Хипотеза о дихотомији Проблема задовољења услова је (вероватно) доказана

На основу предавања Андреја Булатова у Новом Саду у јуну 2017.

Предавање је посвећено успомени на недавно преминуле колеге Косту Дошена и Зорана Путника

Петар Марковић

Департман за математику и информатику
ПМФ Универзитета у Новом Саду

Математика и примене,
Београд, 17. новембар 2017

CSP дефиниција и Хипотеза о дихотомији

Дефиниција

Нека је $\mathbb{A} = (A; \mathcal{R})$ фиксирана коначна релацијска структура. Инстанца проблема задовољења услова $CSP(\mathbb{A})$ је уређена тројка $(V, A, \mathcal{C})$, где $\mathcal{C} = \{(s_1, R_1), \ldots, (s_k, R_k)\}$, а за свако $1 \leq i \leq k$, $R_i \in \mathcal{R}$ и ако је R_i n_i-арна релација, онда $s_i \in V^{n_i}$. Пресликавање $f : V \to A$ је решење инстанце $(V, A, \mathcal{C})$ ако за све $1 \leq i \leq k$ важи $f(s_i) \in R_i$. $CSP(\mathbb{A})$ је проблем одлучивости који прихвата оне инстанце које имају решење, а одбија оне које немају.

Хипотеза о дихотомији (Feder, Vardi 1993/1998)

За сваки $\mathbb{A}$, проблем $CSP(\mathbb{A})$ је или у P или NP-комплетан.

Овом хипотезом сам се бавио последњих 12 година.

Четири доказа хипотезе

Ове године четири доказа најављена и објављена на arxiv-у.

Доказ Дејана Делића прави логичку грешку. Ни стратегија не може да проради, конзистенција пада на системима линеарних једначина.

Доказ Feder, Kinne и Rafiey-а пада на леми која би требала да елиминише локалне полумреже. Willard нашао контрапример. Кључни случај, ако претпоставимо да га нема онда лако и одавно познато.

Докази Андреја Булатова и Дмитрија Жука су врло компликовани и дугачки, али вероватно тачни.

Булатовљев има преко 100 страна, а кључни део је индукцијски корак од 50 страна. Остало сигурно ради (проверио сам), теоријски врло захтевно.

Жуков доказ нешто краћи (70+страна), али мање исписан. Мање захтеван теоријски, али се ослања на Жукове раније радове. Такође индукција која траје цео доказ, вероватно најбоље исписати формализмом симултане индукције. Спирална или циклична?

Примене ван математике

- Базе података - повезане са конзистенцијом и логиком фиксне тачке.
- Машинско учење - повезано са кратким репрезентацијама и споро растућим скуповима дозвољених релација. Не разумем најбоље мада сам коаутор.
- (Rossi, Venable, Walsh, 2008): Друштвени избор.
- (Brown-Cohen, Raghavendra, 2015): Гашење корелација.
- Разне друге (рецимо на једној конференцији чуо сам приче о Телекому Француске).

Примене у комбинаторици: Хомоморфизми

Проблем $CSP(\mathbb{A})$ се може еквивалентно превести на питање о постојању хомоморфизма између релацијских структура. Инстанца $(V, A, \mathcal{C})$ дефинише улазни модел $\mathbb{B} = (V; \mathcal{R}^{\mathbb{B}})$ на истом језику као $\mathbb{A}$ тако да $(V, A, \mathcal{C})$ има решење акко постоји хомоморфизам из $\mathbb{B}$ у $\mathbb{A}$.

Кад је језик само једна бинарна релација - хомоморфизми (усмерених) графова.

(Feder, Vardi): Може се увек свести на графовски проблем исте сложености (цена: број елемената расте). Но тешко ће ићи радећи само графове, многе познате редукције мењају језик.

Нешетрилова тема током више деценија, обструкције (или забрањене фамилије), дефинабилне фамилије обструкција.

Примена комбинаторике: Кодирање релације графом

Ако је $R \subseteq A^{I \cup J}$, можемо заменити R бинарном релацијом E_R између туплова елемената у A^I и у A^J. Овде $(\overline{a}, \overline{b}) \in E_R$ акко постоји $\overline{c} \in A^{I \cup J}$ такво да $\pi_I(\overline{c}) = \overline{a}$ и $\pi_J(\overline{c}) = \overline{b}$.

Често коришћено, па и у оба тачна доказа дихотомије (и у Делићевом нетачном), чува све алгебарске особине оригиналне структуре.

Примена *CSP* у логици 1: Дескриптивна сложеност

(Fagin, 1973): Опис класе *NP* егзистенцијалном логиком другог реда. А шта је са *P*?

DATALOG је "логички језик" који симулира оператор најмање фиксне тачке. (Immerman; Vardi): Логика првог реда са тим оператором описује класу *P* ако постоји фиксирано линеарно уређење. Но, без тог линеарног уређења не могу се кодирати проблеми у вези с линеарном алгебром. Додавање оператора бројања не описује у потпуности *P*. Не зна се да ли је довољно додавање оператора рачунања ранга матрице над коначним пољем, али решење Дихотомије сугерише да је прави опис "ту негде", можда и јесте (велики проблем).

(Feder, Vardi; Larose, Zádori; Barto, Kozik): DATALOG успешно решава $CSP(\mathbb{A})$ акко се $CSP(\mathbb{A})$ решава проверама локалне конзистенције акко $\mathbb{A}$ има извесне компатибилне операције (које су касније улепшавали и карактерисали Kozik, Krokin, Valeriote, Willard; Јовановић, -, McKenzie, Moore; Brady; Драганић, -, Уљаревић, Захировић).

Примена CSP у логици 2: Када формуле репрезентују NP?

(Ladner, 1975): Ако $P \neq NP$, онда између P и класе NP-комплетних проблема постоји пребројиво бесконачно класа сложености (за $PTIME$ редукције).

Фагинова теорема може да се рестрикује. Које логичке формуле описују подкласе класе NP које непразно секу сваку класу сложености унутар NP? Које формуле описују подкласе које секу NP само у проблемима у P унија NP-комплетни? Главна тема рада Федера и Вардија.

(Feder, Vardi; Kun) MM_1SNP, $MSNP-\neq$ и $M_1SNP-\neq$ секу све класе сложености унутар NP, док $MM_1SNP-\neq$ има тачно оне сложености које се могу добити код проблема облика $CSP(\mathbb{A})$. На основу Дихотомије, ови други су само у P или NP-комплетни.

Нека је $R \subseteq A^k$ релација и $f : A^n \to A$ операција на скупу A. Онда кажемо да је f компатибилна са R ако за све

$$\begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{k1} \end{bmatrix}, \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{k2} \end{bmatrix}, \dots, \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{kn} \end{bmatrix}, \in R,$$

важи

$$f \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{k1}, & a_{k2}, & \dots, & a_{kn} \end{pmatrix} = \begin{bmatrix} f(a_{11}, a_{11}, \dots, a_{1n}) \\ f(a_{21}, a_{22}, \dots, a_{2n}) \\ \vdots \\ f(a_{k1}, a_{k2}, \dots, a_{kn}) \end{bmatrix} \in R$$

CSP и Универзална алгебра 2: Контрола сложености $CSP(\mathbb{A})$

(Булатов, Jeavons, Крокин, 2000/2005): Сложеност $CSP(\mathbb{A})$ зависи искључиво од скупа свих операција на A које су компатибилне са свим релацијама модела $\mathbb{A}$. Ако међу тим компатибилним операцијама нема ниједна Тејлорова операција, онда је $CSP(\mathbb{A})$ NP-комплетан проблем.

(Више радова): Ако $\mathbb{A}$ има компатибилну Тејлорову операцију, онда има компатибилну Тејорову операцију конкретног облика ... (дајем најлакши за изразити, мада се није баш показао употребљивим): За све $x, y, z \in A$,

$$t(x, x, x, x) = x \text{ и } t(x, y, z, x) = t(y, x, y, z).$$

(Булатов; Жук): Ако $\mathbb{A}$ има компатибилну Тејлорову операцију, онда је $CSP(\mathbb{A})$ решив у полиномном времену.

Оптимизација: Вредносни *CSP*

Max/*MinCSP*: Ако је дата инстанца *CSP*, треба задовољити што више, односно минимизовати број услова који није задовољен.

Општије, можемо доделити сваком услову рационалну вредност и минимизовати суму вредности оних који нису задовољени (вредносни *CSP*). Кад су дозвољене вредности у $\{0, 1\}$, добијамо *Max*/*MinCSP*. (Thapper, Zivny): Вредносни *CSP* има полиномну сложеност акко је решив основним линеарним програмирањем (*BLP*) акко има одређену компатибилну операцију. Иначе је *NP*-тежак (оптимизацијска верзија тешког, бар једнако тешко као *NP*-комплетан проблем одлучивости). Дакле, имају дихотомију.

Уопштени вредносни *CSP* дозвољава и услове који се апсолутно морају испоштовати (дозвољава вредност ∞). (Kozik, Ochremiak; Колмогоров, Крокин, Rolinek): Полиномна сложеност акко се *CSP* може решити у полиномном времену + услов о компатибилној операцији за вредносне. Дакле дихотомија *CSP* $\Rightarrow$ дихотомија уопштених вредносних *CSP*.

Апроксимација *CSP*

Често се вредносни *CSP* или $Max - CSP$ решава апроксимативно.

Khot (Unique Games Conjecture, *CSP* верзија): Нека је свака релација R структуре $\mathbb{A}$ бинарна релација облика $R = \{(a, \pi_R(a)) : a \in A\}$, где је за свако R, π_R пермутација скупа A. Онда је проблем апроксимације вредносног проблема задовољења услова $CSP(\mathbb{A})$ (где није дозвољена вредност ∞) NP-тежак. За ову хипотезу му је додељена Неванлинина награда (еквивалент Филдсове медаље, али за теоријско рачунарство) на Светском конгресу 2014.

(Raghavendra, 2008; Brown-Cohen, Raghavendra, 2015): Ако важи Unique Games Conjecture, онда је вредносне проблеме задовољења услова (где није дозвољена вредност ∞) могућа апроксимација само до на извесну константу, после тога апроксимација постаје NP-тежак проблем. Апроксимацију до на ту константу је могуће достићи једним основним алгоритмом семидефинитног програмирања.

Када је пребрајање *CSP* решења лако

Уопштење *CSP* на супротну страну од оптимизације. Бројимо решења обичне инстанце *CSP*.

(Булатов, 2013) $\#CSP(\mathbb{A})$ је #-решив у полиномном времену акко има Маљцевљеву компатибилну операцију и додатни услов на дефинабилне релације еквиваленције (= конгруенције алгебре компатибилних операција), иначе $\#CSP(\mathbb{A})$ је $\#P$-комплетан

$\#P$

($\#P$ проблем пребраја прихватајуће путеве у дрвету рачуна неке недетерминистичке Тјурингове машине; $\#P$-комплетан је такав $\#P$ проблем да се сваки $\#P$ проблем може у полиномном детерминистичном времену свести на њега, дакле тежак је бар колико и решавање детерминистичких NP-комплетних проблема).

Случајни *CSP*

Уобичајени проблеми одлучивости се тичу *најгорег случаја*. Сложеност случајне инстанце је повезана са бројем корака потребним да се разреши *просечна* инстанца. Случајни *CSP* је решаван, али за сада без озбиљне посвећености ограничавању језика, углавном су решаване ситуације које су у обичном *CSP*-у *NP*-комплетне. Простор за примену?

(Deolalikar, 2011): Нетачан доказ $P \neq NP$ редукцијом случајног *CSP* на статистичку физику.

ХВАЛА НА ПАЖЊИ