Short pp-definitions

$\mathbb{A} = (A, R_1 \ldots R_k)$

$\langle \mathbb{A} \rangle_{\exists,\wedge}$ ... all pp-definable relations

Def: $\mathbb{A}$ pp-defs. of length $\leq f(n)$

$\forall n \; \forall Q \in \langle \mathbb{A} \rangle_{\exists,\wedge} \cap A^n$ Q has pp-definition ψ
$|\psi| \leq f(n)$

short pp-def. ... pp-defs. of polynomial length
$O(n^\ell)$ for some ℓ.

Examples

•) $\mathbb{A} = (\{0,1\}; \{(x,y,z) \mid x+y=z\}, 0, 1)$

$Q \in A^n \cap \langle \mathbb{A} \rangle$ ... affine subspaces of $\mathbb{Z}_2^n$ ...

Q -- conjunction of $\leq n$ many of

$$x_{i_1} + x_{i_2} + \ldots + x_{i_k} = c \qquad c \in \{0,1\}$$

$$\exists y_2 \ldots y_k : (x_{i_1} + x_{i_2} = y_2) \wedge (y_2 + x_{i_3} = y_3) \wedge \ldots \wedge (y_k = c)$$

pp-fm of length $O(n^2)$

$\rightsquigarrow$ affine $\mathbb{A}$ ✓

•) $\mathbb{A} = (\{0,1\}, \text{all binary})$

$\text{maj} \in \text{Pol}\,\mathbb{A}$

$Q \in \langle \mathbb{A} \rangle \iff Q = \bigwedge_{|I| \leq 2} pr_I Q$

pp-dfs $\leq O(n^2)$

If $\exists f(yx\ldots x) \approx f(xyx\ldots x) \approx \ldots \approx f(x\ldots xy) \approx x$

NU polymorphism of arity k

$\rightsquigarrow$ pp-defs of length $O(n^{k-1})$

If $\langle \mathbb{A} \rangle \overset{\supseteq ?}{=} \langle \mathbb{B} \rangle$

$\mathbb{A}$ pp-defs of length $\leq f(n)$? ?

$\Rightarrow$ $\mathbb{B}$ — " — $\leq c \cdot f(n)$

$\mathbb{B} \in \mathsf{EHSP}\,\mathbb{A}$

If $\mathbb{A}, \mathbb{B}$ pp-bi-interpretable

$\Rightarrow$ $\mathbb{B}$ pp-defs. $\leq c_1 \cdot f(c_2 \cdot n)$

Def $\underline{A}$ ... algebraic structure / clone

$\underline{A}$ has short pp-defs. $\Leftrightarrow$ $\mathrm{Inv}\,\underline{A} = \{ R \leq \underline{A}^n, n \in \mathbb{N} \}$

has short pp-defs.

2 If $\mathbb{A}$ pp-defs of length $\le f(n)$

$\Rightarrow \quad |\langle \mathbb{A} \rangle \cap A^n| \le c^{f(n)}$ for some $c > 1$

So short pp-def $\Rightarrow$ few subpowers

Conjecture

- $\underline{A}$ has short pp-defs. $\Longleftrightarrow$ $\underline{A}$ has few subpowers
- $\underline{A}$ has pp-defs of length $O(n^{\max(k-1,2)})$ $\overset{\Rightarrow}{\Longleftrightarrow}$ $\underline{A}$ has k-edge term

$\underline{A}$ has few subpowers $\iff$

$\exists$ k-edge-term $t \in \mathrm{Clo}\,\underline{A}^{(k+1)}$

$$
\begin{aligned}
t(y\,y\,x\,x \dots x) &\approx x\\
t(y\,x\,y\,x \dots x) &\approx x\\
t(x\,x\,x\,y\,x \dots x) &\approx x\\
&\vdots\\
t(x \dots x\,y) &\approx x
\end{aligned}
$$

few subpowers

$\Downarrow$

finitely related

k-edge-term $\iff$ $i_{\underline{A}}(n) = O(n^{k-1})$

$|n|$pp-def Rel. of arity $n|$

$SMP(\underline{A})$

Input: $\bar{a}_1, \ldots \bar{a}_k, \bar{b} \in A^n$

Question: $\bar{b} \in Sg_{\underline{A}^n}(\bar{a}_1, \ldots \bar{a}_k)$

Is $SMP(\underline{A}) \in P$ for $\underline{A}$ with few subpowers?

If YES, then can encode $R \leq \underline{A}^n$ efficiently as $Sg_{\underline{A}^n}(\bar{a}_1 \ldots \bar{a}_k)$

$\bar{b} \notin Sg_{\underline{A}^n}(\bar{a}_1 \ldots \bar{a}_k) \Rightarrow \exists$ pp-fma. ψ $\neg\psi(\bar{b})$, $\psi(\bar{a}_i)$

$\underline{A}$ short pp-defs $\Rightarrow$ $SMP(\underline{A}) \in coNP$

$\underline{A}$ few subpowers

$\forall\ R \leq \underline{A}^n$: has a compact representation

$$S \subseteq R \qquad |S| = O(n^{k-1} + n^2)$$

$$Sg(S) = R$$

$$\bar{b} \in \overset{R}{\overset{\shortparallel}{Sg}}(\bar{a}_1, \ldots, \bar{a}_k)$$: can be witnessed by S,

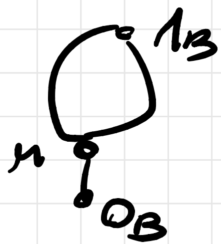
$\rightarrow$ $SMP(\underline{A}) \in NP$

Theorem

If $HSP(\underline{A})$ is residually finite then

pp-defs of length $O(n^{k-1}+n^2) \iff$ k-edge term

$\underline{B}$ is ST $\quad \mathrm{Con}\,\underline{B}$



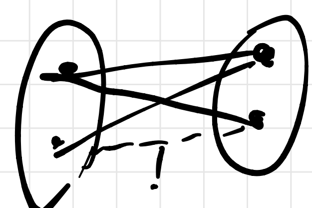
Proof idea

- enough to consider critical rels
  - 1-irreducible
  - no dummy variables

$\underline{A}$ few subpowers

$\underset{\text{critical}}{R} \leq \underline{A}^n \to n \leq k$

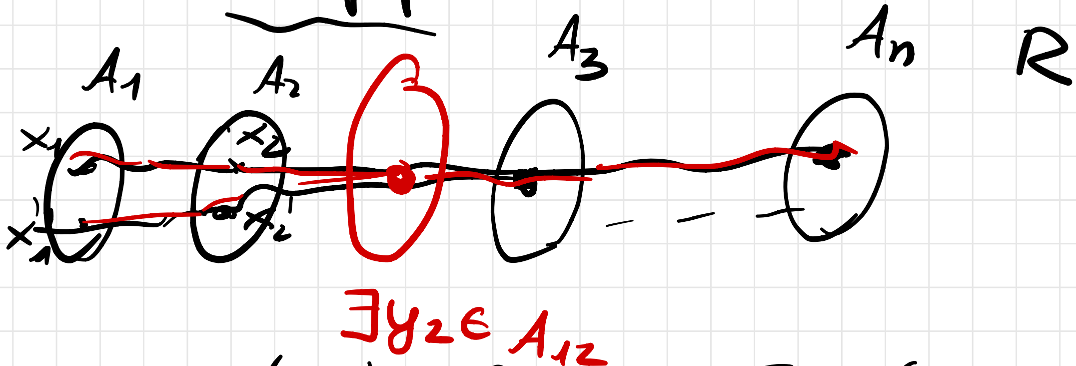
or R has parallelogram property

$pr_I R$  $pr_{[n]\setminus I} R$

Lemma $R \leq \underline{A}^n$ $\exists R_1 \dots R_\ell$ cr. p.p.

$$R = \underbrace{\bigwedge_{|I|<k} pr_I R}_{O(n^{k-1})} \wedge \underbrace{R_1 \wedge \dots \wedge R_\ell}_{\ell \leq |A|^2 \cdot n}$$

$\hookrightarrow$ only consider R critical, parallelogram property for R cr. p.p.



$$(x_1, x_2) \sim (x_1', x_2') \Leftrightarrow \exists \bar{z} : (x_1 x_2 \bar{z}) \in R$$
$$(x_1' x_2' \bar{z}) \in R$$

$$\underline{A}_{12} := pr_{\{12\}} R / \sim$$

$\downarrow$

$\underline{A}_{12}$ is SI $\rightarrow$ $|A_{12}| \in C$

$|A_{12}| \leq |A_1| \cdot |A_2|$

$\square$

group

N central

G not abelian

$$M = \{(x,x) \mid x \in N\} \trianglelefteq G \times G$$

M has unique cover $N \times N$

$$|G| < \underbrace{|G \times G / M|}_{\text{SI}} \leq |G|^2$$

Maroti doesn't work

$$\underline{A} = \left(\overset{L}{\{0,1\}} \times \overset{U}{\{0,1\}},\ g(xyz)\right)$$

$$g((l_1,u_1),(l_2u_2),(l_3u_3)) = (l_1+l_2+l_3+\hat{g}(u_1u_2u_3),\ maj(u_1u_2u_3))$$

$\hat{g}$ symetric

$\hat{g}(100) = 1$

$\hat{g}(u_1u_2u_3) = 0$ else

HSP($\underline{A}$) not r.f.

affine