Short definitions in constraint languages

Jakub Bulín[a], joint work with Michael Kompatscher

105. Arbeitstagung Allgemeine Algebra
Prague, June 2, 2024

[a]Supported by Charles University project UNCE/SCI/004 & MEYS Inter-excellence project LTAUSA19070

[1] J. Bulín and M. Kompatscher: *Short definitions in constraint languages*, 48th International Symposium on Mathematical Foundations of Computer Science (MFCS 2023)

The motivation

Some properties of linear algebra (over a finite field)

- few subspaces, $2^{O(n^2)}$
- small generating sets, $O(n^2)$
- subspace membership in P (echelon form + row-reduce)

- short definitions, $O(n^2)$ ... express any linear system using $x + y = z, x = 0, x = 1$, $\exists$ (auxiliary vars), $\wedge$ (conjunction)

Some properties of finite abelian groups

- few sub[groups of]powers
- small generating sets
- subpower membership in P

- short definitions

Some properties of finite groups

- few subpowers
- small generating sets
- subpower membership in P (Schreier-Sims: SGS + sifting)

- short definitions??

Some properties of finite Mal'tsev algebras

- few subpowers
- small generating sets
- subpower membership in NP, is it in P??

- short definitions??

The what and the why

Explaining the title

"...constraint languages"

- A constraint language over a finite domain A:

$$\Gamma = \{R_1, \ldots, R_m\} \text{ where } R_i \subseteq A^{n_i}$$

- **Example (2-SAT)** $A = \{0,1\}$, $\Gamma_{\mathrm{2SAT}} = \{R_{00}, R_{01}, R_{10}, R_{11}\}$ where $R_{ij} = \{0,1\}^2 \setminus \{(i,j)\}$ (e.g. R_{01} encodes $x \vee \neg y$)

"...definitions in..."

- A primitive positive (pp-) formula: $\exists, \wedge, =$ and symbols from Γ
- A pp-definition: $\phi(x_1, \ldots, x_n)$ defines $R \subseteq A^n$ in the usual way
- The relational clone: $\langle\Gamma\rangle = \{R \mid R \text{ is pp-definable from } \Gamma\}$

"Short..."

- Each $R \in \langle\Gamma\rangle_n$ has a pp-definition of length polynomial in n

Motivation: constraint satisfaction

$\mathrm{CSP}(\Gamma)$

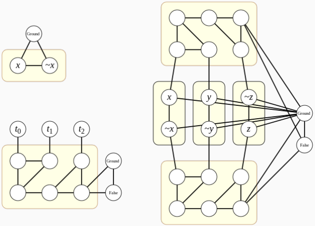
input a pp-sentence Φ over Γ

question $\Gamma \models \Phi$?

Example The 2-CNF formula $(x \vee \neg y) \wedge (y \vee z) \wedge (z \vee \neg x)$ is encoded as $\Phi = (\exists x)(\exists y)(\exists z)(R_{01}(x, y) \wedge R_{00}(y, z) \wedge R_{01}(z, x))$

Moreover:

- solution sets are pp-definable
- pp-definitions are gadget reductions



Theorem (Jeavons, Cohen, Gyssens JACM 1997)

If $\Delta \subseteq \langle \Gamma \rangle$, *then* $\mathrm{CSP}(\Delta)$ *reduces to* $\mathrm{CSP}(\Gamma)$.

The examples

Nonexamples and boring examples

Γ has short definitions, if $\exists$ polynomial $p(n)$ such that each $R \in \langle\Gamma\rangle_n$ has a pp-definition $\phi(x_1, \ldots, x_n)$ of length $|\phi| \le p(n)$.

Nonexamples (3-SAT, Horn-SAT)

Cardinality argument: short definitions $\Rightarrow \langle\Gamma\rangle_n \in 2^{O(n^k)}$

- Γ_{3SAT} doesn't have short definitions, $\langle\Gamma_{\mathrm{3SAT}}\rangle_n$ contains all 2^{2^n} n-ary relations
- Similarly for $\Gamma_{\mathrm{HornSAT}}$, $|\langle\Gamma_{\mathrm{HornSAT}}\rangle|_n$ is double exponential

Boring example (2-SAT)

Γ_{2SAT} has short definitions: each $R \in \langle\Gamma_{\mathrm{2SAT}}\rangle_n$ satisfies the 2-Helly property (and binary relations are pp-definable from Γ_{2SAT}):

$$R(x_1, \ldots, x_n) \leftrightarrow \bigwedge_{1 \le i \le j \le n} \mathrm{pr}_{ij} R(x_i, x_j)$$

$\Rightarrow$ pp-definitions of length $O(n^2)$

Interesting example

Interesting example (Linear systems over $\mathbb{Z}_2$)

- $A = \{0, 1\}$, $\Gamma_{\mathrm{Lin}} = \{R_{\mathrm{Lin}}, C_0, C_1\}$ where $C_a = \{a\}$ and

$$R_{\mathrm{Lin}} = \{(a, b, c) \in \{0, 1\}^3 \mid a + b = c\}$$

- $\langle \Gamma_{\mathrm{Lin}} \rangle_n$ consists of all affine subspaces of $\mathbb{Z}_2^n$
- Each subspace is a conjunction of at most n linear equations
- Each equation can be pp-defined in $O(n)$:
  - for example, $x_1 + x_2 + x_3 = 1$ is defined by

$$(\exists u_1)(\exists u_2)(x_1 + x_2 = u_1 \ \wedge \ u_1 + x_3 = u_2 \ \wedge \ u_2 = 1)$$

  - in general, $x_{i_1} + x_{i_2} + \cdots + x_{i_k} = a$ is defined by

$$(\exists u_1) \dots (\exists u_{k-1})(\bigwedge_{1 \le j \le k-1} R_{\mathrm{Lin}}(x_{i_j}, x_{i_{j+1}}, u_j) \wedge C_a(u_k))$$

$\Rightarrow$ pp-definitions of length $O(n^2)$

The conjecture and the result

Few subpowers

Γ has few subpowers if $|\langle\Gamma\rangle_n| \leq 2^{p(n)}$ for some polynomial $p(n)$

Theorem ([B]IMMVW TransAMS+SICOMP 2010)

A constraint language has $2^{O(n^k)}$ subpowers iff it is invariant under a k-edge function. In that case, $\mathrm{CSP}(\Gamma)$ can be solved by a Gaussian-elimination-like algorithm. Otherwise, it has $\Omega(2^{c^n})$ subpowers for some $c > 1$.

- Γ_{2SAT} is invariant under the 2-edge function called majority: [2]
  $\mathrm{maj}(x, x, y) = \mathrm{maj}(x, y, x) = \mathrm{maj}(y, x, x) = x$
- Γ_{Lin} is invariant under the 2-edge Mal'tsev function $x - y + z$

(general k-edge is a "combination" of those two types of behavior)

[2] In general, a k-ary function $f(x, x, \ldots, x, y) = \cdots = f(y, x, \ldots, x) = x$, called near-unanimity is equivalent to the k-Helly property (boring!)

Few subpowers = short definitions?

Conjecture (B., Kompatscher)

(weak) Γ has short definitions iff it has few subpowers.

(strong) Γ has $O(n^k)$ definitions iff it has a k-edge function.

- Short definitions imply few subpowers (cardinality argument)
- True for $|A| = \{0, 1\}$: essentially only Γ_{2SAT} and Γ_{Lin} (Post's lattice 1941, first noted by Lagerkvist, Wahlström 2014)
- True if invariant under a near-unanimity (Helly property)

Main theorem (B., Kompatscher)

True if the algebra of polymorphisms of Γ generates a residually finite variety.[3] **Corollary** True if $|A| = 3$.

[3] For groups, this means being an A-group (Sylow subgroups are abelian)

(I don't have time for) the proof

Proof overview

I. Switch to the right formalism (algebras, multisorted)

II. Get rid of the boring case (reduce to parallelogram relations)

III. Reduce to "equation-like" relations (critical, reduced)

IV. Simlulate the "shortening" construction for linear equations[4]

[4]Step IV. is the only place where we need residual finiteness. Otherwise, in "$x + y = u$" the domain for u may grow too fast (in general, "$x + y \neq y + x$").

Step I – Switch to the right formalism: algebras

$R \subseteq A^n$ is invariant under $f : A^k \to A$, write $R \perp f$:

$$\mathbf{a^i} \in R \text{ for } 1 \leq i \leq k \;\Rightarrow\; f(\mathbf{a^1}, \ldots, \mathbf{a^k}) \in R$$

Fact: $\langle \Gamma \rangle = (\Gamma^{\perp})^{\perp}$, and also $\langle \mathcal{F} \rangle = (\mathcal{F}^{\perp})^{\perp}$ (the *function clone*, i.e. all term functions built from $\mathcal{F}$)

Examples

- $\langle \Gamma_{\mathrm{2SAT}} \rangle = \{\mathrm{maj}\}^{\perp}$
- $\langle \Gamma_{\mathrm{Lin}} \rangle = \{x - y + z\}^{\perp}$
- $\{\leq\}^{\perp}$ = all monotone Boolean functions

Observe: If $\langle \Gamma \rangle = \langle \Gamma' \rangle$, then Γ has short definitions iff Γ' does.

Thus natural to consider the polymorphism algebra $\mathbf{A} = (A; \Gamma^{\perp})$.
Invariant relations are sub-[universes of]powers of $\mathbf{A}$, $R \leq \mathbf{A}^n$.

Step I – Switch to the right formalism: multisorted

Fundamental theorem of...

- arithmetic: $n = p_1^{e_1} \cdots p_k^{e_k}$ e.g. $6 = 2 \cdot 3$
- abelian groups: $G = \mathbb{Z}_{p_1}^{e_1} \times \cdots \times \mathbb{Z}_{p_k}^{e_k}$ e.g. $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$
- general algebras: $\mathbf{A} \leq \mathbf{A_1} \times \cdots \times \mathbf{A_k}$ where $\mathbf{A_i} \in \mathrm{HSP}(\mathbf{A})$ are subdirectly irreducible (SI)

Working with subdirect decompositions...

- Residually finite = finite bound on SIs = $\exists N$ all $\mathbf{A_i} \in \mathrm{HS}(\mathbf{A}^N)$
- Multisorted relations: $R \leq A^n \longleftrightarrow R' \leq \prod_{j=1}^{m} \mathbf{A_{i_j}}$
- Multisorted definitions over a family of algebras $\{\mathbf{A_1}, \ldots \mathbf{A_k}\}$
- $\mathbf{A}$ has pp-definitions of length $O(n^k)$ iff $\{\mathbf{A_1}, \ldots \mathbf{A_k}\}$ does, etc. (some technical work needed here)

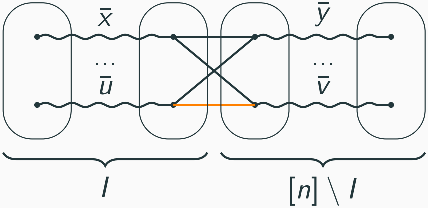
Step II – Get rid of the boring case

Lemma (Kearnes, Szendrei 2012 + Brady 2022)

If Γ is invariant under a k-edge function, then every $R \in \langle\Gamma\rangle$ can be written as

$$R = R' \wedge \bigwedge_{|I| \leq k} \mathrm{proj}_I(R)$$

for some $R' \in \langle\Gamma\rangle$ with the parallelogram property:



For every $I \subset [n]$:

$(\bar{x}, \bar{y}), (\bar{x}, \bar{v}), (\bar{u}, \bar{y}) \in R'$
$\Rightarrow (\bar{u}, \bar{v}) \in R'$

[Picture by Michael]

Examples

- Γ_{Lin}: $R' = R$ (affine subspaces have the parallelogram property)
- Γ_{2SAT}: $R' = A^n$, already $R = \bigwedge_{|I| \leq 2} \mathrm{proj}_I(R)$ (boring!)

Step III – Reduce to "equation-like" relations

$R \in \langle \Gamma \rangle$ is critical if it is $\wedge$-*irreducible* and has *no dummy variables*

Lemma: Every parallelogram relation is an intersection of at most $n \cdot |A|^2$ critical parallelogram relations (c.p.r.'s).

Proof: somewhat like choosing codimension-many linear equations to define a subspace

Similarity "$x_1 + x_2 = x_1' + x_2'$ iff for some u, $x_1 + x_2 = u$ and $x_1' + x_2' = u$"

The linkedness congruence $\sim_I$ on $\mathrm{proj}_I R$:

$$\mathbf{x} \sim_I \mathbf{x}' \ \text{ iff } \ (\exists \mathbf{z})(R(\mathbf{x}, \mathbf{z}) \wedge R(\mathbf{x}', \mathbf{z}))$$

R is reduced if $\sim_{\{i\}}$ is trivial for any $i \in [n]$.

Easy: C.p.r.'s can be defined from reduced c.p.r.'s in $O(n)$

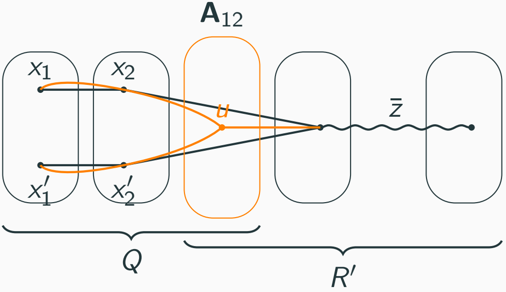
Key Lemma: If R is a reduced c.p.r., then for any $I \subset [n]$ the algebra $\mathbf{A_I} = {}^{\mathrm{proj}_I R}/_{\sim_I}$ is SI. (multisorted Kearnes, Szendrei)

Step IV – Simlulate "shortening" linear equations

$\Gamma' =$ all multisorted 3-ary relations over $\mathrm{HS}(\mathbf{A}^N)$. By induction on n: a reduced c.p.r. $R \in \langle \Gamma' \rangle$ has a $O(n)$-long pp-definition.

Define:

$$R(x_1, \ldots, x_n) \leftrightarrow (\exists u \in \mathbf{A_{12}})(Q(x_1, x_2, u) \wedge R'(u, x_3, \ldots, x_n))$$



$(x_1, x_2, u) \in Q \Leftrightarrow$
$u = (x_1, x_2)/_\sim$

$(y, \bar{z}) \in R' :\Leftrightarrow$
$u = (x_1, x_2)/_\sim, (x_1, x_2, \bar{z}) \in R$

[Picture by Michael]
[slightly ruined by B.]

By Key Lemma, $\mathbf{A_{12}} = \mathrm{proj}_{12} R/_{\sim_{12}}$ is SI, so by residual finiteness it is in $\mathrm{HS}(\mathbf{A}^N)$. Thus $Q \in \Gamma'$; the arity of R' is $n - 1$.

The application

Representing relations

A "representation" of $R \in \langle \Gamma \rangle$ must be both small and efficient

Examples

- basis of a vector subspace (+ row reduction)
- SGS of a permutation group (+ sifting in Schreier-Sims algo)

Fact: Few subpowers $\Leftrightarrow$ small generating sets (BIMMVW 2010)
But are they efficient?

Subpower membership problem $\mathrm{SMP}(\mathbf{A})$:

A is a finite algebra (e.g. the polymoprhism algebra of Γ)

input tuples $\mathbf{b}, \mathbf{a^1}, \ldots, \mathbf{a^k}$ from A^n

question is **b** in the subpower generated by $\mathbf{a^1}, \ldots, \mathbf{a^k}$?

Question (BIMMVW 2010)

Is $\mathrm{SMP}(\mathbf{A})$ in $\mathtt{P}$ for **A** with few subpowers?

Polynomial evaluability

Let **A** have few subpowers

- **Question:** $\mathrm{SMP}(\mathbf{A})$ in $\mathtt{P}$? (BIMMVW 2010)
- **Theorem:** $\mathrm{SMP}(\mathbf{A})$ in $\mathtt{NP}$. (Bulatov, Mayr, Szendrei 2019)
  If **A** generates a residually small variety, then $\mathrm{SMP}(\mathbf{A})$ in $\mathtt{P}$.

Fact (B., Kompatscher)

Short definitions $\Rightarrow \mathrm{SMP}(\mathbf{A})$ in $\mathtt{NP} \cap \mathtt{co\text{-}NP}$

Proof: Guess $\phi(x_1, \ldots, x_n)$, *verify* $\phi(\mathbf{a^i})$ *for* $1 \leq i \leq k$ *but* $\neg\phi(\mathbf{b})$

Question

Given generators for R, can we compute a short pp-definition in polynomial time?

- If true, then $\mathrm{SMP}(\mathbf{A})$ in $\mathtt{P}$
- True for $A = \{0, 1\}$, otherwise open