Short definitions in constraint languages

Jakub Bulín, Michael Kompatscher

Charles University
28.08.2023
MFCS - Bordeaux
Short pp-definitions
Structures with short pp-definitions

\[ \mathbb{A} = (A; R_1, \ldots, R_k) \ldots \text{ finite relational structure} \]

\[ Q \subseteq A^n \text{ is pp-definable over } \mathbb{A} \text{ if} \]

\[ Q(x_1, \ldots, x_n) \iff \exists y_1, \ldots, y_k \ R_i(x) \land \ldots \land R_j(x) \]

\[ \psi(x_1, \ldots, x_n) \text{ pp-formula over } \mathbb{A} \]

\[ \langle \mathbb{A} \rangle := \text{all pp-definable relations} \]

Definition

- \( \mathbb{A} \) has **pp-definitions of length** \( \leq f(n) \) if \( \forall Q \in \langle \mathbb{A} \rangle \cap A^n : Q \) is definable by a pp-formula \( \psi \) with \( |\psi| \leq f(n) \)
- \( \mathbb{A} \) has **short pp-definitions** if \( \mathbb{A} \) has pp-definitions of length \( \leq p(n) \), for a polynomial \( p(n) \).

**Question:** Which \( \mathbb{A} \) have short pp-definitions?
Affine spaces

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

\[ Q \in \langle \mathbb{A} \rangle \iff Q \text{ affine subspace of } \mathbb{Z}_2^n \]

\[ \iff \text{given by } \leq n \text{ equations:} \]

\[ x_{i_1} + x_{i_2} + \ldots + x_{i_k} = a \iff \exists y_2, \ldots, y_k : (x_{i_1} + x_{i_2} = y_2) \land (y_2 + x_{i_3} = y_3) \land \ldots \land (y_{k-1} + x_k = y_k) \land (y_k = a) . \]

\[ \Rightarrow \text{pp-definitions of length } O(n^2) . \]
Affine spaces

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

\[ Q \in \langle \mathbb{A} \rangle \iff \text{Q affine subspace of } \mathbb{Z}_2^n \]
\[ \iff \text{given by } \leq n \text{ equations:} \]
\[ x_{i_1} + x_{i_2} + \ldots + x_{i_k} = a \iff \]
\[ \exists y_2, \ldots, y_k : (x_{i_1} + x_{i_2} = y_2) \land (y_2 + x_{i_3} = y_3) \land \ldots \land (y_{k-1} + x_k = y_k) \land (y_k = a). \]

\[ \Rightarrow \text{pp-definitions of length } O(n^2). \]

2-SAT

\[ \mathbb{A} = (\{0, 1\}; (R_{a,b})_{a,b \in \{0,1\}}), \text{ with } R_{a,b} = \{0, 1\}^2 \setminus \{(a, b)\}. \]

\[ Q \in \langle \mathbb{A} \rangle \iff Q(x_1, \ldots, x_n) = \bigwedge_{1 \leq i, j \leq n} \text{pr}_{\{i,j\}} Q(x_i, x_j). \]

\[ \Rightarrow \text{pp-definitions of length } O(n^2). \]
Observation 1

\( \mathbb{A} \) has pp-defs. of length \( \leq p(n) \)

\( \langle \mathbb{A} \rangle = \langle \mathbb{B} \rangle \Rightarrow \mathbb{B} \) has pp-defs. of length \( \leq c \cdot p(n) \)
Algebras/Clones with short pp-definitions

Observation 1

\[ \mathcal{A} \text{ has pp-defs. of length } \leq p(n) \]
\[ \langle \mathcal{A} \rangle = \langle \mathcal{B} \rangle \Rightarrow \mathcal{B} \text{ has pp-defs. of length } \leq c \cdot p(n) \]

\[ \text{Pol}(\mathcal{A}) = \{ f : \mathcal{A}^n \to \mathcal{A} \mid n \in \mathbb{N} \} \ldots \text{ polymorphism clone of } \mathcal{A} \]
\[ \mathcal{A} \ldots \text{ algebraic structure} \]
\[ \text{Inv}(\mathcal{A}) = \{ R \leq \mathcal{A}^n \mid n \in \mathbb{N} \} \text{ invariant relations of } \mathcal{A} \]
\[ \text{Inv}(\text{Pol}(\mathcal{A})) = \langle \mathcal{A} \rangle \Rightarrow \text{ short pp-definitions is a property of } \text{Pol}(\mathcal{A}) \]

(even up to clone isomorphism).
Observation 1

\[ \mathbb{A} \text{ has pp-defs. of length } \leq p(n) \]
\[ \langle \mathbb{A} \rangle = \langle \mathbb{B} \rangle \Rightarrow \mathbb{B} \text{ has pp-defs. of length } \leq c \cdot p(n) \]

\[ \text{Pol}(\mathbb{A}) = \{ f : \mathbb{A}^n \rightarrow \mathbb{A} \mid n \in \mathbb{N} \} \ldots \text{ polymorphism clone of } \mathbb{A} \]
\[ \mathbb{A} \ldots \text{ algebraic structure} \]
\[ \text{Inv}(\mathbb{A}) = \{ R \leq \mathbb{A}^n \mid n \in \mathbb{N} \} \text{ invariant relations of } \mathbb{A} \]
\[ \text{Inv}(\text{Pol}(\mathbb{A})) = \langle \mathbb{A} \rangle \Rightarrow \text{short pp-definitions is a property of } \text{Pol}(\mathbb{A}) \]
\[ \text{(even up to clone isomorphism).} \]

Definition

\[ \mathbb{A} \text{ has short pp-definitions}, \text{ if } \text{Inv}(\mathbb{A}) = \langle \mathbb{A} \rangle \text{ has short pp-definitions.} \]

Examples

- Affine subspaces of \( \mathbb{Z}_2^n \leftrightarrow \mathbb{A} = (\{0, 1\}, x - y + z) \)
- 2-SAT \( \leftrightarrow \mathbb{A} = (\{0, 1\}, \text{maj}(x, y, z)) \)
Observation 2

\[ \mathbb{A} \text{ has pp-definitions of length } \leq p(n) \]
\[ \Rightarrow |\langle \mathbb{A} \rangle \cap A^n| \leq c^{p(n)} \text{ for some } c > 1 \]
Observation 2

\( \mathbb{A} \) has pp-definitions of length \( \leq p(n) \)
\[ \Rightarrow |\langle \mathbb{A} \rangle \cap A^n| \leq c^{p(n)} \text{ for some } c > 1 \]

If \( p \) is polynomial, we say Pol(\( \mathbb{A} \)) has few subpowers.

So short pp-definitions \( \Rightarrow \) few subpowers.
Observation 2

$\mathbb{A}$ has pp-definitions of length $\leq p(n)$
$\Rightarrow |\langle \mathbb{A} \rangle \cap A^n| \leq c^{p(n)}$ for some $c > 1$

If $p$ is polynomial, we say $\text{Pol}(\mathbb{A})$ has few subpowers.

So short pp-definitions $\Rightarrow$ few subpowers.

If $\mathbb{A}$ has few subpowers:

- $\mathbb{A}$ has an edge term $t$ (IMMVW’10):
  
  $t(y, y, x, x, x, \ldots, x) \approx x$
  
  $t(y, x, y, x, x, \ldots, x) \approx x$
  
  $t(x, x, x, x, x, \ldots, x) \approx x$

  $\ldots$

  $t(x, x, x, x, x, \ldots, y) \approx x$

- $\text{Inv}(\mathbb{A}) = \langle \mathbb{A} \rangle$ for some finite $\mathbb{A} = (A; R_1, \ldots, R_n)$ (AMM’14)
A conjecture about few subpowers
Conjecture (Bulín)

- **(weak)** \( A \) has short pp-defs. \( \iff \) \( A \) has few subpowers.
- **(strong)** \( A \) has pp-defs. of length \( O(n^k) \) \( \iff \) \( A \) has a \( k \)-edge term.
Conjecture (Bulín)

- **(weak)** $A$ has short pp-defs. $\iff A$ has few subpowers.
- **(strong)** $A$ has pp-defs. of length $O(n^k)$ $\iff A$ has a $k$-edge term.

**True for**

- $A$ is affine
- $A$ has NU-term
  \[ y \approx t(y, x, \ldots, x) \approx t(x, y, x, \ldots, x) \approx \ldots \approx t(x, \ldots, x, y) \]
- $|A| = 2$ (Lagerkvist, Wahlström ’14)
Conjecture (Bulín)

- (weak) $A$ has short pp-defs. $\iff A$ has few subpowers.
- (strong) $A$ has pp-defs. of length $O(n^k)$ $\iff A$ has a $k$-edge term.

True for

- $A$ is affine
- $A$ has NU-term
  
  $y \approx t(y, x, \ldots, x) \approx t(x, y, x, \ldots, x) \approx \ldots \approx t(x, \ldots, x, y)$
- $|A| = 2$ (Lagerkvist, Wahlström ’14)

$|A| = 3$ not covered by above
Theorem (Bulín, MK '23)

If $\text{HSP}(\mathbf{A})$ is residually finite, then
$\mathbf{A}$ has pp-definition of length $O(n^k) \iff \mathbf{A}$ has a $k$-edge term.
**Theorem (Bulín, MK ’23)**

If $\text{HSP}(A)$ is residually finite, then $A$ has pp-definition of length $O(n^k) \iff A$ has a $k$-edge term.

$B$ is *subdirectly irreducible*, if $\text{Con}(B) = \begin{array}{c} 1_B \\ \mu \\ 0_B \end{array}$

$\text{HSP}(A)$ *residually finite*, if $B \in \text{HSP}(A)$ is SI $\iff B \in \{B_1, \ldots, B_k\}$, $|B_i| < \infty$. 

---

**Corollary (Bulín, MK ’23)**

If $|A| = 3$, then $A$ has pp-definition of length $O(n^k) \iff A$ has a $k$-edge term.
Theorem (Bulín, MK ’23)

If $\text{HSP}(A)$ is residually finite, then $A$ has pp-definition of length $O(n^k) \iff A$ has a $k$-edge term.

$B$ is subdirectly irreducible, if $\text{Con}(B) = \mu$

$\text{HSP}(A)$ residually finite, if $B \in \text{HSP}(A)$ is SI $\iff B \in \{B_1, \ldots, B_k\}$, $|B_i| < \infty$.

(folklore) $|A| = 3$, $A$ few subpowers $\Rightarrow \text{HSP}(A)$ is residually finite.

Corollary (Bulín, MK ’23)

If $|A| = 3$, then $A$ has pp-definition of length $O(n^k) \iff A$ has a $k$-edge term.
Proof idea
A relation $R \leq A^n$ is called **critical** if

- $R$ is $\wedge$-irreducible ($R_1, R_2 > R \Rightarrow R_1 \cap R_2 > R$)
- $R$ has no dummy variables
A relation $R \leq A^n$ is called critical if

- $R$ is $\wedge$-irreducible ($R_1, R_2 > R \Rightarrow R_1 \cap R_2 > R$)
- $R$ has no dummy variables

**Lemma**

A... $k$-edge-term, $R \leq A^n$. Then

$$R = \bigwedge_{|J| \leq k} (\text{pr}_J R) \wedge R_1 \wedge \ldots \wedge R_l \text{ for } l \leq n \cdot |A|^2, \text{ } R_i \text{ critical, parallelogram property.}$$
Proof step 1: Reduction to critical relations

A relation $R \leq A^n$ is called critical if

- $R$ is $\wedge$-irreducible ($R_1, R_2 > R \Rightarrow R_1 \cap R_2 > R$)
- $R$ has no dummy variables

Lemma

A $k$-edge-term, $R \leq A^n$. Then

$$R = \bigwedge_{|J| \leq k} (pr_J R) \wedge R_1 \wedge \ldots \wedge R_l$$
for $l \leq n \cdot |A|^2$, $R_l$ critical, parallelogram property.

$R \subseteq A^n$ has the parallelogram property if $\forall I \subseteq [n]$

$$(\bar{x}, \bar{y}), (\bar{x}, \bar{v}), (\bar{u}, \bar{y}) \in R \Rightarrow (\bar{u}, \bar{v}) \in R$$
Task: find short pp-definitions for $R \leq A^n$ critical, parallelogram property
Proof step 2: Similarity

**Task:** find short pp-definitions for $R \leq A^n$ critical, parallelogram property

**Strategy:** as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') \iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x_1', x_2', \bar{z})$

- $\sim \in \mathrm{Con}(\text{pr}_{1,2} R), A_{1,2} := (\text{pr}_{1,2} R)/\sim$
Proof step 2: Similarity

Task: find short pp-definitions for $R \leq A^n$ critical, parallelogram property

Strategy: as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x'_1, x'_2) :\iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x'_1, x'_2, \bar{z})$

- $\sim \in \text{Con}(\text{pr}_{1,2} R), \ A_{1,2} := (\text{pr}_{1,2} R)/\sim$
Proof step 2: Similarity

**Task:** find short pp-definitions for $R \leq A^n$ critical, parallelogram property

**Strategy:** as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x_1', x_2', \bar{z})$
- $\sim \in \text{Con}(\text{pr}_{1,2} R), \ A_{1,2} := (\text{pr}_{1,2} R)/\sim$

\[
\begin{align*}
(x_1, x_2, y) \in Q :\iff & \\
& y = (x_1, x_2)/\sim
\end{align*}
\]
Proof step 2: Similarity

**Task:** find short pp-definitions for $R \leq A^n$ critical, parallelogram property

**Strategy:** as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x_1', x_2') :\iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x_1', x_2', \bar{z})$
- $\sim \in \text{Con}(\text{pr}_{1,2} R), A_{1,2} := (\text{pr}_{1,2} R)/\sim$

\[ (x_1, x_2, y) \in Q :\iff \]
\[ y = (x_1, x_2)/\sim \]

\[ (y, \bar{z}) \in R' :\iff \]
\[ y = (x_1, x_2)/\sim, (x_1, x_2, \bar{z}) \in R \]
Proof step 2: Similarity

**Task:** find short pp-definitions for $R \leq A^n$ critical, parallelogram property

**Strategy:** as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x'_1, x'_2) :\iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x'_1, x'_2, \bar{z})$
- $\sim \in \text{Con}(\text{pr}_{1,2} R), A_{1,2} := (\text{pr}_{1,2} R)/\sim$

\[
\begin{align*}
R(x_1, x_2, x_3, \ldots, x_n) \iff & \exists y \in A_{1,2} Q(x_1, x_2, y) \land R'(y, x_3, \ldots, x_n). \quad \text{Problem: in general } A_{1,2} \neq A \\
\text{But: } & R \text{ critical } \Rightarrow A_{1,2} \text{ is SI } \Rightarrow \text{bounded by residual finiteness. } \square
\end{align*}
\]
Proof step 2: Similarity

**Task:** find short pp-definitions for $R \leq A^n$ critical, parallelogram property

**Strategy:** as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x'_1, x'_2) \iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x'_1, x'_2, \bar{z})$
- $\sim \in \text{Con}(\text{pr}_{1,2} R)$, $A_{1,2} := (\text{pr}_{1,2} R)/\sim$

\[ Q \quad A_{1,2} \quad R' \]

\[ (x_1, x_2, y) \in Q \iff y = (x_1, x_2)/\sim \]
\[ (y, \bar{z}) \in R' \iff y = (x_1, x_2)/\sim, (x_1, x_2, \bar{z}) \in R \]

$R(x_1, x_2, x_3, \ldots, x_n) \iff \exists y \in A_{1,2} Q(x_1, x_2, y) \land R'(y, x_3, \ldots, x_n)$.

**Problem:** in general $A_{1,2} \neq A$
**Task:** find short pp-definitions for $R \leq A^n$ critical, parallelogram property

**Strategy:** as for $x_1 + x_2 + \ldots + x_n = a$

- $(x_1, x_2) \sim (x'_1, x'_2) :\iff \exists \bar{z} R(x_1, x_2, \bar{z}) \land R(x'_1, x'_2, \bar{z})$
- $\sim \in \text{Con}(\text{pr}_{1,2} R), A_{1,2} := (\text{pr}_{1,2} R)/\sim$

Proof:

- $R(x_1, x_2, x_3, \ldots, x_n) \iff \exists y \in A_{1,2} Q(x_1, x_2, y) \land R'(y, x_3, \ldots, x_n)$.

**Problem:** in general $A_{1,2} \neq A$

But: $R$ critical $\Rightarrow A_{1,2}$ is SI $\Rightarrow$ bounded by residual finiteness.
Application:

Subpower Membership Problem
Subpower Membership Problem

\( A \text{... finite algebra} \)

\textbf{SMP}(A)

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

\textbf{Decide:} Is \( \bar{b} \in Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k) \)?

\textbf{Question (IMMVW’10):} Is \( \text{SMP}(A) \in P \) for \( A \) with few subpowers?
Subpower Membership Problem

\( \mathbf{A} \) ... finite algebra

SMP(\( \mathbf{A} \))

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

**Decide:** Is \( \bar{b} \in Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k) \)?

**Question (IMMVW’10):** Is SMP(\( \mathbf{A} \)) \( \in \) P for \( \mathbf{A} \) with few subpowers?

**Observation**

\( \bar{b} \notin Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k) \iff \exists \text{pp-fma.} \psi : \neg \psi(\bar{b}) \land \psi(\bar{a}_1) \land \ldots \land \psi(\bar{a}_k) \)

\( \mathbf{A} \) has short pp-definitions \( \Rightarrow \) SMP(\( \mathbf{A} \)) \( \in \) coNP.
A... finite algebra

\[ \text{SMP}(A) \]

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

**Decide:** Is \( \bar{b} \in Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k) \)?

**Question (IMMVW’10):** Is \( \text{SMP}(A) \in P \) for \( A \) with few subpowers?

**Observation**

\( \bar{b} \notin Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k) \iff \exists \text{pp-fma.} \psi : \neg \psi(\bar{b}) \land \psi(\bar{a}_1) \land \ldots \land \psi(\bar{a}_k). \)

A has short pp-definitions \( \Rightarrow \) \( \text{SMP}(A) \in \text{coNP}. \)

**Theorem (BMS’19)**

- \( \text{SMP}(A) \in \text{NP} \) if \( A \) has few subpowers

**(weak) Conjecture** \( \Rightarrow \) \( \text{SMP}(A) \in \text{NP} \cap \text{coNP}. \)
A... finite algebra

SMP(A)

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

**DECIDE:** Is $\bar{b} \in Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k)$?

**Question (IMMVW’10):** Is SMP(A) $\in$ P for A with few subpowers?

**Observation**

$\bar{b} \notin Sg_{A^n}(\bar{a}_1, \ldots, \bar{a}_k) \iff \exists \text{pp-fma. } \psi : \neg \psi(\bar{b}) \land \psi(\bar{a}_1) \land \ldots \land \psi(\bar{a}_k)$.

A has short pp-definitions $\Rightarrow$ SMP(A) $\in$ coNP.

**Theorem (BMS’19)**

- SMP(A) $\in$ NP if A has few subpowers
- SMP(A) $\in$ P if further HSP(A) is residually finite.

**(weak) Conjecture** $\Rightarrow$ SMP(A) $\in$ NP $\cap$ coNP.
Thank you for your attention!

Any questions?