Div divů

Petr Glivický

petrglivicky@gmail.com

Výjezdní zasedání KTIML 2010

Content

Motivace

- Pohybujeme se ve světě Peanovy aritmetiky (PA) (= teorie konečných množin).

Motivace

- Pohybujeme se ve světě Peanovy aritmetiky (PA) (= teorie konečných množin).
- Stejně jako teorie (nekonečných) množin (ZF), je PA neúplná, rekurzivně nezúplnitelná, má 2^{ω} různých kompletních rozšíření.

Motivace

- Pohybujeme se ve světě Peanovy aritmetiky (PA) (= teorie konečných množin).
- Stejně jako teorie (nekonečných) množin (ZF), je PA neúplná, rekurzivně nezúplnitelná, má 2^{ω} různých kompletních rozšíření.
- Narozdíl od ZF je známo jen několik nezávislých tvrzení v PA. Žádné z nich není aritmeticky zajímavé (tj. např. hovořící o prvočíslech či diofantických rovnicích).

Motivace

- Pohybujeme se ve světě Peanovy aritmetiky (PA) (= teorie konečných množin).
- Stejně jako teorie (nekonečných) množin (ZF), je PA neúplná, rekurzivně nezúplnitelná, má 2^{ω} různých kompletních rozšíření.
- Narozdíl od ZF je známo jen několik nezávislých tvrzení v PA. Žádné z nich není aritmeticky zajímavé (tj. např. hovořící o prvočíslech či diofantických rovnicích).
- **Vzdálený cíl:** vytvořit metodu pro prokazování konzistencí v Peanově aritmetice.

Na jednom modelu Presburgerovy aritmetiky (Pr) může existovat mnoho různých peanovských součinů:

Na jednom modelu Presburgerovy aritmetiky (Pr) může existovat mnoho různých peanovských součinů:

Tvrzení (GCH)

Saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ nespočetné regulární kardinality lze (vhodnou realizací operace $\cdot$) expandovat do (saturovaného) modelu každého bezesporného rozšíření PA v jazyce L.

Na jednom modelu Presburgerovy aritmetiky (Pr) může existovat mnoho různých peanovských součinů:

Tvrzení (GCH)

Saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ nespočetné regulární kardinality lze (vhodnou realizací operace $\cdot$) expandovat do (saturovaného) modelu každého bezesporného rozšíření PA *v jazyce L.*

Tvrzení

Spočetný rekurzivně saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ lze expandovat do modelu každého bezesporného rekurzivního rozšíření PA *v jazyce L.*

Na jednom modelu Presburgerovy aritmetiky (Pr) může existovat mnoho různých peanovských součinů:

Tvrzení (GCH)

Saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ nespočetné regulární kardinality lze (vhodnou realizací operace $\cdot$) expandovat do (saturovaného) modelu každého bezesporného rozšíření PA *v jazyce L.*

Tvrzení

Spočetný rekurzivně saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ lze expandovat do modelu každého bezesporného rekurzivního rozšíření PA *v jazyce L.*

Jaká je struktura systému peanovských součinů na daném modelu?

Na jednom modelu Presburgerovy aritmetiky (Pr) může existovat mnoho různých peanovských součinů:

Tvrzení (GCH)

Saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ nespočetné regulární kardinality lze (vhodnou realizací operace $\cdot$) expandovat do (saturovaného) modelu každého bezesporného rozšíření PA *v jazyce L.*

Tvrzení

Spočetný rekurzivně saturovaný model $\mathcal{M}_+ \models \mathrm{Pr}$ lze expandovat do modelu každého bezesporného rekurzivního rozšíření PA *v jazyce L.*

Jaká je struktura systému peanovských součinů na daném modelu? Speciálně, které hodnoty peanovského součinu jsou na sobě (ne)závislé?

Potkavší se dvojice

Otázka

Shodují-li se hodnoty dvou peanovských součinů na nějaké podmnožině modelu, kde všude se již nutně musí také shodovat, kde se mohou lišit?

Potkavší se dvojice

Otázka

Shodují-li se hodnoty dvou peanovských součinů na nějaké podmnožině modelu, kde všude se již nutně musí také shodovat, kde se mohou lišit?

Snadno se ukáže následující:

Tvrzení

Existuje model $\mathcal{M}_+ \models \mathrm{Pr}$ *s prvky* $c, d > a > \mathbb{N}$ *a dvojice peanovských součinů* $(\cdot, \circ)$ *na* M *taková, že v* $\langle \mathcal{M}_+, \cdot, \circ \rangle$ *platí*
$(\forall x)(a \cdot x = a \circ x)\ \&\ (c \cdot d \neq c \circ d)$

Potkavší se dvojice

Otázka

Shodují-li se hodnoty dvou peanovských součinů na nějaké podmnožině modelu, kde všude se již nutně musí také shodovat, kde se mohou lišit?

Snadno se ukáže následující:

Tvrzení

Existuje model $\mathcal{M}_+ \models \mathrm{Pr}$ *s prvky* $c, d > a > \mathbb{N}$ *a dvojice peanovských součinů* $(\cdot, \circ)$ *na* M *taková, že v* $\langle \mathcal{M}_+, \cdot, \circ \rangle$ *platí* $(\forall x)(a \cdot x = a \circ x)\ \&\ (c \cdot d \neq c \circ d)$

Je možné, aby se součiny shodovaly na nějakém $\{a\} \times M$ a lišily se někde pod a?

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.

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.

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.

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.

Důkaz této věty lze převést na problém eliminace kvantifikátorů v lineární aritmetice (LA).

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.

Důkaz této věty lze převést na problém eliminace kvantifikátorů v lineární aritmetice (LA).

Definice

Lineární aritmetika je teorie v jazyce $L_1 = \langle 0, 1, +, \leq, \boxed{a} \rangle$ rozšiřující Pr o axiomy vyjadřující, že $\boxed{a}$ je unární funkce skalárního násobení prvkem a, a o schéma indukce pro všechny L_1-formule.

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.

Důkaz této věty lze převést na problém eliminace kvantifikátorů v lineární aritmetice (LA).

Definice

Lineární aritmetika je teorie v jazyce $L_1 = \langle 0, 1, +, \leq, \boxed{a} \rangle$ rozšiřující Pr o axiomy vyjadřující, že $\boxed{a}$ je unární funkce skalárního násobení prvkem a, a o schéma indukce pro všechny L_1-formule.

LA se nachází mezi Pr a PA. Analýza LA poskytuje určitý vhled do komplexity peanovských součinů.

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Důkaz je založen na „divovém kalkulu“ — kalkulu termů jazyka $L_{div} = \langle 0, 1, +, -, \leq, \_ \cdot r, \_ \operatorname{div} r \rangle_{r \in R}$, kde $R = \mathcal{M} \cap \mathbb{Q}[\boxed{a}]$.

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Důkaz je založen na „divovém kalkulu“ — kalkulu termů jazyka $L_{div} = \langle 0, 1, +, -, \leq, \_ \cdot r, \_ \operatorname{div} r \rangle_{r \in R}$, kde $R = \mathcal{M} \cap \mathbb{Q}[\boxed{a}]$.
Dva hlavní motivy důkazu jsou:

- Geometrický:

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Důkaz je založen na „divovém kalkulu“ — kalkulu termů jazyka $L_{div} = \langle 0, 1, +, -, \leq, \_ \cdot r, \_ \operatorname{div} r \rangle_{r \in R}$, kde $R = \mathcal{M} \cap \mathbb{Q}[\boxed{a}]$.
Dva hlavní motivy důkazu jsou:

- Geometrický: Každá křivka $y = (qx) \operatorname{div} r$ v M^2 pro $q, r \in R$ je parametrizována jistou dvojicí forem definovaných na n-rozměrné „spirále“, kde n je délka řetězového zlomku $\frac{q}{r}$.

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Důkaz je založen na „divovém kalkulu“ — kalkulu termů jazyka $L_{div} = \langle 0, 1, +, -, \leq, \_ \cdot r, \_ \operatorname{div} r \rangle_{r \in R}$, kde $R = \mathcal{M} \cap \mathbb{Q}[\boxed{a}]$.
Dva hlavní motivy důkazu jsou:

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

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Důkaz je založen na „divovém kalkulu“ — kalkulu termů jazyka $L_{div} = \langle 0, 1, +, -, \leq, \_ \cdot r, \_ \operatorname{div} r \rangle_{r \in R}$, kde $R = \mathcal{M} \cap \mathbb{Q}[\boxed{a}]$.
Dva hlavní motivy důkazu jsou:

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

Eliminace kvantifikátorů v LA

Věta

Každá L_1-formule je v LA ekvivalentní nějaké existenční formuli (a nějaké univerzální formuli).

Důkaz je založen na „divovém kalkulu“ — kalkulu termů jazyka $L_{div} = \langle 0, 1, +, -, \leq, \_ \cdot r, \_ \operatorname{div} r \rangle_{r \in R}$, kde $R = \mathcal{M} \cap \mathbb{Q}[\boxed{a}]$.
Dva hlavní motivy důkazu jsou:

- Geometrický: Každá křivka $y = (qx) \operatorname{div} r$ v M^2 pro $q, r \in R$ 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 L_{div} lze vyjádřit ve tvaru $t(x) = \sum q_i(x \operatorname{div} r_i) + N(x)$, kde $q_i(x \operatorname{div} r_i)$ jsou „harmonické funkce“ a $N(x)$ je „šum“.

Vedlejší výsledky

- $R^{\pm}$ je neeuklidovský okruh, ve kterém funguje Euklidův algoritmus.

Vedlejší výsledky

- $R^{\pm}$ je neeuklidovský okruh, ve kterém funguje Euklidův algoritmus.
- Eliminační algoritmus poskytuje (alespoň v některých případech) rychlý způsob hledání řešení soustav lineárních rovnic v $\mathbb{N}$ (nerovnic v $\mathbb{Z}$).

Vedlejší výsledky

- $R^{\pm}$ je neeuklidovský okruh, ve kterém funguje Euklidův algoritmus.
- Eliminační algoritmus poskytuje (alespoň v některých případech) rychlý způsob hledání řešení soustav lineárních rovnic v $\mathbb{N}$ (nerovnic v $\mathbb{Z}$).
- Speciální případ eliminace pro formule tvaru existenčně kvantifikované soustavy lineárních nerovnic dává „diskrétní verzi Farkasova lemmatu“.

Lineární aritmetiky vyšších řádů

Analogicky k LA lze definovat lineární aritmetiky v jazycích s více skaláry.

Lineární aritmetiky vyšších řádů

Analogicky k LA lze definovat lineární aritmetiky v jazycích s více skaláry. Označme LA_κ teorii „lineární aritmetiky“ v jazyce obsahujícím κ různých unárních funkčních symbolů skalárního násobení.

Lineární aritmetiky vyšších řádů

Analogicky k LA lze definovat lineární aritmetiky v jazycích s více skaláry. Označme LA_κ teorii „lineární aritmetiky“ v jazyce obsahujícím κ různých unárních funkčních symbolů skalárního násobení.

Pak $\mathrm{LA}_0 = \mathrm{Pr}$, $\mathrm{LA}_1 = \mathrm{LA}$.

Lineární aritmetiky vyšších řádů

Analogicky k LA lze definovat lineární aritmetiky v jazycích s více skaláry. Označme LA_κ teorii „lineární aritmetiky“ v jazyce obsahujícím κ různých unárních funkčních symbolů skalárního násobení.

Pak $\mathrm{LA}_0 = \mathrm{Pr}$, $\mathrm{LA}_1 = \mathrm{LA}$. LA_2 je o mnoho komplikovanější teorie než LA (v polookruhu $M \cap \mathbb{Q}[\boxed{a_1}, \boxed{a_2}]$, kde $\boxed{a_1}, \boxed{a_2}$ jsou skaláry jazyka LA_2, již není Euklidův algoritmus konečný).

Lineární aritmetiky vyšších řádů

Analogicky k LA lze definovat lineární aritmetiky v jazycích s více skaláry. Označme LA_κ teorii „lineární aritmetiky“ v jazyce obsahujícím κ různých unárních funkčních symbolů skalárního násobení.

Pak $\mathrm{LA}_0 = \mathrm{Pr}$, $\mathrm{LA}_1 = \mathrm{LA}$. LA_2 je o mnoho komplikovanější teorie než LA (v polookruhu $M \cap \mathbb{Q}[\boxed{a_1}, \boxed{a_2}]$, kde $\boxed{a_1}, \boxed{a_2}$ jsou skaláry jazyka LA_2, již není Euklidův algoritmus konečný).

LA_2 je mnohem blíže PA než je LA.

Lineární aritmetiky vyšších řádů

Analogicky k LA lze definovat lineární aritmetiky v jazycích s více skaláry. Označme LA_κ teorii „lineární aritmetiky“ v jazyce obsahujícím κ různých unárních funkčních symbolů skalárního násobení.

Pak $\mathrm{LA}_0 = \mathrm{Pr}$, $\mathrm{LA}_1 = \mathrm{LA}$. LA_2 je o mnoho komplikovanější teorie než LA (v polookruhu $M \cap \mathbb{Q}[\boxed{a_1}, \boxed{a_2}]$, kde $\boxed{a_1}, \boxed{a_2}$ jsou skaláry jazyka LA_2, již není Euklidův algoritmus konečný).

LA_2 je mnohem blíže PA než je LA. Doufáme, že její zkoumání poskytne další poznatky o struktuře peanovských součinů.

Poděkování

Děkuji za pozornost.