Height one identities

Libor Barto

Department of Algebra, Charles University, Prague

AAA96 Darmstadt, 1–3 June 2018

CoCoSym: Symmetry in Computational Complexity

This project has received funding from the European Research Council (ERC) under the European Unions Horizon 2020 research and innovation programme (grant agreement No 771005)

Is it the end of UA?

UA (universal algebra) and CSP (constraint satisfaction problems)

- connection discovered about 20 years ago
- central topic in UA
- UA in top TCS conferences (FOCS, STOC) and journals (JACM, SICOMP)
- the main problem in CSP solved [Bulatov'07]; [Zhuk'07]
- **Is it the end of the great period for UA?**

Particularly promising: PCSP (Promise CSP)

- active both in TCS (long time) and UA (last 2 years)
- UA relevant
- UA can definitely contribute
- **this talk:** methods from other fields in UA

Height one identities, CSP, PCSP

- (identification) minor of $f : A^n \to A$ is
  an operation $g : A^m \to A$ defined by

$$g(x_1, \ldots, x_m) = f(\text{ variables })$$

- height one identity is of the form

$$f(\text{ variables }) = g(\text{ variables })$$

- i.e. equality between identification minors of f and g
- **Note:** operation symbols on both sides
  e.g. $f(x, x, y) = x$ is not height one
- **Note:** makes sense for $f, g : A^n \to B$

- for finite relational structure $\mathbb{A}$
  - $\mathrm{CSP}(\mathbb{A})$: given $\mathbb{X}$ find $\mathbb{X} \to \mathbb{A}$
  - ... a computational problem, one for each $\mathbb{A}$
  - **Example:** Find a 3-coloring of a graph (for $\mathbb{A} = \mathbb{K}_3$)
  - $\mathrm{Pol}(\mathbb{A}) = \{f : \mathbb{A}^n \to \mathbb{A}\}$ polymorphisms
  - **Fact:** it is a clone
- complexity of $\mathrm{CSP}(\mathbb{A})$ depends only on
  - $\mathrm{Pol}(\mathbb{A})$ [Jeavons'98]
  - identities in $\mathrm{Pol}(\mathbb{A})$ [Bulatov, Jeavons, Krokhin'05]
  - height one identities in $\mathrm{Pol}(\mathbb{A})$ [B, Opršal, Pinsker'17]
- $\mathrm{CSP}(\mathbb{A})$ is
  - **hard** if polymorphisms don't satisfy some "nontrivial" height one identities
  - **easy** if they do
  - here "nontrivial" means not satisfiable by projections [Bulatov'17]; [Zhuk'17]

- for finite relational structures $\mathbb{A}, \mathbb{B}$ with $\mathbb{A} \to \mathbb{B}$
  - $\mathrm{PCSP}(\mathbb{A})$: given $\mathbb{X}$ such that $\mathbb{X} \to \mathbb{A}$ find $\mathbb{X} \to \mathbb{B}$
  - ... a computational problem, one for each pair $\mathbb{A}, \mathbb{B}$
  - **Example:** Find a 4-coloring of a 3-colorable graph
  - $\mathrm{Pol}(\mathbb{A}, \mathbb{B}) = \{f : \mathbb{A}^n \to \mathbb{B}\}$ polymorphisms
  - **Observe:** general composition does not make sense
  - **Fact:** closed under identification minors
    (it is a clonoid(?), minion(?), ...)
- complexity of $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ depends only on
  - $\mathrm{Pol}(\mathbb{A}, \mathbb{B})$ [Brakensiek, Guruswami'16]
  - height one identities in $\mathrm{Pol}(\mathbb{A}, \mathbb{B})$ [Bulín, Opršal]
- $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ is
  - **hard** if polymorphisms don't satisfy
    some "nontrivial" height one identities
  - **easy** if they do
  - here "nontrivial" means ???

Cyclic monotone Boolean operations

probabilistic method, analysis of Boolean functions

Boolean operation $f : \{0,1\}^n \to \{0,1\}$ is

- cyclic if $f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1)$
- fully symmetric if $f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ for each $\pi \in S_n$
- threshold if it equals thr_α for some α where

$$\mathrm{thr}_\alpha(x_1, \ldots, x_n) = 1 \text{ iff } \sum x_i > \alpha n$$

- monotone if it preserves $\leq$ where $0 \leq 1$

Note: threshold $=$ monotone $+$ fully symmetric

Theorem ([B])

For each k there exists l such that every cyclic monotone Boolean operation of arity $n \geq l$ has an identification minor of arity $\geq k$ which is a threshold operation.

- ∞-many threshold polymorphisms $\Rightarrow$ tractability of PCSP [Brakensiek,Guruswami'16]
- theorem reduces the gap between hardness and tractability for monotone Boolean PCSPs
- height one identities of "permutation type" seems important
- cyclic operations: especially simple + useful in CSP and vCSP

Let $f : \{0,1\}^n \to \{0,1\}$ and $p \in [0,1]$

- choose $x_1, \ldots, x_n \in \{0,1\}$ independently
  - $x_i = 1$ with probability p
  - $x_i = 0$ with probability $1 - p$
- $E_f(p) =$ expected value of $f(x_1, \ldots, x_n)$
- $I_f(p, i)$ influence of the i-th variable
  $=$ probability that $f(x_1, \ldots, x_n)$ changes when x_i is changed
- $I_f(p) := \sum_i I_f(p, i)$ total influence

Theorem ("Russo's Lemma")

$E_f'(p) = I_f(p)$

Theorem ("KKL Theorem" [Kahn, Kalai, Linial'88])

$\exists i \quad I_f(p, i) \geq C \; E_f(p)(1 - E_f(p)) \, \frac{\log n}{n}$

Proof 1/2

Proving: Cyclic monotone $f : \{0,1\}^n \to \{0,1\}$ of sufficiently large arity n has a threshold minor of arity ≥ 10.

Russo's Lemma: $E_f'(p) = I_f(p)$
KKL Theorem: $\exists i \;\; I_f(p,i) \geq C \; E_f(p)(1 - E_f(p)) \; \log n/n$

- take p such that $E_f(p) = 0.5$, say $E_f(0.36) = 0.5$
- f cyclic so $I_f(p,i) = I_f(p,j)$ so $I_f(p) = nI_f(p,i)$
- Russo+KKL: $E_f'(p) = I_f(p) \geq CE_f(p)(1 - E_f(p)) \; \log(n)$
- if $0.00001 \leq E_f(p) \leq 0.99999$ then $E_f'(p) \geq D \log(n)$
- n large $\Rightarrow$
  - if $p < 0.35$ then $E_f(p) < 0.00001$
  - if $p > 0.37$ then $E_f(p) > 0.99999$

$p < 0.35 \Rightarrow E_f(p) < 0.00001 \qquad p > 0.37 \Rightarrow E_f(p) > 0.99999$

- choose a random 10-ary minor of f
  ie. define $g(x_1, \ldots, x_{10}) = f(y_1, \ldots, y_n)$ where
  y_i are chosen uniformly independently from $\{x_1, \ldots, x_{10}\}$
- **Aim**: $\mathrm{P}(g = \mathrm{thr}_{0.35}) > 0$
- $\mathrm{Exp}(g(1,1,1,0,0,0,\ldots,0)) = E_f(3/10) < 0.00001$
- $\mathrm{Exp}(g(1,1,1,1,0,0,\ldots,0)) = E_f(4/10) > 0.99999$
- Expected value of

  $$V := g(1,1,1,0,0,\ldots,0) + g(1,1,0,1,0,\ldots,0) + \cdots + (1 - g(1,1,1,1,0,\ldots,0)) + (1 - g(1,1,1,0,1,0,\ldots,0)) + \ldots$$

  is at most $\binom{10}{3}0.00001 + \binom{10}{4}0.00001 < 1$
- So $\mathrm{P}(V = 0) > 0$
- But $\mathrm{P}(V = 0) = \mathrm{P}(g = \mathrm{thr}_{0.35})$

Blockers

Topological combinatorics, PCP theory

Let $f : [3]^n \to [5]$ where $[i] = \{1, 2, \ldots, i\}$

- $f \in \mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$ if
  $f(x_1, \ldots, x_n) \neq f(y_1, \ldots, y_n)$ whenever $(\forall i)\ x_i \neq y_i$
- subset of coordinates $I \subseteq \{1, \ldots, n\}$ blocks $h : [3]^2 \to [5]$
  if no minor of the form

$$g(x, y) = f(z_1, \ldots, z_n) \text{ with } z_i = x \text{ for } i \in I$$
$$\text{and } z_i \in \{x, y\} \text{ otherwise}$$

  is equal to h

Theorem ([Dinur, Regev, Smyth'05] + [B] + [Opršal])

Each $f \in \mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$ has a "small" subset of coordinates I that blocks some $h : [3]^2 \to [5]$. (small means e.g. $|I| \leq 10^6$)

- "unique blocking with singleton I" **characterizes** NP-hardness of CSP:
  $\mathrm{CSP}(\mathbb{A})$ is NP-hard iff there exists a set of binary functions $\exists H$ such that for each $f \in \mathrm{Pol}(\mathbb{A})$ there exists a unique i such that $\{i\}$ blocks each $h \in H$.
- blocking with larger I (as in Theorem) + some form of uniqueness **sufficient** for NP-hardness of PCSP
- Theorem is a substantial part of the proof that it is NP-hard to 5–color a 3–colorable graph

Theorem ([Dinur, Regev, Smyth'05] + [B] + [Opršal])

Each $f \in \mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$ has a "small" subset of coordinates I that blocks some $h : [3]^2 \to [5]$. (small means e.g. $|I| \leq 10^6$)

- topological combinatorics founded by a proof of Kneser's conjecture [Lovász'78]
- many alternative proofs of Kneser's conjecture
  [Bárány'78], [Greene'02], [Matoušek'04], ...
- Theorem + PCP theory → NP-hardness of PCSP(NAE,k-NAE) [Dinur, Regev, Smyth'05]
- universal algebraic version [B]
- $\mathrm{PCSP}(\mathbb{K}_3, \mathbb{K}_5)$ is NP-hard [Opršal]

- k–sphere $S^k = \{\mathbf{x} \in \mathbb{R}^{k+1} : \|\mathbf{x}\| = 1\}$
- open hemisphere centered at $\mathbf{a}$ = $H(\mathbf{a}) = \{\mathbf{x} \in S^k : \mathbf{a} \cdot \mathbf{x} > 0\}$
- great $(k-1)$–sphere in S^k = $\{\mathbf{x} \in S^k : \mathbf{a} \cdot \mathbf{x} = 0\}$

Theorem (LSB theorem [Lusternik, Schnirelmann'30])

If S^k is covered by $k+1$ open sets, then one of these sets contains both $\mathbf{a}$ and $-\mathbf{a}$ for some $\mathbf{a}$.

$f : A^6 \to B$ is Olšák operation if

$$
\begin{aligned}
t(y, x, x,\ x, y, y) &= \\
t(x, y, x,\ y, x, y) &= \\
t(x, x, y,\ y, y, x)&
\end{aligned}
$$

Theorem ([Opršal])

There is no Olšák operation in $\mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$

Proof: Otherwise

$$
\begin{gathered}
t(1, 2, 3,\ 2, 3, 1), t(2, 3, 1,\ 3, 1, 2), t(3, 1, 2,\ 1, 2, 3), \\
t(2, 1, 1,\ 1, 2, 2), t(3, 2, 2,\ 2, 3, 3), t(1, 3, 3,\ 3, 1, 1)
\end{gathered}
$$

would form a 6-clique in $\mathbb{K}_5$

Theorem: Each $f \in \mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$ has a small subset of coordinates I that blocks some $h : [3]^2 \to [5]$.

- take $f : [3]^n \to [5] \in \mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$
- $k := \#$ of binary operations in $\mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$ minus 1
- distribute n points $\mathbf{p}_1, \ldots, \mathbf{p}_n$ on S^k in general position, ie. no $k+1$ points lie on s great $(k-1)$-sphere
- for $Q \subseteq [n]$ let $f[Q]$ be the binary minor $f(x/y, \ldots)$ where x's are at positions in Q and y's are at the other positions
- for each binary $h \in \mathrm{Pol}(\mathbb{K}_3, \mathbb{K}_5)$ let
  $U_h = \{\mathbf{a} \in S^k : f[\{i : \mathbf{p}_i \in H(\mathbf{a})\}] = h\}$
- LSB theorem: some U_h contains $\mathbf{a}$ and $-\mathbf{a}$ for some $\mathbf{a}$
  cheating!

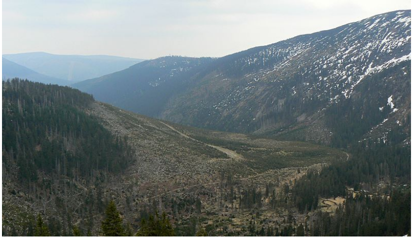
- let's ignore it (can be repaired)
- we have $\mathbf{a} \in S^k$ such that $f[\{i : \mathbf{p}_i \in H(\mathbf{a})\}] = h = f[\{i : \mathbf{p}_i \in H(-\mathbf{a})\}]$
- after reordering of variables

$$\begin{aligned} f(y, y, \dots, y, \quad & x, x, \dots, x, \quad & y, y, \dots, y) = h \\ f(y, y, \dots, y, \quad & y, y, \dots, y, \quad & x, x, \dots, x) = h \end{aligned}$$

  where the initial segment of x's is small
  since $\mathbf{p}_i$'s are in general position
- this set of coordinates blocks h since otherwise

$$f(x, x, \dots, x, \quad x/y, \dots, x/y, \quad x/y, \dots, x/y) = h$$

  and a suitable 6-ary minor would be an Olšák operation



September 2–7, 2018

Špindlerův Mlýn, Czechia

`http://www.karlin.mff.cuni.cz/~ssaos`

Register and pay by June 15th

Summary

- universal algebra can help in a large part of mathematics
- there is so much beautiful math useful in universal algebra

Reading

- G. Kalai: Boolean Functions: Influence, threshold and noise
- R. O'Donnell: Analysis of Boolean functions
- M. de Longueville: 25 years proof of the Kneser conjecture - The advent of topological combinatorics
- J. Matoušek: Using the Borsuk-Ulam Theorem

Summary

- universal algebra can help in a large part of mathematics
- there is so much beautiful math useful in universal algebra

Reading

- G. Kalai: Boolean Functions: Influence, threshold and noise
- R. O'Donnell: Analysis of Boolean functions
- M. de Longueville: 25 years proof of the Kneser conjecture - The advent of topological combinatorics
- J. Matoušek: Using the Borsuk-Ulam Theorem

Thank you!