Few subpowers & short definitions

AI seminar
11/08/2022

- classical logic Qs
- motivated by & tools from the CSP
- generalizing "linear algebra"

- A question I have that connects several open problems
- Recent progress but still work in progress

pp-definability

A – a finite domain

$\mathcal{R} = \{R_1, R_2, \dots\}$ $\quad R_i \subseteq A^{ar(R_i)}$

S is <u>pp-definable</u> from $\mathcal{R}$: definable by $\varphi(\bar{x}) = \exists \bar{y} \bigwedge_j R_{i_j}(\bar{x}_j, \bar{y}_j)$

primitive positive (no $\vee$, no $\neg$)

$S \in \langle \mathcal{R} \rangle$ relational clone, closure under $\cap$, $\times$, perm., proj., $=_A$

"closed one"

Motivation from the CSP

classify constraint languages

<u>gadget</u> constructions: $\mathcal{R}$ constraint language, $\mathcal{R}' \subseteq \langle \mathcal{R} \rangle \Rightarrow$ L-reduction from $CSP(\mathcal{R}')$ to $CSP(\mathcal{R})$

auxiliary variable $\quad$ instance of $CSP(\mathcal{R})$

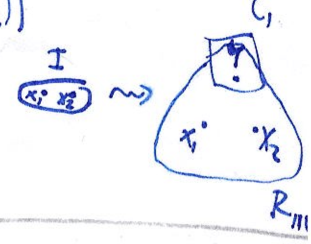
<u>Example:</u> STCON $\leq_L$ HORN-3SAT $\qquad I(x_1, x_2) \Leftrightarrow (\exists y)\,(C_1(y) \wedge R_{110}(y, x_1, x_2))$

directed $\quad$ NL-complete $\quad$ P-complete

$\mathcal{R}' = \{C_0, C_1, I\}$ $\quad C_i = \{i\}$ $\quad I = \{(00), (01), (11)\}$

co-STCON but NL = co-NL (Immerman–Szelepcsényi)

$\mathcal{R} = \{R_{110}, R_{111}, C_0, C_1\}$ $\quad R_{ijk} = \{0,1\}^3 \setminus \{(ijk)\}$



Multivalued logic

$\mathcal{F} = \{f_1, f_2, \dots\}$ $\quad f_i : A^{ar(f_i)} \to A$

$\langle \mathcal{F} \rangle$ function clone, closure under composition, contains projections $f(x_1 \dots x_n) = x_i$

<u>Example:</u> $\langle \neg, \Rightarrow \rangle = \langle \neg, \wedge, \vee \rangle$ = all functions, $\langle \wedge, \vee \rangle$ = monotone functions

<u>Post's lattice</u> (1941) – boolean function clones, nice structure, countable

– generalize to multivalued logic? $\quad$ uncountably many clones for $|A| \geq 3$

How to tell if $g \in \langle \mathcal{F} \rangle$, and if $S \in \langle \mathcal{R} \rangle$? $\quad$ Geiger '68; Bodnarčuk, Kalužnin, Kotov, Romov '69; independently Jeavons, Cohen, Gyssens '98 (for CSP)

<u>Galois correspondence</u> $\quad f \perp R$

$$\begin{tikzcd} \text{functions} \arrow[r, bend left, "\mathrm{Inv}"] & \text{relations} \arrow[l, bend left, "\mathrm{Pol}"] \end{tikzcd}$$

$\langle \mathcal{R} \rangle = \mathrm{Inv}(\mathrm{Pol}(\mathcal{R}))$ $\qquad \mathrm{Inv}(\mathcal{F}) = \mathrm{Inv}(\langle \mathcal{F} \rangle)$

$\langle \mathcal{F} \rangle = \mathrm{Pol}(\mathrm{Inv}(\mathcal{F}))$ $\qquad \mathrm{Pol}(\mathcal{R}) = \mathrm{Pol}(\langle \mathcal{R} \rangle)$

Linear algebra

(point x) + (vector $z-y$)

<u>Example</u>: $\mathbb{Z}_p$, $m(x,y,z) = x - y + z \pmod p$

$\mathrm{Inv}(\{m\})$ = all affine subspaces $= \langle \mathcal{R} \rangle$ where $\mathcal{R} = \{R, C_0, C_1\}$, $R = \{(x,y,z) \mid x+y = z \bmod p\}$

<u>properties</u>:

(substructure) subuniverse of Power of $\mathbb{F} = \mathrm{Pol}(\mathcal{R})$

- <u>few</u> (subspaces) <u>subpowers</u> $S \in \langle \mathcal{R} \rangle$
- small generating sets
- nice <u>representation</u> of S for <u>sifting</u>, <u>computable in P</u>
  (Gauss form) (row-reduction)
- <u>Subpower Membership Problem</u> is in P
  $\mathrm{SMP}(\mathcal{F})$: input $a_1, \dots, a_k, b \in A^n$
  Q: $b \in Sg(a_1, \dots a_k)$?
  ← compute <u>representation</u> of $Sg(a_1, \dots, a_k)$, sift b
- <u>short</u> pp-<u>definitions</u>

<u>Example</u>: $p = 5$

$x_1 + x_2 + x_3 + x_4 = 1 \rightsquigarrow \exists y_1, y_2$ $x_1 + x_2 = y_1$, $y_1 + x_3 = y_2$, $y_2 + x_4 = z$, $z = 1$ $(C_1(z))$

$z = 3 \to z + 2 = 0$
$\to z + 1 + 1 = 0$

Few subpowers

(Berman,) Idziak, Marković, McKenzie, Valeriote, Willard 2010 Trans. AMS + SICOMP

- friends of Ježek, Marković postdoc at Matfyz 2007 (often invented)
- major step towards the CSP dichotomy

<u>def</u> $\mathcal{F}$ has FS $\iff \exists p(n)$ (polynomial) $|\mathrm{Inv}(\mathcal{F})_n| \leq 2^{p(n)}$

equivalently: $\exists p'(n)$ $\forall S \in \mathrm{Inv}(\mathcal{F})_n$ $\exists S' \subseteq S$, $|S'| \leq p'(n)$, $S = Sg(S')$

<u>Thm</u> (BIMMVW)

$\mathcal{F}$ has FS $\iff \exists$ edge operation $e \in \langle \mathcal{F} \rangle$

$e(yyxx\ldots x) = x$
$e(yxyx\ldots x) = x$
$e(xxxyx\ldots x) = x$
$\vdots$
$e(x \ldots\ldots xy) = x$

proof very complicated

$p(n) \in O(n^k)$
$\Updownarrow$
$(k+2)$-ary edge

<u>Examples</u>: ① <u>maltsev</u> $m(xxy) = m(yxx) = y$ $\quad e(xyz) = m(yxz)$, $p(n) \in O(n)$

e.g. $x - y + z$, $x \cdot y^{-1} \cdot z$, groups, loops, qgrps, modules, fields, ...

② <u>majority</u> $maj(xyz)$ $\quad e(x_1, x_2, x_3, x_4) = maj(x_2, x_3, x_4)$, $p(n) \in O(n^2)$

e.g. $\mathcal{R}_{2SAT} = \{R_{00}, R_{01}, R_{10}, R_{11}\}$
$x \vee y$, $x \vee \neg y$

Finite relatedness

<u>def</u> $\mathcal{F}$ is finitely related $\iff \mathrm{Inv}(\mathcal{F}) = \langle \mathcal{R} \rangle$ for some $\mathcal{R}$ finite

<u>Thm</u> (Aichinger, Mayr, McKenzie) Few subpowers are finitely related

proof very complicated, encode as relations, work with representations, well partial order (needs Ramsey's Theorem – nonconstructive

- <u>Example</u>: majority (e.g. 2SAT): $\mathcal{R}$ = all binary invariant relations
- <u>Fun open Q</u>: G group – what is $\mathcal{R}$? Abelian → as for $\mathbb{Z}_p$, otherwise open.

Short definitions

def $\langle R\rangle$ has SD $\iff$ $\exists p(n)\ \forall S \in \langle R\rangle_n$ S is pp-definable by φ, $|\varphi| \leq p(n)$ ③

R finite

me ~2017

- doesn't depend on R: $\langle R\rangle = \langle R'\rangle$ pp-def. R' from R is constant
- instead of $|\varphi|$ can take $|\mathrm{var}(\varphi)|$ or # constraints (predicates)

· SD $\Rightarrow$ FS

$\boxed{\text{Open Q: FS} \Rightarrow \text{SD ?}}$

- recent progress,
- based on new results from CSP theory
- help of Michael Kompatscher

+ can the short defn. be obtained efficiently?

Examples:

- $|A|=2 \Rightarrow \checkmark$
- majority $\Rightarrow$ $R(x_1 \ldots x_n) \iff \bigwedge_{i,j} \mathrm{proj}_{i,j} R\ (x_i, x_j)$

$\binom{n}{2}$ is polynomial ~ $O(n^2)$

(k+1)NU $\Rightarrow$ k-element projections

more on the proof later (if there's time)

Proposition Abelian maltsev $m \in \mathrm{Pol}(R)$ $\Rightarrow$ R has SD

me 2022

↳ e.g. multilinear expansions of abelian groups (fields, modules...)

Proof idea: pp-define the run of the sifting algorithm

$\{(x,y,z,m(x,y,z)) \mid x,y,z \in A\} \in \langle R\rangle$

not that exciting, since abelian = "like a module over abelian ring" (in a technical sense)

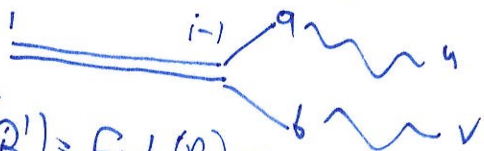
representation for sifting

– a nice small generating set, e.g. vector spaces – Gauss NF + row reduction
groups – SGS, sifting – Schreier-Sims Alg.

Luks 1980 Graph Iso in P for bounded valence

only for Maltsev:

def (i,a,b) fork in R: $\exists u,v \in R$

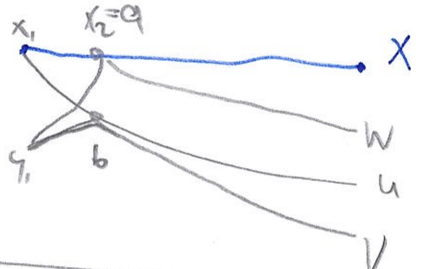


R' is a representation of R if: $R' \subseteq R$ Forks(R') = Forks(R) & $|R'| \leq 2 \cdot |\mathrm{Forks}(R')|$

Lemma Bulatov, Dalmau '06: $\exists$ maltsev $m \in \mathrm{Pol}(R)$ & R' repr. of R $\Rightarrow R = \mathrm{Sg}_m R'$

BIMMVW for FS '10 (add k-el. projections)

Sifting



$m(uvw)$ agrees with x on 1,2

$m(x_1 y_1 y_1) = x_1$

$m(bba) = a = x_2$

Gauss normal form:

```
1 - - - - -
0 0 1 - - -
0 0 0 0 1 - -
0 0 0 0 0 1 -
```

$\Rightarrow$ add 0...0 & take multiples of all rows

Proof of proposition

abelian maltsev $\iff$ $\exists M(xyzu) \in \langle R\rangle_4$ $(x,y,z,u) \in M \iff m(x,y,z) = u$

R'_i witnesses of forks on i-th coordinate ... constant size $\Rightarrow$ pp-defn. is $\leq p(n)$

& $i \sim j \iff w(i) = w(j)$

at most $|A|$ classes of $\sim$

$\Rightarrow$ can express "something is a witness for a fork" and "$m(\bar{x}\bar{y}\bar{z}) = \bar{u}$"

$\Rightarrow$ express that $\bar{x}$ sifted completely through the representation

• Problem: Can we generate a representation in P?

S.D. $\Rightarrow$ can generate repr. of $Sg(a_1, \dots, a_n)$

in general, don't know when to stop (do we have all the forks?)

• Short def is a "better representation" – also tells us that $b \notin R = Sg(a_1, \dots a_n)$

SMP(F) in: $a_1, \dots, a_k, b \in A^n$

Q: $b \in Sg\langle a_1, \dots, a_k \rangle$?

Open Q: Is SMP(F) in P whenever F has FS?

· yes for lin algebra, groups

· yes if F has S.D.

Motivation from CSP

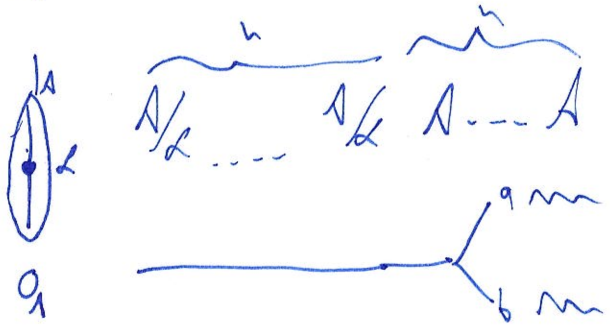
CSP(R) in P $\Rightarrow$ in co-NP but is there an "easy" witness? For ~~F~~ S.D. is such a witness

For lin. alg., the witness is a system of lin. eqn's describing the solution set

---

Idea that doesn't (yet) work

representation modulo a congruence



forks in the 1st half = forks in A/α

in the 2nd half = forks in A but within one α-class

"abelian-like modulo α" $\Rightarrow (a, b) \in \alpha, \quad (a/\alpha = b/\alpha)$

nilpotent? (e.g. groups) $\quad \sim \alpha \sim$

solvable?

"easy": lin. algebra modulo α, "like 2-SAT" in α-classes

---

example of nonabelian malcev: minority on $\{0, 1, 2\}$, $m(x, y, z) = x$