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

Workshop on Finite and Algorithmic Model Theory,
Les Houches, 14 May 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

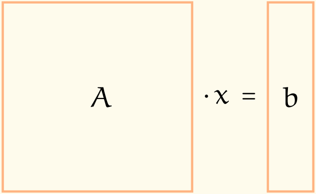
Atserias, Bulatov, Dawar $\mathrm{Slv}(\mathbf{G}) \notin \mathrm{FP{+}C}$

Dawar, Grohe, Holm, Laubner $\mathrm{FP{+}C} \lneq \mathrm{FP{+}rk} \leq \mathrm{PTIME}$

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

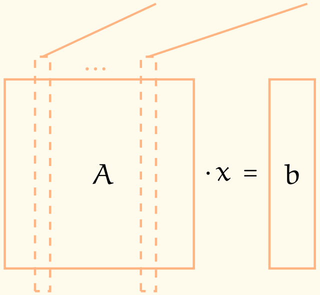
Atserias, Bulatov, Dawar $\mathsf{Slv}(\mathbf{G}) \notin \mathsf{FP{+}C}$

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

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 $\quad \mathsf{Slv}(\mathbf{G}) \notin \mathsf{FP{+}C}$

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

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

A logic for polynomial time

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

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

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 $a_1 \cdot \mathbf{c}_1 + \cdots + a_r \cdot \mathbf{c}_r + a \cdot \mathbf{b} = \mathbf{0}$

Rings Many notions (linear dependence, McCoy, inner rank, ...), unknown complexity, above characterisation fails

Groups Undefined

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

Definability of solvability problems

(1) Inter-definability: $\rightsquigarrow$ natural domain for Slv

Theorem

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

Definability of solvability problems

(1) Inter-definability: $\rightsquigarrow$ natural domain for Slv

Theorem

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

(2) Intra-definability: $\rightsquigarrow$ FO extended by $\mathsf{Slv}_{\mathsf{F}}$

Theorem

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

Definability of solvability problems

(1) Inter-definability: $\rightsquigarrow$ natural domain for Slv

Theorem

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

(2) Intra-definability: $\rightsquigarrow$ FO extended by $\mathsf{Slv}_{\mathsf{F}}$

Theorem

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

(3) Supra-definability: $\rightsquigarrow$ reducing Slv to a uniform problem

Theorem

$\mathsf{Slv}(\star), \mathsf{rk}(\mathbf{F}) \xRightarrow{\text{FO-red.}} \mathsf{GM}$ (group membership)

Inter-definability: a natural class for solvability

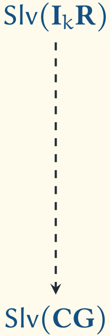
$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: 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 ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



Inter-definability: a natural class for solvability

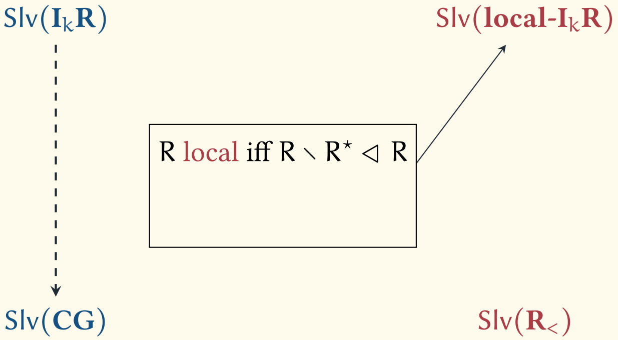
$\mathsf{Slv}(\mathbf{CG})$: Cyclic groups ($\mathbb{Z}_{p^e}$)

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

Inter-definability: a natural class for solvability

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

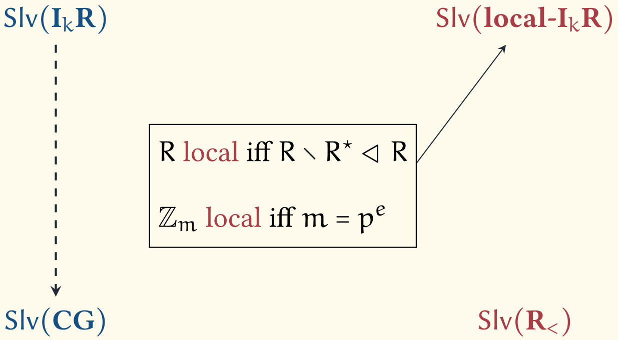
Slv($\mathbf{I}_k\mathbf{R}$): k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



Inter-definability: a natural class for solvability

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

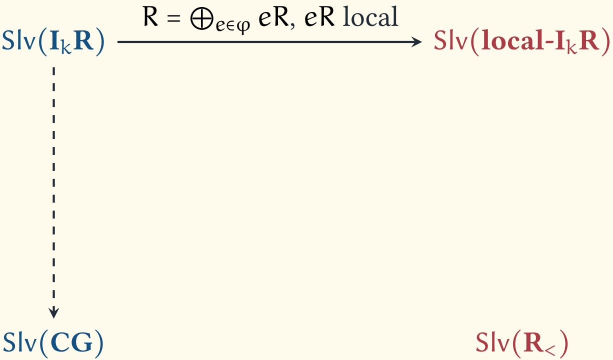
$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



Inter-definability: a natural class for solvability

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

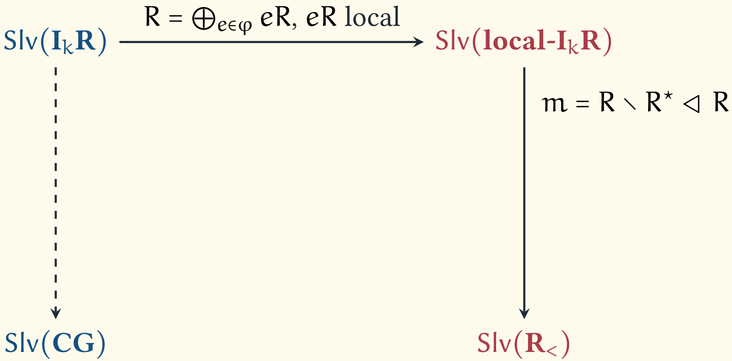
$\mathsf{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



Inter-definability: a natural class for solvability

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

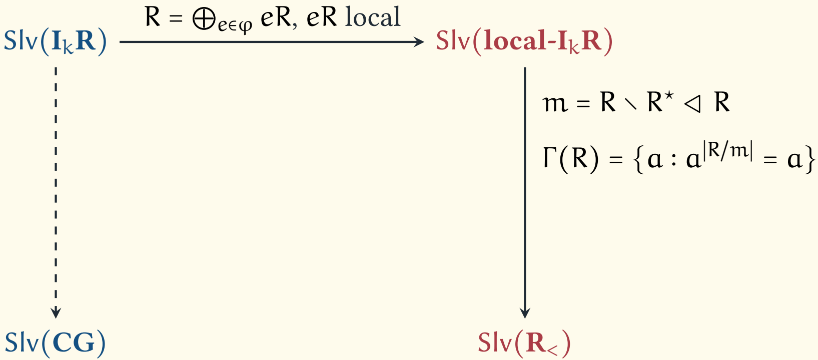
$\mathrm{Slv}(\mathbf{I}_k\mathbf{R})$: k-gen. ideal rings ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)



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 ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \xrightarrow{R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}} \mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R})$

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

$\mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \longrightarrow \mathsf{Slv}(\mathbf{R}_<)$, where:

$\mathfrak{m} = R \setminus R^\star \lhd R$

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

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

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 ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$\mathrm{Slv}(\mathbf{I}_k\mathbf{R}) \xrightarrow{R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}} \mathrm{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R})$

$\mathrm{Slv}(\mathbf{I}_k\mathbf{R}) \dashrightarrow \mathrm{Slv}(\mathbf{CG})$

$\mathrm{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \longrightarrow \mathrm{Slv}(\mathbf{R}_<)$:

$\mathfrak{m} = R \setminus R^\star \lhd R$

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

$\Gamma(R) \tilde{\to} R/\mathfrak{m},\ r \mapsto r + \mathfrak{m}$

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

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 ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$$\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \xrightarrow{R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}} \mathsf{Slv}(\mathbf{local\text{-}I}_k\mathbf{R})$$

$\mathsf{Slv}(\mathbf{local\text{-}I}_k\mathbf{R}) \longrightarrow \mathsf{Slv}(\mathbf{R}_<)$:

$$\mathfrak{m} = R \setminus R^\star \lhd R$$

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

$$\Gamma(R) \tilde{\to} R/\mathfrak{m}, r \mapsto r + \mathfrak{m}$$

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

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

$$(R, +) = \oplus_{g \in \psi} \langle g \rangle$$

$$(A, \mathbf{b}) \mapsto (A_1, \mathbf{b_1}), \ldots, (A_k, \mathbf{b_k})$$

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

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 ($I \lhd R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

$\mathsf{Slv}(\mathbf{I}_k\mathbf{R}) \xrightarrow{R = \bigoplus_{e \in \varphi} eR,\ eR \text{ local}} \mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R})$

$\mathsf{Slv}(\textbf{local-}\mathbf{I}_k\mathbf{R}) \longrightarrow \mathsf{Slv}(\mathbf{R}_<)$:

$\mathfrak{m} = R \setminus R^\star \lhd R$

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

$\Gamma(R) \tilde{\to} R/\mathfrak{m},\ r \mapsto r + \mathfrak{m}$

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

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

$(R, +) = \oplus_{g \in \psi} \langle g \rangle$

$(A, \mathbf{b}) \mapsto (A_1, \mathbf{b_1}), \ldots, (A_k, \mathbf{b_k})$

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

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

Intra-definability: solvability as a logical operator

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

Intra-definability: solvability as a logical operator

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

$$\Downarrow$$

FO+slv : First-order logic closed under solvability quantifier

$\mathrm{FO{+}slv}_F$: 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 $\mathsf{FO}+\mathsf{slv}_\mathsf{F}$-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)

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

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

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: (negation)

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

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

Gaussian elimination implies:

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

Intra-definability: solvability as a logical operator

Theorem

Every FO+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)

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

$$\boxed{\ \varphi\ } \cdot \mathbf{v_y} = \begin{bmatrix}1\\ \vdots \\ 1\end{bmatrix}$$

$$\boxed{\ \psi\ } \cdot \mathbf{v_y} = \begin{bmatrix}1\\ \vdots \\ 1\end{bmatrix}$$

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)

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

$$\begin{array}{l} \boxed{\varphi} \cdot \mathbf{v_y} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \\ \boxed{\psi} \cdot \mathbf{v_y} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \end{array} \rightsquigarrow \left[\begin{array}{c|c} \varphi & \mathbf{0} \\ \hline \mathbf{0} & \psi \end{array}\right] \cdot \mathbf{v_{yy}} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

Intra-definability: solvability as a logical operator

Theorem

Every FO+slv_F-formula is equivalent to a formula of the form

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

Proof illustration: (universal quantification)

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

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

$$\vdots$$

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

Intra-definability: solvability as a logical operator

Theorem

Every 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: (universal quantification)

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

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

Intra-definability: solvability as a logical operator

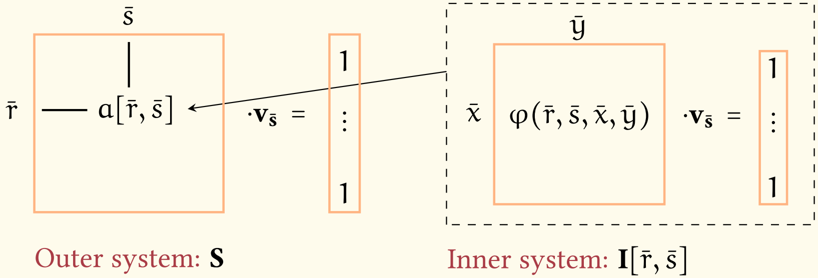
Theorem

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

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

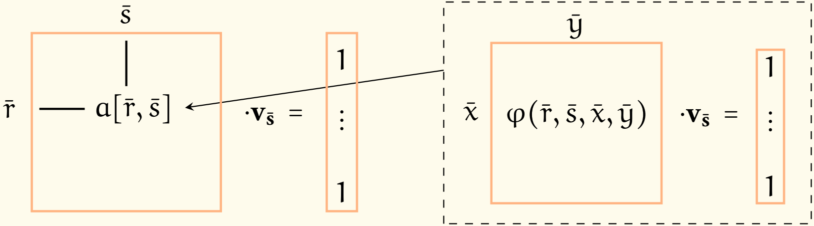
Proof illustration: (nesting of solvability)

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



Proof illustration: (nesting of solvability)

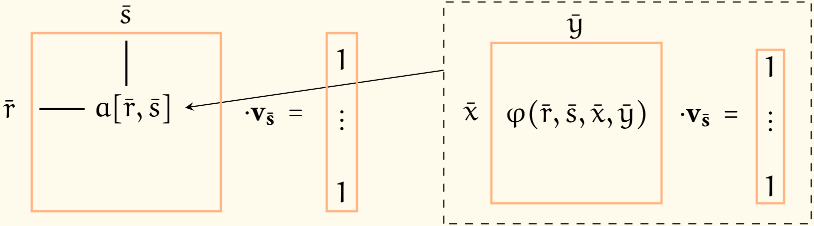
$$\mathsf{slv}(\bar{r}, \bar{s}).\left[\mathsf{slv}(\bar{x}, \bar{y}).\left[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), \mathbf{1}\right], \mathbf{1}\right]$$



Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

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

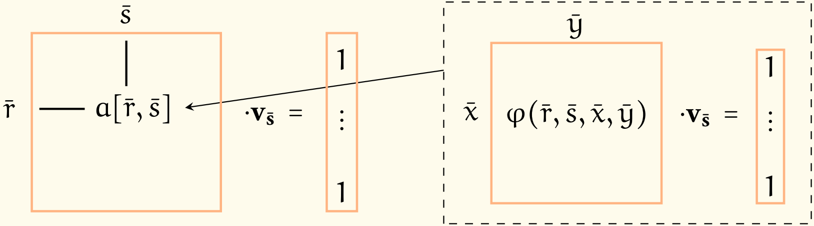


For $\bar{r}$: $\sum_{\bar{s}} \underbrace{a[\bar{r}, \bar{s}] \cdot v_{\bar{s}}} = 1$

Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

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



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

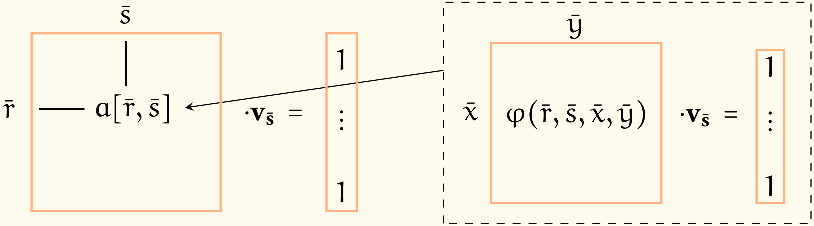
$\rightsquigarrow$

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

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)

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

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

$\rightsquigarrow$

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

Consistency conditions:

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

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

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

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

Consistency conditions:

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

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

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

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

From solvability to group membership

Permutation group membership (GM)

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

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

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

From solvability to group membership

Permutation group membership (GM)

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

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

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

Theorem

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

$$\mathsf{FO}$$

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

From solvability to group membership

Theorem

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

$$\mathsf{FO}$$

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

From solvability to group membership

Theorem

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

$$\text{FO}$$

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

$$\bar{s} \in J$$

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

From solvability to group membership

Theorem

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

FO

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

$\bar{s} \in J$

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

linear system is solvable

$$\iff$$

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

From solvability to group membership

Theorem

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

$$\text{FO}$$

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

$\bar{s} \in J$

$$\bar{r} \in I \quad \left[\ \mathbf{c}_{\bar{s}} := \ \right] \cdot \begin{bmatrix} \vdots \\ x_{\bar{s}} \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ b_{\bar{r}} \\ \vdots \end{bmatrix}$$

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 $\iota : (D, +)^I \to S_{I \times D}$

From solvability to group membership

Outlook: FP + nice operator for GM

- Extension of FP+rk (strict?)
- *All* solvability problems for linear equation systems definable

From solvability to group membership

Outlook: FP + nice operator for GM

- Extension of FP+rk (strict?)
- *All* solvability problems for linear equation systems definable
- Graph isomorphism (bounded colour class size, degree)?

From solvability to group membership

Outlook: FP + nice operator for GM

- Extension of FP+rk (strict?)
- *All* solvability problems for linear equation systems definable
- Graph isomorphism (bounded colour class size, degree)?
- Tractable cases of constraint satisfaction problems?

From solvability to group membership

Outlook: FP + nice operator for GM

- Extension of FP+rk (strict?)
- *All* solvability problems for linear equation systems definable
- Graph isomorphism (bounded colour class size, degree)?
- Tractable cases of constraint satisfaction problems?
- Difficulty: What is nice ?

Definability of polynomial-time problems from algebra