Definability of linear equation systems over groups and rings

A. Dawar, E. Grädel, B. Holm, E. Kopczynski, W. Pakusa

University of Cambridge, University of Warsaw, RWTH Aachen University

Barriers II , Cambridge, 29 March 2012

A logic for polynomial time

Atserias, Bulatov, Dawar	$\mathsf{Slv}(\mathbf{G}) \notin \mathsf{FP{+}C}$
Dawar, Grohe, Holm, Laubner	$\mathsf{FP{+}C} \lneq \mathsf{FP{+}rk} \leq \mathsf{PTIME}$

A logic for polynomial time

Atserias, Bulatov, Dawar $\quad \mathsf{Slv}(\mathbf{G}) \notin \mathsf{FP{+}C}$

Dawar, Grohe, Holm, Laubner $\quad \mathsf{FP{+}C} \lneqq \mathsf{FP{+}rk} \leq \mathsf{PTIME}$

Matrix rank and linear equation systems

Fields $A \cdot x = b$ solvable iff $\mathrm{rk}(A) = \mathrm{rk}(A|b)$:

If $r = \mathrm{rk}(A)$, then $a_1 \cdot \mathbf{c}_1 + \cdots + a_r \cdot \mathbf{c}_r + a \cdot \mathbf{b} = \mathbf{0}$

A logic for polynomial time

Atserias, Bulatov, Dawar	$\mathsf{Slv}(\mathbf{G}) \notin \mathsf{FP{+}C}$
Dawar, Grohe, Holm, Laubner	$\mathsf{FP{+}C} \lneqq \mathsf{FP{+}rk} \leq \mathsf{PTIME}$

Matrix rank and linear equation systems

Fields	$A \cdot x = b$ solvable iff $\mathsf{rk}(A) = \mathsf{rk}(A \vert b)$: If $r = \mathsf{rk}(A)$, then $a_1 \cdot \mathbf{c}_1 + \cdots + a_r \cdot \mathbf{c}_r + a \cdot \mathbf{b} = \mathbf{0}$
Rings	Many notions (linear dependence, McCoy, inner rank, ...), unknown complexity, above characterisation fails
Groups	Undefined

A logic for polynomial time

Atserias, Bulatov, Dawar	$\mathsf{Slv}(\mathbf{G}) \notin \mathsf{FP{+}C}$
Dawar, Grohe, Holm, Laubner	$\mathsf{FP{+}C} \lneq \mathsf{FP{+}rk} \leq \mathsf{PTIME}$

Matrix rank and linear equation systems

Fields	$A \cdot x = b$ solvable iff $\mathsf{rk}(A) = \mathsf{rk}(A\|b)$: If $r = \mathsf{rk}(A)$, then $a_1 \cdot \mathbf{c}_1 + \cdots + a_r \cdot \mathbf{c}_r + a \cdot \mathbf{b} = \mathbf{0}$
Rings	Many notions (linear dependence, McCoy, inner rank, ...), unknown complexity, above characterisation fails
Groups	Undefined

$$\boxed{\text{Question: } \text{Is } \mathsf{Slv}(\mathbf{G}) \in \mathsf{FP{+}rk}?}$$

A systematic study of solvability

Inter-definability: ⇝ natural domain for Slv

A systematic study of solvability

Inter-definability: ⇝ natural domain for Slv

Theorem

k-ideal rings $\xrightarrow{\text{FP-red.}}$ cyclic groups of prime power order.

A systematic study of solvability

Inter-definability: ⇝ natural domain for Slv

Theorem

k-ideal rings $\xRightarrow{\text{FP-red.}}$ cyclic groups of prime power order.

Intra-definability: ⇝ FO extended by $\mathsf{Slv}_{\mathsf{F}}$

A systematic study of solvability

Inter-definability: $\rightsquigarrow$ natural domain for Slv

Theorem

k-ideal rings $\xRightarrow{\text{FP-red.}}$ cyclic groups of prime power order.

Intra-definability: $\rightsquigarrow$ FO extended by Slv_F

Theorem

Normal form for $\mathsf{FO}+\mathsf{slv}_F$.

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[d, dashed] \\
\mathsf{Slv}(\mathbf{CG})
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

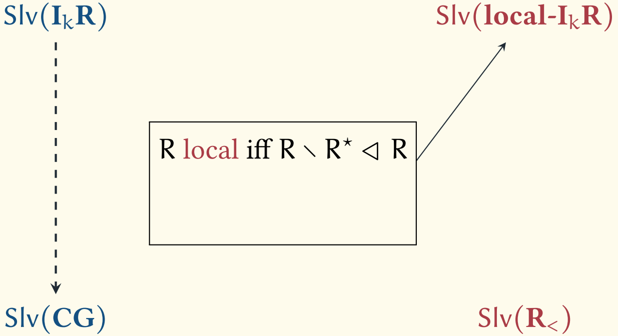
$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[d, dashed] & & \mathsf{Slv}(\mathbf{local\text{-}I}_k\mathbf{R}) \\
\mathsf{Slv}(\mathbf{CG}) & & \mathsf{Slv}(\mathbf{R}_<)
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$

$\mathsf{Slv}(\mathbf{local\text{-}I}_k\mathbf{R})$

R local iff $R \smallsetminus R^\star \lhd R$

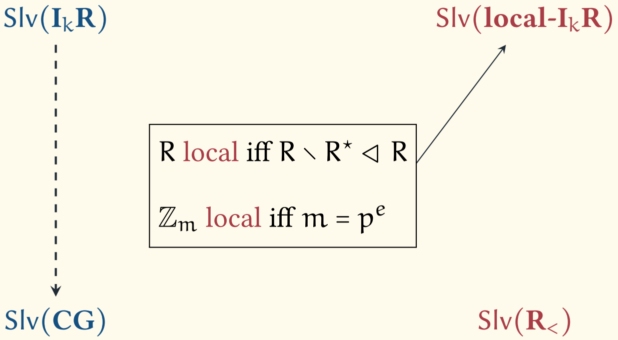
$\mathsf{Slv}(\mathbf{CG})$

$\mathsf{Slv}(\mathbf{R}_<)$

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \triangleleft R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$

$\mathsf{Slv}(\mathbf{local\text{-}I}_k\mathbf{R})$

R local iff $R \smallsetminus R^\star \triangleleft R$

$\mathbb{Z}_m$ local iff $m = p^e$

$\mathsf{Slv}(\mathbf{CG})$

$\mathsf{Slv}(\mathbf{R}_<)$

Inter-definability: a natural class for solvability

$\text{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)
$\text{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\text{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[r, "R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}"] \arrow[d, dashed] & \text{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \\
\text{Slv}(\mathbf{CG}) & \text{Slv}(\mathbf{R}_<)
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathrm{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathrm{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathrm{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[r, "R = \bigoplus_{e\in\varphi} eR,\ eR \text{ local}"] \arrow[d, dashed] & \mathrm{Slv}(\textbf{local-I}_k\mathbf{R}) \arrow[d, "\mathfrak{m} = R \setminus R^\star \lhd R"] \\
\mathrm{Slv}(\mathbf{CG}) & \mathrm{Slv}(\mathbf{R}_<)
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[rr, "R = \bigoplus_{e\in\varphi} eR,\ eR \text{ local}"] \arrow[d, dashed] & & \mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \arrow[d, "\begin{array}{l} \mathfrak{m} = R \setminus R^\star \lhd R \\ \Gamma(R) = \{a : a^{|R/\mathfrak{m}|} = a\} \end{array}"] \\
\mathsf{Slv}(\mathbf{CG}) & & \mathsf{Slv}(\mathbf{R}_<)
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathrm{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)
$\mathrm{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathrm{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[r, "R = \bigoplus_{e\in\varphi} eR,\ eR \text{ local}"] \arrow[d, dashed] & \mathrm{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \arrow[d, "\begin{array}{l} \mathfrak{m} = R \smallsetminus R^\star \lhd R \\ \Gamma(R) = \{a : a^{|R/\mathfrak{m}|} = a\} \\ \Gamma(R) \tilde{\to} R/\mathfrak{m}, r \mapsto r + \mathfrak{m} \end{array}"] \\
\mathrm{Slv}(\mathbf{CG}) & \mathrm{Slv}(\mathbf{R}_<)
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)
$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[rr, "R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}"] \arrow[d, dashed] & & \mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \arrow[d] \\
\mathsf{Slv}(\mathbf{CG}) & & \mathsf{Slv}(\mathbf{R}_<)
\end{tikzcd}$$

$$m = R \setminus R^\star \lhd R$$

$$\Gamma(R) = \{a : a^{|R/m|} = a\}$$

$$\Gamma(R) \xrightarrow{\sim} R/m, r \mapsto r + m$$

$$r \mapsto \sum \underbrace{a_{i_1 \cdots i_k}}_{\in \Gamma(R)} \pi_1^{i_1} \cdots \pi_k^{i_k}$$

Inter-definability: a natural class for solvability

$\mathrm{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)
$\mathrm{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathrm{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[r, "{R = \bigoplus_{e\in\varphi} eR,\ eR \text{ local}}"] \arrow[d, dashed] & \mathrm{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \arrow[d, "{\begin{array}{l} \mathfrak{m} = R \setminus R^\star \lhd R \\ \Gamma(R) = \{a : a^{|R/\mathfrak{m}|} = a\} \\ \Gamma(R) \xrightarrow{\sim} R/\mathfrak{m}, r \mapsto r + \mathfrak{m} \\ r \mapsto \sum \underbrace{a_{i_1\cdots i_k}}_{\in\Gamma(R)} \pi_1^{i_1}\cdots\pi_k^{i_k} \end{array}}"] \\
\mathrm{Slv}(\mathbf{CG}) & \mathrm{Slv}(\mathbf{R}_<) \arrow[l, "{\begin{array}{c} (R,+) = \oplus_{g\in\psi}\langle g\rangle \\ (A,\mathbf{b}) \mapsto (A_1,\mathbf{b_1}),\ldots,(A_k,\mathbf{b_k}) \end{array}}"']
\end{tikzcd}$$

Inter-definability: a natural class for solvability

$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)
$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\begin{tikzcd}
\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \arrow[r, "R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}"] \arrow[d, dashed] & \mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \arrow[d, "\begin{array}{l} \mathfrak{m} = R \setminus R^\star \lhd R \\ \Gamma(R) = \{a : a^{|R/\mathfrak{m}|} = a\} \\ \Gamma(R) \overset{\sim}{\to} R/\mathfrak{m}, r \mapsto r + \mathfrak{m} \\ r \mapsto \sum \underbrace{a_{i_1 \dots i_k}}_{\in \Gamma(R)} \pi_1^{i_1} \cdots \pi_k^{i_k} \end{array}"] \\
\mathsf{Slv}(\mathbf{CG}) & \mathsf{Slv}(\mathbf{R}_<) \arrow[l, "\begin{array}{c} (R,+) = \oplus_{g \in \psi} \langle g \rangle \\ (A, \mathbf{b}) \mapsto (A_1, \mathbf{b_1}), \dots, (A_k, \mathbf{b_k}) \end{array}"']
\end{tikzcd}$$

$$\boxed{\text{Theorem} \quad \mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \leq^{T}_{FP} \mathsf{Slv}(\mathbf{CG})}$$

Intra-definability: solvability as a logical operator

$$\mathsf{slv}(\bar{x},\bar{y},\bar{r}_i).\Big[\underset{\text{coefficient matrix}}{\varphi_M(\bar{x},\bar{y},\bar{r})}, \underset{\text{solution vector}}{\varphi_b(\bar{x},\bar{r})}, \underbrace{(\varphi_R,\varphi_+,\varphi_\cdot)(\bar{r}_1,\bar{r}_2,\bar{r}_3)}_{\text{finite ring}}\Big]$$

Intra-definability: solvability as a logical operator

$$\mathsf{slv}(\bar{x},\bar{y},\bar{r}_i).\Big[\varphi_M(\bar{x},\bar{y},\bar{r}),\varphi_b(\bar{x},\bar{r}),\underbrace{(\varphi_R,\varphi_+,\varphi_\cdot)(\bar{r}_1,\bar{r}_2,\bar{r}_3)}_{\text{finite ring}}\Big]$$

coefficient matrix   solution vector

$$\Downarrow$$

$\mathsf{FO{+}slv}$: First-order logic closed under solvability quantifier

$\mathsf{FO{+}slv}_\mathsf{F}$: Solvability quantifier over a fixed finite field F

Intra-definability: solvability as a logical operator

Theorem

Every $\mathsf{FO}{+}\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi_M(\bar{x},\bar{y}),\mathbf{1}\big],\ \text{with } \varphi_M \text{ quantifier-free.}$$

Intra-definability: solvability as a logical operator

Theorem

Every $\mathsf{FO{+}slv_F}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi_M(\bar{x}, \bar{y}), \mathbf{1}\big], \text{ with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (negation)

$$\neg\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi, \mathbf{1}\big]$$

$$\text{Non-solvability} \ \equiv \ \neg\exists\mathbf{x} : \mathbf{Mx} = \mathbf{b} \ \overset{?}{\equiv} \ \exists\mathbf{y} : \mathbf{M'y} = \mathbf{b'} \equiv \text{Solvability}$$

Intra-definability: solvability as a logical operator

Theorem

Every $\mathsf{FO}+\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi_M(\bar{x},\bar{y}),\mathbf{1}\big],\ \text{ with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (negation)

$$\neg\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi,\mathbf{1}\big]$$

$$\text{Non-solvability} \ \equiv\ \neg\exists\mathbf{x}:\mathbf{Mx}=\mathbf{b}\ \overset{?}{\equiv}\ \exists\mathbf{y}:\mathbf{M'y}=\mathbf{b'} \equiv \text{Solvability}$$

Gaussian elimination implies:

$$\neg\exists\mathbf{x}:\mathbf{Mx}=\mathbf{b}\ \equiv\ \exists\mathbf{y}:\mathbf{y}(\mathbf{M}|\mathbf{b})=(0,\ldots,0|1).$$

Intra-definability: solvability as a logical operator

Theorem

Every $\mathsf{FO}{+}\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi_M(\bar{x}, \bar{y}), \mathbf{1}\big], \text{ with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (conjunction)

$$\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi, \mathbf{1}\big] \wedge \mathsf{slv}(\bar{x}, \bar{y}).\big[\psi, \mathbf{1}\big]$$

$$\boxed{\quad \varphi \quad} \cdot \mathbf{v}_{\mathbf{y}} = \boxed{\begin{matrix} 1 \\ \vdots \\ 1 \end{matrix}}$$

$$\boxed{\quad \psi \quad} \cdot \mathbf{v}_{\mathbf{y}} = \boxed{\begin{matrix} 1 \\ \vdots \\ 1 \end{matrix}}$$

Intra-definability: solvability as a logical operator

Theorem

Every FO+$\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi_M(\bar{x}, \bar{y}), \mathbf{1}\big], \text{ with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (conjunction)

$$\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi, \mathbf{1}\big] \wedge \mathsf{slv}(\bar{x}, \bar{y}).\big[\psi, \mathbf{1}\big]$$

$$\begin{array}{l} \boxed{\;\varphi\;} \cdot \mathbf{v_y} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}} \\[1em] \boxed{\;\psi\;} \cdot \mathbf{v_y} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}} \end{array} \quad \rightsquigarrow \quad \boxed{\begin{array}{c|c} \varphi & \mathbf{0} \\ \hline \mathbf{0} & \psi \end{array}} \cdot \mathbf{v_{yy}} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}$$

Intra-definability: solvability as a logical operator

Theorem

Every $\mathsf{FO}+\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi_M(\bar{x},\bar{y}),\mathbf{1}\big],\ \text{with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (universal quantification)

$$\forall z\,(\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi(\bar{x},\bar{y},z),\mathbf{1}\big])$$

$$\boxed{\quad\varphi(z_1)\quad} \cdot \mathbf{v_y} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}$$

$$\vdots$$

$$\boxed{\quad\varphi(z_n)\quad} \cdot \mathbf{v_y} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}$$

Intra-definability: solvability as a logical operator

Theorem

Every $\mathsf{FO}+\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi_M(\bar{x},\bar{y}),\mathbf{1}\big],\ \text{with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (universal quantification)

$$\forall z\,(\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi(\bar{x},\bar{y},z),\mathbf{1}\big])$$

$$\begin{array}{c} \boxed{\varphi(z_1)} \cdot \mathbf{v_y} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}} \\ \vdots \\ \boxed{\varphi(z_n)} \cdot \mathbf{v_y} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}} \end{array} \quad \rightsquigarrow \quad \boxed{\begin{array}{c|c} \varphi(z_1) & \mathbf{0} \\ \hline & \ddots & \\ \hline \mathbf{0} & \varphi(z_n) \end{array}} \cdot \mathbf{v_{yy}} = \boxed{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}$$

Intra-definability: solvability as a logical operator

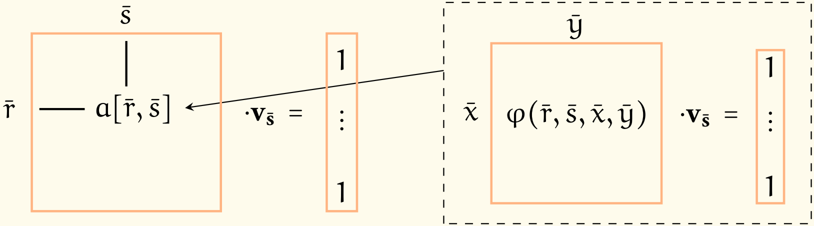
Theorem

Every FO+$\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi_M(\bar{x},\bar{y}),\mathbf{1}\big],\ \text{with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (nesting of solvability)

$$\mathsf{slv}(\bar{r},\bar{s}).\big[\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi(\bar{r},\bar{s},\bar{x},\bar{y}),\mathbf{1}\big],\mathbf{1}\big]$$



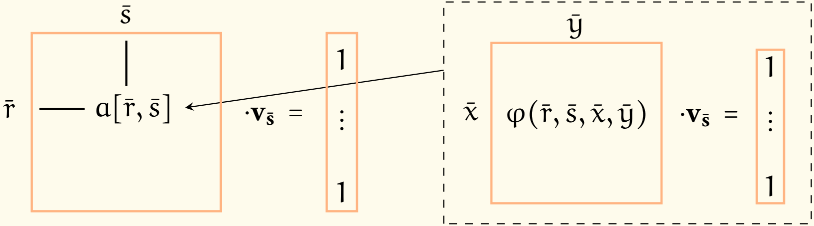
Outer system: $\mathbf{S}$

Inner system: $\mathbf{I}[\bar{r},\bar{s}]$

Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

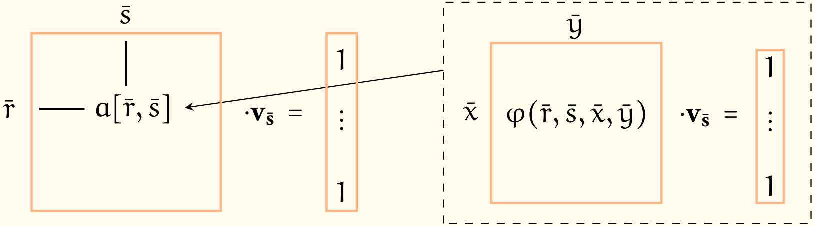
$$\mathsf{slv}(\bar{r},\bar{s}).\big[\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi(\bar{r},\bar{s},\bar{x},\bar{y}),\mathbf{1}\big],\mathbf{1}\big]$$



Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

$$\mathsf{slv}(\bar{r},\bar{s}).\big[\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi(\bar{r},\bar{s},\bar{x},\bar{y}),\mathbf{1}\big],\mathbf{1}\big]$$

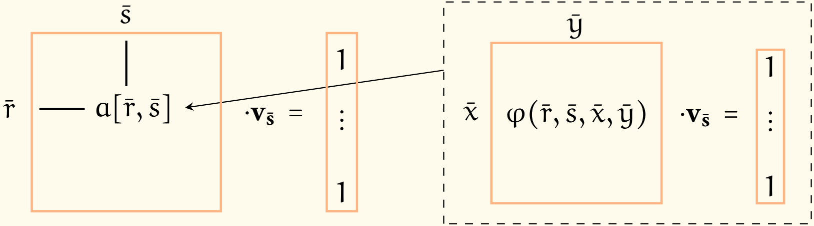


For $\bar{r}$: $\sum_{\bar{s}} \underbrace{a[\bar{r},\bar{s}]\cdot v_{\bar{s}}} = 1$

Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

$$\mathsf{slv}(\bar{r},\bar{s}).\left[\mathsf{slv}(\bar{x},\bar{y}).\left[\varphi(\bar{r},\bar{s},\bar{x},\bar{y}),\mathbf{1}\right],\mathbf{1}\right]$$



For $\bar{r}$: $\sum_{\bar{s}} \underbrace{a[\bar{r},\bar{s}]\cdot v_{\bar{s}}}_{} = 1$

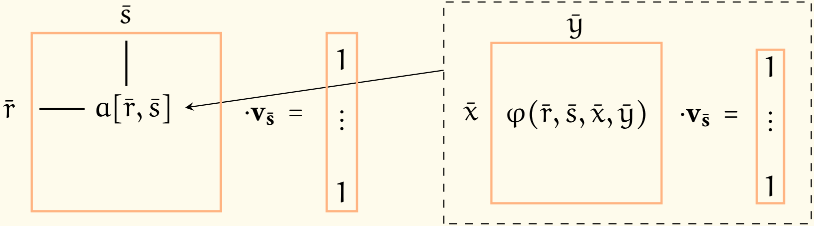
$\rightsquigarrow$

For $\bar{r}$: $\sum_{\bar{s}} 1\cdot v[\bar{r},\bar{s}] = 1$

Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

$$\mathsf{slv}(\bar{r},\bar{s}).\big[\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi(\bar{r},\bar{s},\bar{x},\bar{y}),\mathbf{1}\big],\mathbf{1}\big]$$



For $\bar{r}$: $\sum_{\bar{s}} \underbrace{a[\bar{r},\bar{s}]\cdot v_{\bar{s}}}_{\rightsquigarrow} = 1 \quad \rightsquigarrow$

For $\bar{r}$: $\sum_{\bar{s}} 1\cdot v[\bar{r},\bar{s}] = 1$

Consistency conditions:

$$v[\bar{r},\bar{s}] = 1 \;\Rightarrow\; a[\bar{r},\bar{s}] = 1$$

$$v[\bar{r},\bar{s}] \neq v[\bar{r}',\bar{s}] \;\Rightarrow\; a[\bar{r},\bar{s}] \neq a[\bar{r}',\bar{s}]$$

Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

$$\mathsf{slv}(\bar{r}, \bar{s}).\Big[\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), \mathbf{1}\big], \mathbf{1}\Big]$$

For $\bar{r}$: $\sum_{\bar{s}} \underbrace{a[\bar{r}, \bar{s}] \cdot v_{\bar{s}}}_{} = 1$ $\rightsquigarrow$

$\rightsquigarrow$

For $\bar{r}$: $\sum_{\bar{s}} 1 \cdot v[\bar{r}, \bar{s}] = 1$

Consistency conditions:

$$\begin{cases} v[\bar{r}, \bar{s}] = 1 \;\Rightarrow\; a[\bar{r}, \bar{s}] = 1 \\ v[\bar{r}, \bar{s}] \neq v[\bar{r}', \bar{s}] \;\Rightarrow\; a[\bar{r}, \bar{s}] \neq a[\bar{r}', \bar{s}] \end{cases}$$

How to formalise: “If $v = 1$ then $A \cdot x = 1$ solvable”

Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

$$\mathsf{slv}(\bar r, \bar s).\Big[\mathsf{slv}(\bar x, \bar y).\big[\varphi(\bar r, \bar s, \bar x, \bar y), \mathbf{1}\big], \mathbf{1}\Big]$$

For $\bar r$: $\sum_{\bar s} \underbrace{a[\bar r, \bar s] \cdot v_{\bar s}}_{\big\downarrow} = 1 \quad \rightsquigarrow$

For $\bar r$: $\sum_{\bar s} 1 \cdot v[\bar r, \bar s] = 1$

$$\left\{\begin{array}{l} \text{Consistency conditions:} \\ v[\bar r, \bar s] = 1 \Rightarrow a[\bar r, \bar s] = 1 \\ v[\bar r, \bar s] \neq v[\bar r', \bar s] \Rightarrow a[\bar r, \bar s] \neq a[\bar r', \bar s] \end{array}\right.$$

How to formalise: "If $v = 1$ then $A \cdot x = 1$ solvable"

$$\left[\begin{array}{c|c} & -v+1 \\ A & \vdots \\ & -v+1 \end{array}\right] \cdot \mathbf{x} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

Conclusion and outlook

Theorem

Every $\mathsf{FO}{+}\mathsf{slv}_{\mathsf{F}}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x}, \bar{y}).\big[\varphi_M, \mathbf{1}\big], \text{ with } \varphi_M \text{ quantifier-free.}$$

Theorem

k-ideal rings $\xRightarrow{\text{FP-red.}}$ cyclic groups of prime power order.

Conclusion and outlook

Theorem

Every $\mathsf{FO}+\mathsf{slv}_\mathsf{F}$-formula is equivalent to a formula of the form

$$\mathsf{slv}(\bar{x},\bar{y}).\big[\varphi_M, \mathbf{1}\big], \text{ with } \varphi_M \text{ quantifier-free.}$$

Theorem

k-ideal rings $\overset{\text{FP-red.}}{\Longrightarrow}$ cyclic groups of prime power order.

Outlook: Permutation group membership (GM)

Given: Permutations $\pi_1,\ldots,\pi_k$ and π on a set Ω

Question: Is $\pi \in \langle \pi_1,\ldots,\pi_l \rangle \leq S_\Omega$?

$$\mathsf{GM}, \#\mathsf{GM} \in \mathsf{PTIME}$$

Outlook: from solvability to group membership

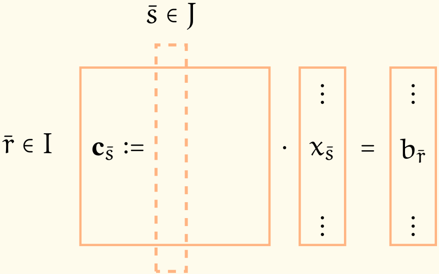
Theorem

$$\begin{tikzcd}
\mathsf{Slv}(\mathbf{D}) \arrow[r, mapsto, "\mathsf{FO}"'] & \mathsf{GM}\ (\pi \in \langle \pi_1, \ldots, \pi_k \rangle \leq S_\Omega?) \\
\mathsf{rk}(\mathbf{F}) \arrow[r, mapsto] & \#\mathsf{GM}(\text{Compute: } |\langle \pi_1, \ldots, \pi_k \rangle|)
\end{tikzcd}$$

Outlook: from solvability to group membership

Theorem

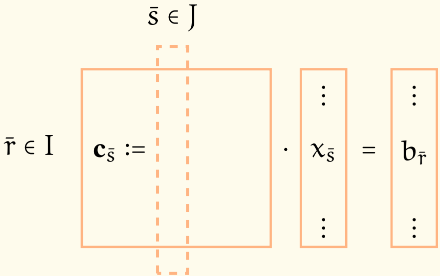
$$\begin{tikzcd} \mathsf{Slv}(\mathbf{D}) \arrow[r, mapsto, "\mathrm{FO}"'] & \mathsf{GM}\,(\pi \in \langle \pi_1, \ldots, \pi_k \rangle \leq S_\Omega?) \\ \mathsf{rk}(\mathbf{F}) \arrow[r, mapsto] & \#\mathsf{GM}(\text{Compute: } |\langle \pi_1, \ldots, \pi_k \rangle|) \end{tikzcd}$$



Outlook: from solvability to group membership

Theorem

$$\begin{tikzcd} \mathsf{Slv}(\mathbf{D}) \arrow[r, mapsto, "\mathrm{FO}"'] & \mathrm{GM}\,(\pi \in \langle \pi_1, \ldots, \pi_k \rangle \leq S_\Omega?) \\ \mathsf{rk}(\mathbf{F}) \arrow[r, mapsto] & \#\mathrm{GM}(\text{Compute: } |\langle \pi_1, \ldots, \pi_k \rangle|) \end{tikzcd}$$



linear system is solvable

$$\Longleftrightarrow$$

$$\mathbf{b} \in \langle \mathbf{c}_{\bar{s}} \cdot d \,:\, d \in D, \bar{s} \rangle \leq (D, +)^I$$

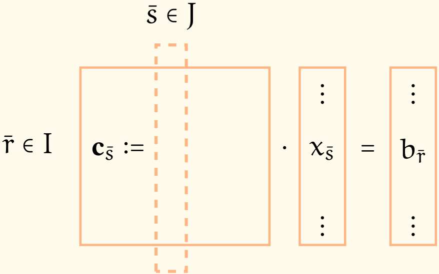
Outlook: from solvability to group membership

Theorem

$$\mathsf{Slv}(\mathbf{D}) \longmapsto \mathsf{GM}\ (\pi \in \langle \pi_1, \ldots, \pi_k \rangle \leq S_\Omega?)$$

FO

$$\mathsf{rk}(\mathbf{F}) \longmapsto \#\mathsf{GM}(\text{Compute: } |\langle \pi_1, \ldots, \pi_k \rangle|)$$



$$\begin{array}{cc} & \bar{s} \in J \\ \bar{r} \in I & \mathbf{c}_{\bar{s}} := \end{array} \cdot \begin{pmatrix} \vdots \\ x_{\bar{s}} \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ b_{\bar{r}} \\ \vdots \end{pmatrix}$$

linear system is solvable

$$\Longleftrightarrow$$

$$\mathbf{b} \in \langle \mathbf{c}_{\bar{s}} \cdot d \;:\; d \in D, \bar{s} \rangle \leq (D, +)^I$$

Cayley's theorem: FO-definable embedding $\iota : (D, +) \to S_D$

$\rightsquigarrow$ FO-definable embedding $\iota : (D, +)^I \to S_{I \times D}$