle \mathcal{M}_+, \_ \cdot a \rangle$ je fixátorem pro X_a.

Potkavší se dvojice

Věta

Nechť $\mathcal{M} = \langle \mathcal{M}_+, \cdot \rangle$ je saturovaný model PA*, $a \in M \setminus \mathbb{N}$. Pak existuje peanovský součin $\circ$ na $\mathcal{M}_+$ takový, že $(\cdot\,, \circ)$ je potkavší se dvojice s bodem setkání a.*

Problém je ekvivalentní s otázkou, zda existují $c, d < a$ taková, že (c, d) je peanovsky nezávislý na $X_a = \{(a, m); m \in M\}$. Je $|X_a| = |M|$ a $\mathcal{F} = \langle \mathcal{M}_+, \_ \cdot a \rangle$ je fixátorem pro X_a.

Aplikací druhého tvrzení o nezávislosti lze úlohu převést na problém eliminace kvantifikátorů v $\mathcal{F}$. Eliminace v $\mathcal{F}$ je přitom důsledkem eliminace kvantifikátorů v tzv. lineárních teoriích.

Lineární teorie

Doded je diskrétně uspořádaný, regulárně kvazieuklidovský obor integrity mající stupně.

Lineární teorie

Doded je diskrétně uspořádaný, regulárně kvazieuklidovský obor integrity mající stupně.

Lineál je struktura tvaru $\mathcal{F} = \langle F, 0, 1, +, -, \leq, c, r, q^{-1} \rangle_{C_\mathcal{F}, D_\mathcal{F}, {}^+D_\mathcal{F}}$, kde $D_\mathcal{F}$ je doded a $\mathcal{F}$ i $\mathcal{F}|C_\mathcal{F}$ jsou uspořádané $D_\mathcal{F}$-moduly (přesněji jejich expanze).

Lineární teorie

Doded je diskrétně uspořádaný, regulárně kvazieuklidovský obor integrity mající stupně.

Lineál je struktura tvaru $\mathcal{F} = \langle F, 0, 1, +, -, \leq, c, r, q^{-1} \rangle_{C_\mathcal{F}, D_\mathcal{F}, {}^+D_\mathcal{F}}$, kde $D_\mathcal{F}$ je doded a $\mathcal{F}$ i $\mathcal{F}|C_\mathcal{F}$ jsou uspořádané $D_\mathcal{F}$-moduly (přesněji jejich expanze).

Lineární teorie je taková, jejíž každý model je ekvidefinovatelný s nějakým lineálem (na témže nosiči).

Lineární teorie

Doded je diskrétně uspořádaný, regulárně kvazieuklidovský obor integrity mající stupně.

Lineál je struktura tvaru $\mathcal{F} = \langle F, 0, 1, +, -, \leq, c, r, q^{-1} \rangle_{C_\mathcal{F}, D_\mathcal{F}, {}^+D_\mathcal{F}}$, kde $D_\mathcal{F}$ je doded a $\mathcal{F}$ i $\mathcal{F}|C_\mathcal{F}$ jsou uspořádané $D_\mathcal{F}$-moduly (přesněji jejich expanze).

Lineární teorie je taková, jejíž každý model je ekvidefinovatelný s nějakým lineálem (na témže nosiči).

Příklady: teorie $\mathbb{Z}$-grup (aditivní aritmetika), 1-lineární aritmetika, teorie uspořádaných D-modulů s D dodedem (např. $\mathbb{Z}$, $R_\tau \subseteq \mathbb{Q}[x]$)

Eliminace kvantifikátorů v lineárních teoriích

Nechť T je lineární teorie, $\mathcal{F}_{\mathcal{A}}$ je (nějaký) lineál ekvidefinovatelný s $\mathcal{A} \models T$ a C, F jsou množiny všech definic nových konstantních resp. všech symbolů z lineálů $\mathcal{F}_{\mathcal{A}}$ s $\mathcal{A} \models T$.

Eliminace kvantifikátorů v lineárních teoriích

Nechť T je lineární teorie, $\mathcal{F}_{\mathcal{A}}$ je (nějaký) lineál ekvidefinovatelný s $\mathcal{A} \models T$ a C, F jsou množiny všech definic nových konstantních resp. všech symbolů z lineálů $\mathcal{F}_{\mathcal{A}}$ s $\mathcal{A} \models T$.

T^C resp. T^F značí extenzi T o definice z C resp. F.

Eliminace kvantifikátorů v lineárních teoriích

Nechť T je lineární teorie, $\mathcal{F}_{\mathcal{A}}$ je (nějaký) lineál ekvidefinovatelný s $\mathcal{A} \models T$ a C, F jsou množiny všech definic nových konstantních resp. všech symbolů z lineálů $\mathcal{F}_{\mathcal{A}}$ s $\mathcal{A} \models T$.

T^C resp. T^F značí extenzi T o definice z C resp. F.

Věta

Pro každou formuli $\varphi(x, \overline{y})$ jazyka T^F existuje konečně mnoho termů $t_i(\overline{y})$, $i < n$, takových, že platí:

$$T \vdash (\exists x)\varphi(x, \overline{y}) \to \bigvee_{i<n} \varphi(t_i(\overline{y}), \overline{y}).$$

Eliminace kvantifikátorů v lineárních teoriích

Důsledek

T^F má eliminaci kvantifikátorů a je otevřeně axiomatizovatelná.

Eliminace kvantifikátorů v lineárních teoriích

Důsledek

T^F má eliminaci kvantifikátorů a je otevřeně axiomatizovatelná.

Důsledek

1) $C_{\mathcal{F}_\mathcal{A}}$ je (jakožto podstruktura $\mathcal{A}$) prvomodelem teorie $Th(\mathcal{A})$.
2) Jednoduché kompletní extenze T jsou jednoznačně určeny atomickými sentencemi jazyka T^F, které v nich platí.

Eliminace kvantifikátorů v lineárních teoriích

Důsledek

T^F má eliminaci kvantifikátorů a je otevřeně axiomatizovatelná.

Důsledek

1) $C_{\mathcal{F}_\mathcal{A}}$ je (jakožto podstruktura $\mathcal{A}$) prvomodelem teorie $Th(\mathcal{A})$.
2) Jednoduché kompletní extenze T jsou jednoznačně určeny atomickými sentencemi jazyka T^F, které v nich platí.

Důsledek

1) Každá funkce definovatelná v $\mathcal{A} \models T$ je realizací nějakého po částech termu jazyka T^F s parametry z A.
2) Každá definovatelná množina v $\mathcal{A} \models T$ je sjednocením lineárních obrazů mnohostěnů s vrcholy v $(C_{\mathcal{F}_\mathcal{A}}/D_{\mathcal{F}_\mathcal{A}})^n$ pro nějaké n.

Metoda důkazu

Důkaz věty je založen na kalkulu termů jazyka T^F zobecňujícím kalkulus řetězových zlomků.

Metoda důkazu

Důkaz věty je založen na kalkulu termů jazyka T^F zobecňujícím kalkulus řetězových zlomků.
Dva hlavní motivy důkazu jsou:

- Geometrický: Každá křivka $y = r^{-1}(qx)$ v F^2 pro $q, r \in D_{\mathcal{F}}$ je parametrizována jistou dvojicí forem definovaných na n-rozměrné „spirále“, kde n je délka řetězového zlomku $\frac{q}{r}$.
  Analogie s eliptickými křivkami.

Metoda důkazu

Důkaz věty je založen na kalkulu termů jazyka T^F zobecňujícím kalkulus řetězových zlomků.
Dva hlavní motivy důkazu jsou:

- Geometrický: Každá křivka $y = r^{-1}(qx)$ v F^2 pro $q, r \in D_{\mathcal{F}}$ je parametrizována jistou dvojicí forem definovaných na n-rozměrné „spirále“, kde n je délka řetězového zlomku $\frac{q}{r}$. Analogie s eliptickými křivkami.
- Fourierovský: Každý term t jazyka T^F lze vyjádřit ve tvaru $t(x) = \sum q_i(r_i^{-1}x) + N(x)$, kde $q_i(r_i^{-1}x)$ jsou „harmonické funkce“ a $N(x)$ je „šum“.

Aplikace

Přímou aplikací uvedených výsledků je deskriptivní analýza modelů lineární aritmetiky, tj. struktur tvaru $\mathcal{N} = \langle N, +, a \cdot \_ \rangle$. To lze chápat jako příspěvek k probíhajícímu výzkumu deskriptivní složitosti expanzí $\langle \mathbb{N}, +, \ldots \rangle$ aditivní struktury přirozených čísel $\langle \mathbb{N}, + \rangle$.

Aplikace

Přímou aplikací uvedených výsledků je deskriptivní analýza modelů lineární aritmetiky, tj. struktur tvaru $\mathcal{N} = \langle N, +, a \cdot \_ \rangle$. To lze chápat jako příspěvek k probíhajícímu výzkumu deskriptivní složitosti expanzí $\langle \mathbb{N}, +, \ldots \rangle$ aditivní struktury přirozených čísel $\langle \mathbb{N}, + \rangle$.

Termy t_i ze znění hlavní věty je možné nalézt algoritmicky. Toho je možné využít pro tvorbu algoritmů řešících úlohy jako „existence a nalezení mřížového bodu v mnohostěnu“, „nalezení projekce (stínu) mřížky“ a jiné.

Další výsledky

Vedlejším produktem důkazu eliminace kvantifikátorů v lineárních teoriích byla konstrukce 2^{ω} neizomorfních oborů integrity (volitelně PID nebo non-UFD), které jsou ω-stage euklidovské ale nejsou k-stage euklidovské pro žádné $k \in \omega$ [1]. Pokud víme, žádný takový obor nebyl dosud znám.

[1] P. Glivický, J. Šaroch, *Quasi-Euclidean subrings of* $\mathbb{Q}[x]$, přijato do Communications in Algebra.

Poděkování

Děkuji za pozornost.