Proměnné, rovnice a řešení

Štěpán Holub

MFF UK

Vila Lanna, 19. 3., 2011

1. Řešitelnost rovnic na slovech
2. Několik málo proměnných
3. Systémy rovnic
4. Testovací množiny
5. Ekvivalenční množiny

Rozhodnutelnost rovnic na slovech

1970 : Nerozhodnutelnost řešitelnosti diofantických rovnic (10. Hilbertův problém)

1977 : Rozhodnutelnost řešitelnosti rovnic na slovech s konstantami: G. S. Makanin

Makaninův algoritmus

Základní myšlenky

- Omezení exponentu periodicity p v řešení. Řešení, které je příliš periodické, tj. nějaká proměnná se zobrazuje na slovo obsahující nějaký faktor tvaru u^p pro příliš velké p, lze zkrátit.
- Nedeterministické transformace rovnic:
  - Volba vzájemného vztahu délek jednotlivých neznámých
  - Transformace garantující růst exponentu periodicity
- $\Rightarrow$ Konečný graf, který je třeba prohledat

Složitost Makaninova algoritmu

Složitost závisí na exponentu periodicity.

1996 A. Kościelski, L. Pacholski:

$$\mathrm{P}(n) \in \mathcal{O}(2^{1.07n}),$$

kde n je délka rovnice.

1998 C. Gutierrez : Složitost Makaninova algoritmu je dána velikostí grafu jako

$$\mathrm{SPACE}(2^{\mathcal{O}(n^2)})$$

Plandowského algoritmus

W. Plandowski, W. Rytter(1998), W. Plandowski(1999b)

- Řešení lze exponenciálně komprimovat
- Komprimovaná forma řešení se nedeterministicky uhodne
- Ověření správnosti je polynomiální
- Výsledná složitost:

$$\mathrm{NPTIME}(n \cdot \log \mathtt{N}(n)),$$

kde $\mathtt{N}(n)$ je omezení délky nejkratšího řešení.

$$\mathrm{PSPACE}(n)$$

jiná forma kódování řešení

Optimální složitost

1979 D. Angluin Je NP-těžké rozhodnout, jestli dané slovo leží v daném *pattern language*

$$abaaabab = x_1 abx_2 bax_1 abx_2$$

$\Rightarrow$ NP jako dolní odhad.

Optimální složitost

Nejlepší horní odhady:

$$\mathrm{NPTIME}(n \cdot \log \mathtt{N}(n)), \quad \mathrm{PSPACE}(n)$$

Odhady délky nejkratšího řešení $\mathtt{N}(n)$:

- Makaninův algoritmus: $2^{2^{\mathtt{P}(n)}}$
- W. Plandowski (1999a):

$$2^{2^{\mathcal{O}(n)}}$$

$\Rightarrow$ NEXPTIME

Hypotéza:

- Nejkratší řešení je nejvýše exponenciálně dlouhé
- Řešitelnost rovnic na slovech je NP-úplná

Množina řešení

1982 G. S. Makanin: zobecnění algoritmu pro volné grupy

1985 A. A. Razborov: reprezentace všech řešení konečným grafem pro volné grupy

1990 J. Jaffar: vyčíslení řešení (terminuje pro konečně mnoho řešení)

2006 W. Plandowski: reprezentace všech řešení konečným grafem pro slova v EXPSPACE

Jedna proměnná

1994 S. Eyono Obono, P. Goralčík, M. N. Maksimenko: $\mathcal{O}(n \log n)$

2002 R. Dąbrowski, W. Plandowski: $\mathcal{O}(n + \#_x \log n)$

$$A_0 X A_1 X \ldots X A_r = X B_1 X \ldots X B_s$$

Základní vlastnosti:

- $\log n$ kandididátských dvojic (u, v): $B_1 X B_1 X$ je prefix $B_1 A_0 A_0$;
- pro každou kandidátskou dvojici

$$\mathtt{Sol}(e) \bigcap (uv)^+ u = \begin{cases} \emptyset & \\ (uv)^k u & \text{pro jediné } k \\ (uv)^+ u & \text{tzv. "dlouhá řešení"} \end{cases}$$

Jedna proměnná : otevřený problém

Problém: Kolik různých (tj. s různými kandidátskými dvojicemi) řešení může existovat?

Hypotéza: Nejvýše dvě.

$$A_0XA_1X\ldots XA_r = XB_1X\ldots XB_s$$

Základní vlastnosti:

- $\log n$ kandididátských dvojic (u, v): B_1XB_1X je prefix $B_1A_0A_0$;
- pro každou kandidátskou dvojici

$$\texttt{Sol}(e)\bigcap(uv)^+u = \begin{cases} \emptyset & \\ (uv)^k u & \text{pro jediné } k \\ (uv)^+u & \text{tzv. "dlouhá řešení"} \end{cases}$$

Jedna proměnná : otevřený problém

Problém: Kolik různých (tj. s různými kandidátskými dvojicemi) řešení může existovat?

Hypotéza: Nejvýše dvě.

$$A_0XA_1X\ldots XA_r = XB_1X\ldots XB_s$$

2009 W. Plandowski, M. Laine

- dlouhé řešení nepřipouští žádné jiné
- pro rovnice s nejvýše čtyřmi výskyty proměnné existují nejvýše dvě řešení

Příklad: Rovnice $XbXacbcac = cbcacbXaX$ má řešení c a $cbcac$.

Jedna proměnná : otevřený problém

Problém: Kolik různých (tj. s různými kandidátskými dvojicemi) řešení může existovat?

Hypotéza: Nejvýše dvě.

$$A_0XA_1X\ldots XA_r = XB_1X\ldots XB_s$$

2009 W. Plandowski, M. Laine

- dlouhé řešení nepřipouští žádné jiné
- pro rovnice s nejvýše čtyřmi výskyty proměnné existují nejvýše dvě řešení

Příklad: Rovnice $XbXacbcac = cbcacbXaX$ má řešení c a $cbcac$.

$$cbcacbcac = cbcacbcac \quad cbcacbcbcacacbcac = cbcacbcbcacacbcac$$

Dvě proměnné

- Bez konstant: pouze komutující řešení
- S konstantami

2004 R. Dąbrowski, W. Plandowski: Popis řešení v čase $\mathcal{O}(n^5)$

Tři proměnné

Bez konstant: Poslední parametrizovatelný případ.

Příklad: Rovnice $xz = zy$ má parametrické řešení

$$x = (uv)^i \qquad y = (vu)^i \qquad z = (uv)^j u$$

1971 J. I. Hmelevskij: Každá rovnice ve třech proměnných je parametrizovatelná. Rovnice $xyz = zvx$ parametrizovatelná není.

Tři proměnné

Bez konstant: Poslední parametrizovatelný případ.

Příklad: Rovnice $xz = zy$ má parametrické řešení

$$x = (uv)^i \qquad y = (vu)^i \qquad z = (uv)^j u$$

1971 J. I. Hmelevskij: Každá rovnice ve třech proměnných je parametrizovatelná. Rovnice $xyz = zvx$ parametrizovatelná není.

Problém: Nezávislost systému rovnic

Věta o kompaktnosti

Věta: (M. H. Albert, J. Lawrence 1985; V. S. Guba 1985)
Každý systém rovnic $S = \{(u_i, v_i) \mid i \in I\}$ má ekvivalentní konečný podsystém $T \subseteq S$.

Důkaz: Vnoření do prostoru matic + Hilbertova věta o bázi.
□

Věta o kompaktnosti

Věta: (M. H. Albert, J. Lawrence 1985; V. S. Guba 1985)
Každý systém rovnic $S = \{(u_i, v_i) \mid i \in I\}$ má ekvivalentní konečný podsystém $T \subseteq S$.

Důkaz: Vnoření do prostoru matic + Hilbertova věta o bázi. □

ekvivalentní formulace

Věta: Každý jazyk L má konečnou testovací množinu T.

Definice: $T \subseteq L$ je testovací množina jazyka L, pokud pro libovolné dva homomorfismy g a h platí

$$g \equiv_T h \quad \Leftrightarrow \quad g \equiv_L h$$

Věta o kompaktnosti

Věta: (M. H. Albert, J. Lawrence 1985; V. S. Guba 1985)
Každý systém rovnic $S = \{(u_i, v_i) \mid i \in I\}$ má ekvivalentní konečný podsystém $T \subseteq S$.

Důkaz: Vnoření do prostoru matic + Hilbertova věta o bázi. □

ekvivalentní formulace

Věta: Každý jazyk L má konečnou testovací množinu T.

Definice: $T \subseteq L$ je testovací množina jazyka L, pokud pro libovolné dva homomorfismy g a h platí

$$g \equiv_T h \quad \Leftrightarrow \quad g \equiv_L h$$

Problém: Je velikost ekvivalentního podsystému (resp. testovací množiny) pro daný počet proměnných omezena?

Tři proměnné

Problém: Je velikost nezávislého systému rovnic ve třech neznámých omezena?

Hypotéza: Neexistuje nezávislý systém tří rovnic o třech neznámých, který by měl neperiodické řešení.

Tři proměnné

Problém: Je velikost nezávislého systému rovnic ve třech neznámých omezena?

Hypotéza: Neexistuje nezávislý systém tří rovnic o třech neznámých, který by měl neperiodické řešení.

2003 D. Nowotka, T. Harju: Nezávislý systém dvou rovnic o třech neznámých s neperiodickým řešením obsahuje pouze balancované rovnice.

Tři proměnné

Problém: Je velikost nezávislého systému rovnic ve třech neznámých omezena?

Hypotéza: Neexistuje nezávislý systém tří rovnic o třech neznámých, který by měl neperiodické řešení.

2003 D. Nowotka, T. Harju: Nezávislý systém dvou rovnic o třech neznámých s neperiodickým řešením obsahuje pouze balancované rovnice.

Příklad:

$$xyz = zyx$$

$$x \mapsto a \quad y \mapsto b \quad z \mapsto aba$$

$$xyyz = zyyx$$

$$x \mapsto a \quad y \mapsto b \quad z \mapsto abba$$

$$x \mapsto a \quad y \mapsto b \quad z \mapsto a$$

Omezené jazyky

Definice: $L \subset a_0^* a_1^* \cdots a_n^*$

Rovnosti $g(w) = h(w)$ vedou k rovnicím $x_0^{k_0} x_1^{k_1} \cdots x_n^{k_n} = y_0^{k_0} y_1^{k_0} \cdots y_n^{k_n}$.

Omezené jazyky

Definice: $L \subset a_0^* a_1^* \cdots a_n^*$

Rovnosti $g(w) = h(w)$ vedou k rovnicím $x_0^{k_0} x_1^{k_1} \cdots x_n^{k_n} = y_0^{k_0} y_1^{k_0} \cdots y_n^{k_n}$.

1998 J. Kortelainen: Systém

$$u_0 x_0^i u_1 x_1^i u_2 \cdots u_{n-1} x_n^i u_n = v_0 y_0^i v_1 y_1^i v_2 \cdots v_{m-1} y_m^i v_m$$

pro $i \in \mathbb{N}_0$ je ekvivalentní podsystému pro $i = 0, 1, \ldots, m + n + 2$.

Omezené jazyky

Definice: $L \subset a_0^* a_1^* \cdots a_n^*$

Rovnosti $g(w) = h(w)$ vedou k rovnicím $x_0^{k_0} x_1^{k_1} \cdots x_n^{k_n} = y_0^{k_0} y_1^{k_0} \cdots y_n^{k_n}$.

1998 J. Kortelainen: Systém

$$u_0 x_0^i u_1 x_1^i u_2 \cdots u_{n-1} x_n^i u_n = v_0 y_0^i v_1 y_1^i v_2 \cdots v_{m-1} y_m^i v_m$$

pro $i \in \mathbb{N}_0$ je ekvivalentní podsystému pro $i = 0, 1, \ldots, m + n + 2$.

2001 Š.H: Systém

$$x_0^i x_1^i \cdots x_n^i = y_0^i y_1^i \cdots y_m^i$$

pro $i \in \mathbb{N}$ je ekvivalentní podsystému pro $1, 2, 3, 4$.

Omezené jazyky

Definice: $L \subset a_0^* a_1^* \cdots a_n^*$

Rovnosti $g(w) = h(w)$ vedou k rovnicím $x_0^{k_0} x_1^{k_1} \cdots x_n^{k_n} = y_0^{k_0} y_1^{k_0} \cdots y_n^{k_n}$.

1998 J. Kortelainen: Systém

$$u_0 x_0^i u_1 x_1^i u_2 \cdots u_{n-1} x_n^i u_n = v_0 y_0^i v_1 y_1^i v_2 \cdots v_{m-1} y_m^i v_m$$

pro $i \in \mathbb{N}_0$ je ekvivalentní podsystému pro $i = 0, 1, \ldots, m + n + 2$.

2001 Š.H: Systém

$$x_0^i x_1^i \cdots x_n^i = y_0^i y_1^i \cdots y_m^i$$

pro $i \in \mathbb{N}$ je ekvivalentní podsystému pro $1, 2, 3, 4$.

Problém: Stačí $n = 1, 2, 3$?

Prize problem

I will pay **100** € to the first person who gives an answer (with a proof) to the following question:

Is there a positive integer $n \geq 2$ and words $u_1, u_2, \ldots, u_n$ such that both equalities

$$\begin{cases} (u_1 u_2 \cdots u_n)^2 = u_1^2 u_2^2 \cdots u_n^2, \\ (u_1 u_2 \cdots u_n)^3 = u_1^3 u_2^3 \cdots u_n^3, \end{cases}$$

hold and the words u_i, $i = 1, \ldots, n$, do not pairwise commute (that is, $u_i u_j \neq u_j u_i$ for at least one pair of indices $i, j \in \{1, 2, \ldots, n\}$)?

Komutativní jazyky

Definice: S každým slovem $a_1 a_2 \cdots a_n \in L$ obsahuje L také všechny jeho permutace $a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(n)}$.

1997 I. Hakala a J. Kortelainen: Každý komutativní jazyk nad n proměnnými má testovací množinu velikosti $\mathcal{O}(n^2)$. Existují komutativní jazyky jejichž testovací množiny mají velikost $\Omega(n^2)$.

Komutativní jazyky

Definice: S každým slovem $a_1 a_2 \cdots a_n \in L$ obsahuje L také všechny jeho permutace $a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(n)}$.

1997 I. Hakala a J. Kortelainen: Každý komutativní jazyk nad n proměnnými má testovací množinu velikosti $\mathcal{O}(n^2)$. Existují komutativní jazyky jejichž testovací množiny mají velikost $\Omega(n^2)$.

2001 Š.H. a Kortelainen: Nejmenší testovací množina jazyka

$$\{a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(n)} \mid \sigma \in \mathbb{S}_n\}$$

má velikost mezi $n - 1$ a $5n$.

Ekvivalenční množiny

Definice: Ekvivalenční množina homomorfismů g a h je

$$\mathrm{Eq}(g,h) = \{w \mid g(w) = h(w)\}.$$

Ekvivalenční množiny

Definice: Ekvivalenční množina homomorfismů g a h je

$$\mathtt{Eq}(g, h) = \{w \mid g(w) = h(w)\}.$$

Rozhodnout, zda $\mathtt{Eq}(g, h)$ obsahuje neprázdné slovo je známý Postův korespondenční problém (PCP).

1979 K. Čulík II, A. Salomaa, A. Ehrenfeucht a R. Rozenberg: Každou rekursivně vyčíslitelnou množinu lze vyjádřit pomocí ekvivalenční množiny.

Binární ekvivalenční množiny

$$\mathtt{Eq}(g,h) = \{w \mid g(w) = h(w)\}, \quad w \in \{a,b\}^+$$

Binární ekvivalenční množiny

$$\mathtt{Eq}(g,h) = \{w \mid g(w) = h(w)\}, \quad w \in \{a,b\}^+$$

2003 Š.H.: Každá binární ekvivalenční množina je generovaná nejvýše dvěma slovy. Dvougenerované množiny mají tvar $\{a^i b, ba^i\}^+$.

Binární ekvivalenční množiny

$$\mathrm{Eq}(g,h) = \{w \mid g(w) = h(w)\}, \quad w \in \{a,b\}^+$$

2003 Š.H.: Každá binární ekvivalenční množina je generovaná nejvýše dvěma slovy. Dvougenerované množiny mají tvar $\{a^i b, ba^i\}^+$.

2008 J. Hadravová, Š.H.: Jednoduché jednogenerované množiny s alespoň 9 výskyty obou písmen jsou tvaru $(ab)^i a$ nebo $a^i b^j$.

Problém: Úplná charakterizace jednogenerovaných binárních ekvivalenčních slov.

Děkuji za pozornost