Racunska složenost Constraint Satisfaction Problema, značaj i kratak pregled novijih rezultata

Petar Marković

Departman za matematiku i informatiku PMF, Novi Sad

Matematika i primene
Beograd, oktobar 2015

Motivacija za CSP - Faginova teorema

Definicija

$SO\exists := \{(\exists R_1)\dots(\exists R_k)\varphi : \varphi \text{ je prvog reda}\}.$

Modeli su konačne relacijske strukture jezika $L(\varphi) \setminus \{R_1, \dots, R_k\}$.

Faginova Teorema (1974)

$SO\exists = NP$

Ova teorema je početak oblasti deskriptivne teorije složenosti.

Definicija

Strict NP (skraćeno SNP) je klasa formula drugog reda u $SO\exists$ gde su sve promenljive prvog reda kvantifikovane univerzalno.

Teorema Kolaitis-Vardi (1987)

SNP reprezentuje NP.

Ulepšavanje Faginove teoreme

Dodaćemo tri ograničenja klasi SNP:

- Monotonost: sve atomske formule su istog znaka (pišemo $MSNP$).
- Monadičnost: sve promenljive drugog reda su unarni predikati (pišemo M_1SNP).
- Nema nejednakosti: sve upotrebe atomske formule $=$ su pozitivnog znaka, a samim tim ih možemo i eliminisati (pišemo $SNP- \neq$).

Teoreme Feder-Vardi (1993/1998)

MM_1SNP, $MSNP- \neq$ i $M_1SNP- \neq$ svi reprezentuju NP.

Veza sa CSP

Neka je $\mathcal{A}$ fiksiran konačan model. Onda je $CSP(\mathcal{A}) = \{\mathcal{B} : Hom(\mathcal{B}, \mathcal{A}) \neq \emptyset\}$.

Teorema Feder-Vardi, 1993/1998; Kun (2013)

CSP reprezentuje $MMSNP- \neq$.

Feder i Vardi su dokazali reprezentaciju slučajnim P algoritmom (u smislu Monte Karlo algoritma, dakle postoji mogućnost greške, ali verovatnoća greške teži nuli kad raste ulaz). Kun je derandomizovao.

Hipoteza o dihotomiji i veza sa $P =?NP$

Feder i Vardi u istom radu postavljaju hipotezu da $CSP(\mathcal{A})$ može biti jedino u P ili NP-kompletan, bez drugih mogućnosti. Ovo je Hipoteza o dihotomiji. Indirektna veza sa $P =?NP$ je

Teorema Ladnera, 1975

Ako $P \neq NP$, onda postoji beskonačno mnogo klasa složenosti (do na redukcije u polinomnom vremenu) unutar NP.

Dakle, ili ne važi Hipoteza o dihotomiji, ili $MMSNP- \neq$ ne reprezentuje $MMSNP$, ili $P = NP$!
Najverovatnije važe Hipoteza o diotomiji i $P \neq NP$, ali $MMSNP- \neq$ ne reprezentuje $MMSNP$. Pravi značaj CSP je kao opšteg okvira u kom je moguće izraziti brojne praktične probleme informatike (Constraint Programming). U tom smislu Hipoteza o dihotomiji daje nadu u klasifikaciju praktično rešivih CSP problema.

Polimorfizmi

Definicija

$f : A^n \to A$ je polimorfizam $\mathcal{A}$ ako je kompatibilna sa svakom relacijom $R^{\mathcal{A}}$ strukture $\mathcal{A}$.

Veza sa složenošću $CSP(\mathcal{A})$ data je sledećom teoremom:

Teorema Bulatova, Jeavonsa i Krokina (2000)

Složenost $CSP(\mathcal{A})$ je u klasi K akko postoje neki polimorfizmi $\mathcal{A}$ koji zadovoljavaju neki skup identiteta.

Teorema Bartoa, Opršala i Pinskera (preprint)

Složenost $CSP(\mathcal{A})$ je u klasi K akko postoje neki polimorfizmi $\mathcal{A}$ koji zadovoljavaju neki skup *linearnih* identiteta.

Algebarska hipoteza o dihotomiji

Teorema Bulatova, Jeavonsa i Krokina (2000), Kearnesa, -, McKenzieja (2014)

$CSP(\mathcal{A})$ je NP-kompletan ako ne postoji polimorfizam $f(x,y,z,u)$ koji zadovoljava

$$\begin{aligned} f(x,x,x,x) &\approx x \\ f(x,y,z,y) &\approx f(y,z,x,x). \end{aligned}$$

Algebarska hipoteza o dihotomiji Bulatova, Jeavonsa i Krokina (2000)

Ako $\mathcal{A}$ ima polimorfizam f kao u gornjoj teoremi, onda je $CSP(\mathcal{A})$ u P.

Implicira Hipotezu o dihotomiji i potvrdjena u mnogim slučajevima. Dajemo pregled parcijalnih rezultata u sledećim slajdovima.

Mali $|A|$

Teorema Shaefera (1978)

Algebarska hipoteza o dihotomiji važi za $|A| = 2$.

Dokaz lako sledi iz Postove mreže (1941).

Teorema Bulatova (2006)

Algebarska hipoteza o dihotomiji važi za $|A| = 3$.

55 strana, daje nove tehnike (za strpljive koji su razumeli rad).

Teorema Bašića, -, Marótija i Moconje (u pripremi)

Algebarska hipoteza o dihotomiji važi za $|A| = 4$.

Dokaz čeka ispis. Bulatovljev troelementni rezultat je malo uopšten na par strana (multisorted verzija), ali ceo dokaz je duuuuuuugačak. Jedna bitna nova tehnika (Maróti).

Ograničena širina

Grubo govoreći, smanjuje se svaka relacija dok se ne izjednače projekcije na sve male podskupove ulaza.

Definicija

Ako sledeća tri uslova uvek impliciraju postojanje rešenja instance $CSP(\mathcal{A})$

- Svaki constraint je neprazan,
- Instanca je k-konzistentna, tj. sve projekcije na podskupove sa $\leq k$ elemenata su iste i
- Instanca je n-gusta, tj svaki podskup ulaza sa $\leq n$ elemenata je unutar domena nekog constrainta,

onda $CSP(\mathcal{A})$ ima širinu (k, n).

Ako $CSP(\mathcal{A})$ ima širinu (k, n) za neke $k, n \in \omega$, onda $CSP(\mathcal{A})$ ima ograničenu širinu. Za fiksirano k i n uvek možemo svesti na k-konzistentnu i n-gustu ekvivalentnu instancu u polinomnom vremenu (ali ne znamo da li neprazno $\Rightarrow$ ima rešenja).

Karakterizacija ograničene širine

Teorema Bartoa (2014)

$CSP(\mathcal{A})$ može imati samo širine $(1,1)$, $(2,3)$ ili neograničenu.

Teorema Dalmaua i Pearsona (1999)

$CSP(\mathcal{A})$ ima širinu $(1,1)$ akko $\mathcal{A}$ ima idempotentni totalno simetrični polimorfizam arnosti $\max\{|R^{\mathcal{A}}| : R \text{ je u jeziku}\}$

Teoreme Larosea i Zádorija(2007); Bartoa i Kozika(2014) i Jovanović, -, McKenzieja i Moorea (2015)

$CSP(\mathcal{A})$ ima ograničenu širinu akko $\mathcal{A}$ ima polimorfizam $f(x,y,z,u)$ koji zadovoljava

$$\begin{aligned} f(x,x,x,x) &\approx x \text{ i} \\ f(y,x,x,x) \approx f(x,y,x,x) &\approx f(x,x,y,x) \approx f(x,x,x,y) \approx \\ \approx f(x,y,y,x) &\approx f(x,y,x,y) \approx f(x,x,y,y). \end{aligned}$$

Malo kompatibilnih relacija (few subpowers)

Neka je $\mathcal{A}$ relacijska struktura. Kažemo da $\mathcal{A}$ ima "few subpowers" (termin iz Univerzalne algebre) ako je broj relacija arnosti n definabilnih pp-formulama log-polinoman.

Teorema Bermana, Idziaka, -, McKenzieja, Valeriotea i Willarda (2010)

$\mathcal{A}$ ima few subpowers akko postoji polimorfizam $e(x_0, \ldots, x_m)$ koji zadovoljava

$$\begin{aligned}
e(y, y, x, x, x, \ldots, x, x) &\approx x \\
e(y, x, y, x, x, \ldots, x, x) &\approx x \\
e(x, x, x, y, x \ldots, x, x) &\approx x \\
e(x, x, x, x, y \ldots, x, x) &\approx x \\
\vdots \qquad &\vdots \quad \vdots \\
e(x, x, x, x, x, \ldots, x, y) &\approx x
\end{aligned}$$

Few subpowers algoritam

Teorema Iste ekipe sem Bermana (2010)

Ako $\mathcal{A}$ ima few subpowers, onda je $CSP(\mathcal{A})$ u P.

Algoritam podseća donekle na Gausovu eliminaciju. Nadje se mali generatorni skup za prostor svih rešenja, pa se dodaje novi constraint i iz starog malog generatornog skupa i računa se mali generatorni skup za prostor svih rešenja koji zadovoljavaju dodatni constraint.

Few subpowers su našli od tada mnoge primene van CSP, ali to nije tema ovog predavanja.

Korišćenje konačnog karaktera

U Univerzalnoj algebri nije ranije postojala teorija koja koristi uslov da je skup operacija skup svih polimorfizama *konačnog* skupa relacija (osim jedne polu-trivijalne teoreme).

Hipoteza Zádorija (pre 2008.), Teorema Bartoa (2013)

Ako je $\mathcal{A}$ konačna relacijska struktura na konačnom jeziku i ima Jónssonove polimorfizme, onda ima NU polimorfizam.

Dokaz prvo reši $CSP(A)$ sa Jónssonovim polimorfizmima (Barto i Kozik 2009), zatim postojanje NU polimorfizma postavi kao instancu $CSP(\mathcal{A})$.

Hipoteza Valeriotea (2011), Teorema Bartoa (2015)

Ako je $\mathcal{A}$ konačna relacijska struktura na konačnom jeziku i ima Dayove polimorfizme, onda ima few subpowers.

Dokaz koristi rezultate [Zhuk (2014)], [-, Maróti i McKenzie (2012)] i [Kozik, Krokhin, Valeriote i Willard (2015)]. Mnogo zeznut!

Redukcija na digrafe

Teorema Federa i Vardija (1993/1998)

Za svaku konačnu strukturu $\mathcal{A}$ postoji digraf $\Gamma_{\mathcal{A}}$ takav da se $CSP(\mathcal{A})$ i $CSP(\Gamma_{\mathcal{A}})$ svode jedan na drugog u polinomnom vremenu.

Zašto ne radimo samo digrafe? Redukcija ne čuva polimorfizme i stoga mnogi poznati algoritmi ne bi radili u kombinaciji sa redukcijom.

Redukcija na digrafe 2

Hipoteza - (2010), Teorema Kazde (2011)

Ako konačan digraf Γ ima Maljcevljev polimorfizam, onda Γ ima majority polimorfizam.

Ali to je i skoro sve što je problematično, kao što je dokazano u

Teorema Bulina, Delića, Jacksona i Nivena (2015)

Ako je $\mathcal{A}$ konačna relacijska struktura na konačnom jeziku onda postoji digraf $\Gamma_{\mathcal{A}}$ takav da $CSP(\mathcal{A})$ i $CSP(\Gamma_{\mathcal{A}})$ imaju sve iste polimorfizme sem onih koji nisu kompatibilni sa digrafom $a \to b \leftarrow c \to d$.

Veze sa modernom teorijom složenosti (approximability)

Teorema Brown-Cohena i Raghavendre (2015)

Ako $\mathcal{A}$ ima polimorfizam "linearnosti" manje od 1, onda svaka relacija u $\mathcal{A}$ ima strukturne osobine "iste" kao one koje su dokazali Barto i Kozik za polimorfizam Kearnesa, - i McKenzieja.

Teoreme Raghavendre (2008) i Brown-Cohena i Raghavendre (2015)

Preformulacija Unique Games Conjecture preko CSP i polimorfizama CSP.