universität innsbruck

Automata and Logic

Aart Middeldorp and Johannes Niederhauser

Outline

Definitions

- $\mathrm{FV}(\varphi)$ denotes list of free variables in φ in fixed order with first-order variables preceding second-order ones
- assignment for φ with $\mathrm{FV}(\varphi) = (x_1, \dots, x_m, X_1, \dots, X_n)$ is tuple $(i_1, \dots, i_m, I_1, \dots, I_n)$ such that $i_1, \dots, i_m$ are elements of $\mathbb{N}$ and $I_1, \dots, I_n$ are finite subsets of $\mathbb{N}$
- assignments are identified with strings over $\{0,1\}^{m+n}$
- string over $\{0,1\}^{m+n}$ is m-admissible if first m rows contain exactly one 1 each

Remarks

- every m-admissible string x induces assignment $\underline{x}$
- every assignment is induced by (not necessarily unique) m-admissible string: if x is m-admissible then $x\mathbf{0}$ is m-admissible and $\underline{x} = \underline{x\mathbf{0}}$

Lemma

set of m-admissible strings over $\{0,1\}^{m+n}$ is regular and accepted by DFA $\mathcal{A}_{m,n}$

Definition

$L_a(\varphi) = \{x \in (\{0,1\}^{m+n})^* \mid x \text{ is } m\text{-admissible and } \underline{x} \vDash \varphi\}$

Theorem

$L_a(\varphi)$ is regular for every WMSO formula φ

Definitions

- homomorphism $\mathsf{drop}_i \colon (\{0,1\}^k)^* \to (\{0,1\}^{k-1})^*$ is defined for $1 \leqslant i \leqslant k$ by dropping i-th component from vectors in $\{0,1\}^k$
- $\mathsf{stz}(A) = \{x \mid x\mathbf{0}\cdots\mathbf{0} \in A\} \supseteq A$ for $A \subseteq (\{0,1\}^{m+n})^*$ "shorten trailing zeros"

Lemma

$A \subseteq (\{0,1\}^k)^*$ is regular $\implies$ $\text{stz}(A)$ is regular

Final Task

transform $L_a(\varphi)$ into $L(\varphi)$ for WMSO formula φ with $\text{FV}(\varphi) = \{P_a \mid a \in \Sigma^*\}$ using regularity preserving operations

Procedure

① eliminate assignments which do not correspond to string in Σ^*

② map strings in 0^*10^* to elements of Σ using homorphism $h\colon \{0,1\}^{|\Sigma|} \to \Sigma$ which maps 0^k10^l to $k{+}1$-th element of Σ

Lemma

$L(\varphi) = h(L_a(\varphi) \cap \{0^k10^l \mid k+1+l = |\Sigma|\}^*)$ is regular

Corollary

WMSO definable sets are regular

MONA

- MONA is state-of-the-art tool that implements decision procedures for WS1S and WS2S
- WS1S is weak monadic second-order theory of 1 successor = WMSO

Automata

- (deterministic, non-deterministic, alternating) finite automata
- regular expressions
- (alternating) Büchi automata

Logic

- (weak) monadic second-order logic
- Presburger arithmetic
- linear-time temporal logic

Outline

Definition

formulas of Presburger arithmetic

$$\varphi ::= \bot \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \exists\, x.\, \varphi \mid t_1 = t_2 \mid t_1 < t_2$$

$$t ::= 0 \mid 1 \mid t_1 + t_2 \mid x$$

Examples

1. $\exists\, y.\, x = y + y + y + 1$
2. $\forall\, x.\, (\exists\, y.\, x = y + y) \vee (\exists\, y.\, x + 1 = y + y)$

Abbreviations

$$\varphi \wedge \psi := \neg(\neg\varphi \vee \neg\psi) \qquad \varphi \rightarrow \psi := \neg\varphi \vee \psi \qquad \top := \neg\bot$$

$$\forall\, x.\, \varphi := \neg\exists\, x.\, \neg\varphi \qquad t_1 \leqslant t_2 := t_1 < t_2 \vee t_1 = t_2$$

$$n := \underbrace{1 + \cdots + 1}_{n} \qquad n\, x := \underbrace{x + \cdots + x}_{n} \qquad \text{for } n > 1$$

Definitions

- assignment α is mapping from first-order variables to $\mathbb{N}$
- extension to terms: $\alpha(0) = 0 \quad \alpha(1) = 1 \quad \alpha(t_1 + t_2) = \alpha(t_1) + \alpha(t_2)$
- assignment α satisfies formula φ ($\alpha \vDash \varphi$):

$$
\begin{array}{lcl}
\alpha \nvDash \bot & & \\
\alpha \vDash \neg\varphi & \iff & \alpha \nvDash \varphi \\
\alpha \vDash \varphi_1 \vee \varphi_2 & \iff & \alpha \vDash \varphi_1 \text{ or } \alpha \vDash \varphi_2 \\
\alpha \vDash \exists\, x.\, \varphi & \iff & \alpha[x \mapsto n] \vDash \varphi \text{ for some } n \in \mathbb{N} \\
\alpha \vDash t_1 = t_2 & \iff & \alpha(t_1) = \alpha(t_2) \\
\alpha \vDash t_1 < t_2 & \iff & \alpha(t_1) < \alpha(t_2)
\end{array}
$$

Remark

$t_1 < t_2$ can be modeled as $\exists\, x.\, x \neq 0 \wedge t_1 + x = t_2$

Remark

every $t_1 = t_2$ can be written as $a_1 x_1 + \cdots + a_n x_n = b$ with $a_1, \ldots, a_n, b \in \mathbb{Z}$

Side Remark

Presburger arithmetic admits complete first-order axiomatization:

- $\forall\, x.\, x + 1 \neq 0$
- $\forall\, x.\, \forall\, y.\, x + 1 = y + 1 \rightarrow x = y$
- induction

$$\psi(0) \wedge \forall\, x.\, (\psi(x) \rightarrow \psi(x+1)) \rightarrow \forall\, x.\, \psi(x)$$

  for every formula $\psi(x)$ with single free variable x
- $\forall\, x.\, x + 0 = x$
- $\forall\, x.\, \forall\, y.\, x + (y + 1) = (x + y) + 1$

Example (Frobenius Coin Problem)

given natural numbers $a_1, \ldots, a_n > 0$

$$(\forall y. x < y \rightarrow \exists x_1. \ldots \exists x_n. a_1 x_1 + \cdots + a_n x_n = y) \land \neg(\exists x_1. \ldots \exists x_n. a_1 x_1 + \cdots + a_n x_n = x)$$

expresses largest number x that does not satisfy $a_1 x_1 + \cdots + a_n x_n = x$ for some $x_1, \ldots, x_n \in \mathbb{N}$

Theorem (Presburger 1929)

Presburger arithmetic is decidable

Decision Procedures

- quantifier elimination
- automata techniques
- translation to WMSO

Example

Presburger arithmetic formula φ: $x + 2y - 3z = 2$

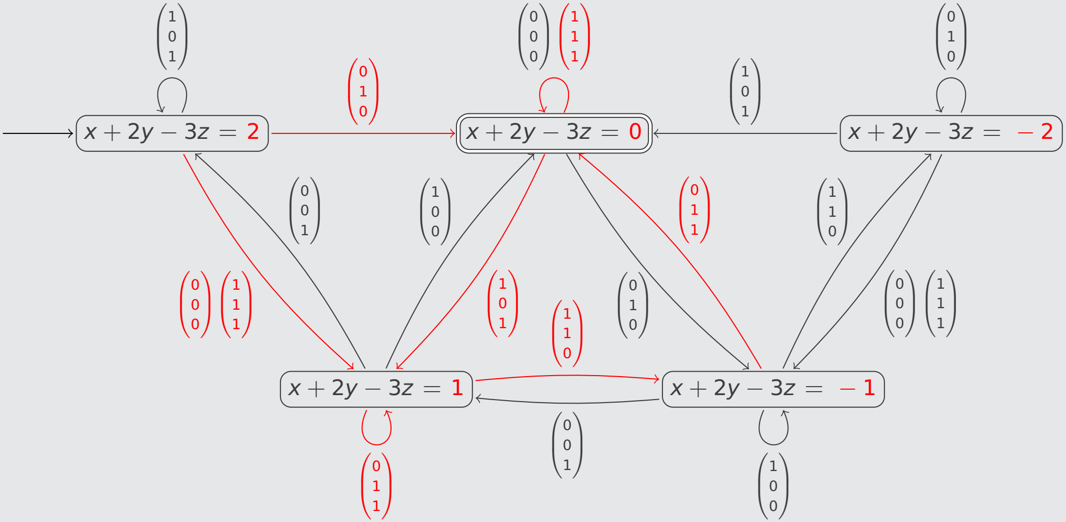
some accepted strings:

- $\begin{pmatrix}0\\1\\0\end{pmatrix}$ $\quad x = 0 \quad y = 1 \quad z = 0$
- $\begin{pmatrix}0\\1\\0\end{pmatrix}\begin{pmatrix}1\\1\\1\end{pmatrix}$ $\quad x = (10)_2 = 2 \quad y = (11)_2 = 3 \quad z = (10)_2 = 2$
- $\begin{pmatrix}1\\1\\1\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}$ $\quad x = (0101)_2 = 5 \quad y = (1111)_2 = 15 \quad z = (1011)_2 = 11$

some rejected strings:

- $\begin{pmatrix}0\\0\\0\end{pmatrix}$ $\quad x = 0 \quad y = 0 \quad z = 0$
- $\begin{pmatrix}0\\1\\0\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}$ $\quad x = (010)_2 = 2 \quad y = (101)_2 = 5 \quad z = (110)_2 = 6$

Example (cont'd)



Definition (Representation)

- sequence of n natural numbers is represented as string over

$$\Sigma_{n} = \{(b_1 \cdots b_n)^{\mathrm{T}} \mid b_1, \dots, b_n \in \{0,1\}\}$$

- $x = \begin{pmatrix} b_1^1 \\ \vdots \\ b_n^1 \end{pmatrix} \begin{pmatrix} b_1^2 \\ \vdots \\ b_n^2 \end{pmatrix} \cdots \begin{pmatrix} b_1^m \\ \vdots \\ b_n^m \end{pmatrix} \in \Sigma_n^*$ represents $x_1 = (b_1^m \cdots b_1^2 b_1^1)_2, \dots, x_n = (b_n^m \cdots b_n^2 b_n^1)_2$
- $\underline{x} = (x_1, \dots, x_n)$

Example

- $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ represents $x_1 = 10$, $x_2 = 7$, $x_3 = 6$
- $x_1 = 1$, $x_2 = 2$, $x_3 = 3$ is represented by $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, $\dots$

Definition

for Presburger arithmetic formula φ with $\mathrm{FV}(\varphi) = (x_1, \ldots, x_n)$

$$L(\varphi) = \{x \in \Sigma_n^* \mid \underline{x} \vDash \varphi\}$$

Theorem (Presburger 1929)

Presburger arithmetic is decidable

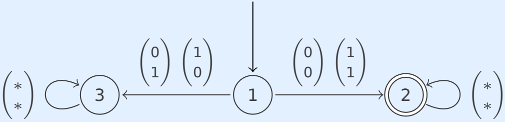
Proof Sketch

- construct finite automaton A_φ for every Presburger arithmetic formula φ
- induction on φ
- $L(A_\varphi) = L(\varphi)$

Outline

Question

Consider the following automaton A:



For which of the following formulas φ does $L(A) = L(\varphi)$ hold ?

A $x = y$

B $x + y > 0$

C $\exists z.\, x + y = 2z$

D $(\exists z.\, x = 2z \wedge \forall z.\, \neg(y = 2z)) \vee (\exists z.\, y = 2z \wedge \forall z.\, \neg(x = 2z))$

Outline

Definition (Automaton for Atomic Formula)

DFA $A_\varphi = (Q, \Sigma_n, \delta, s, F)$ for $\varphi(x_1, \dots, x_n)$: $a_1x_1 + \cdots + a_nx_n = b$

- $Q \subseteq \{i \mid |i| \leqslant |b| + |a_1| + \cdots + |a_n|\} \cup \{\bot\}$
- $\delta(i, (b_1 \cdots b_n)^\mathsf{T}) = \begin{cases} \dfrac{i - (a_1b_1 + \cdots + a_nb_n)}{2} & \text{if } i - (a_1b_1 + \cdots + a_nb_n) \text{ is even} \\ \bot & \text{if } i - (a_1b_1 + \cdots + a_nb_n) \text{ is odd or } i = \bot \end{cases}$
- $s = b$
- $F = \{0\}$

Lemma

if $\delta(i, (b_1 \cdots b_n)^\mathsf{T}) = j$ then $a_1x_1 + \cdots + a_nx_n = j \iff a_1(2x_1 + b_1) + \cdots + a_n(2x_n + b_n) = i$

Theorem

1. A_φ is well-defined
2. $L(A_\varphi) = L(\varphi)$

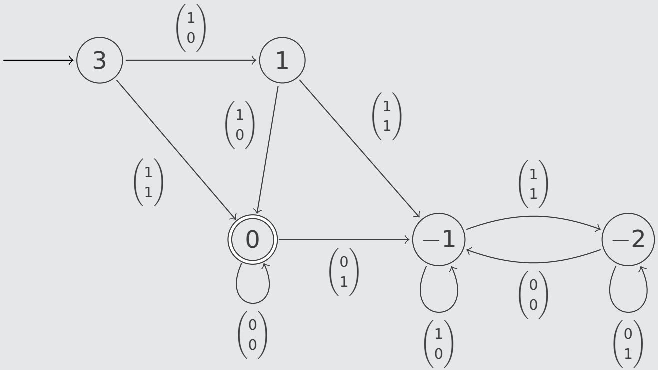
Example

$\varphi(x,y)\colon\ x + 2y = 3$

- $Q = \{3, \perp, 1, 0, -1, -2\} \qquad s = 3 \qquad F = \{0\}$
- $\delta(3, \binom{0}{0}) = \delta(3, \binom{0}{1}) = \perp \quad \delta(3, \binom{1}{0}) = 1 \quad \delta(3, \binom{1}{1}) = 0$
- $\delta(\perp, \binom{0}{0}) = \delta(\perp, \binom{0}{1}) = \delta(\perp, \binom{1}{0}) = \delta(\perp, \binom{1}{1}) = \perp$
- $\delta(1, \binom{0}{0}) = \delta(1, \binom{0}{1}) = \perp \quad \delta(1, \binom{1}{0}) = 0 \quad \delta(1, \binom{1}{1}) = -1$
- $\delta(0, \binom{1}{0}) = \delta(0, \binom{1}{1}) = \perp \quad \delta(0, \binom{0}{0}) = 0 \quad \delta(0, \binom{0}{1}) = -1$
- $\delta(-1, \binom{0}{0}) = \delta(-1, \binom{0}{1}) = \perp \quad \delta(-1, \binom{1}{0}) = -1 \quad \delta(-1, \binom{1}{1}) = -2$
- $\delta(-2, \binom{1}{0}) = \delta(-2, \binom{1}{1}) = \perp \quad \delta(-2, \binom{0}{0}) = -1 \quad \delta(-2, \binom{0}{1}) = -2$

Example

$\varphi(x, y)\colon\ x + 2y = 3$



Theorem

1. A_φ is well-defined
2. $L(A_\varphi) = L(\varphi)$

Proof

- $q \in Q \subseteq \{i \mid |i| \leqslant |b| + |a_1| + \cdots + |a_n|\} \cup \{\bot\}$ and $b' = (b_1 \cdots b_n)^T \in \Sigma_n$
- if $q = \bot$ or $i - (a_1 b_1 + \cdots + a_n b_n)$ is odd then $\delta(q, b') = \bot$
- suppose $q = i$ with $|i| \leqslant |b| + |a_1| + \cdots + |a_n|$ and $i - (a_1 b_1 + \cdots + a_n b_n)$ is even

$$\delta(i, b') = \frac{i - (a_1 b_1 + \cdots + a_n b_n)}{2} \in Q$$

$$\begin{aligned} |i - (a_1 b_1 + \cdots + a_n b_n)| &\leqslant |i| + |a_1 b_1| + \cdots + |a_n b_n| \\ &\leqslant |i| + |a_1| + \cdots + |a_n| \\ &\leqslant 2\,(|b| + |a_1| + \cdots + |a_n|) \end{aligned}$$

Outline

Boolean Operations

boolean operation	automata construction	
$\neg$	complement	C
$\wedge$	intersection	I
$\vee$	union	U

Example

Presburger arithmetic formula

$$\neg((x + 2y - 3z \neq 2 \;\wedge\; 2x - y + z = 3) \;\vee\; x - 3y - z \neq 1))$$

is implemented as

$$\mathsf{C}(\mathsf{U}(\mathsf{I}(\mathsf{C}(A_{x+2y-3z=2}), A_{2x-y+z=3}), \mathsf{C}(A_{x-3y-z=1})))$$

Example

Presburger arithmetic formula

$$x + 2y - 3z = 2 \ \wedge \ x + 2y = 3$$

- $A_{x+2y-3z=2}$ operates on alphabet $\Sigma_3 = (\{0,1\}^3)^\mathsf{T}$
- $A_{x+2y=3}$ operates on alphabet $\Sigma_2 = (\{0,1\}^2)^\mathsf{T}$
- before intersection can be computed $A_{x+2y=3}$ needs to operate on Σ_3

Definition (Cylindrification)

$\mathrm{C}_i(R) \subseteq \Sigma_{n+1}^*$ is defined for $R \subseteq \Sigma_n^*$ and index $1 \leqslant i \leqslant n+1$ as

$$\mathrm{C}_i(R) = \left\{ x_1 \cdots x_m \in \Sigma_{n+1}^* \;\middle|\; \mathrm{drop}_i(x_1) \cdots \mathrm{drop}_i(x_m) \in R \right\}$$

with $\mathrm{drop}_i\big((b_1 \cdots b_{n+1})^\mathsf{T}\big) = (b_1 \cdots b_{i-1} b_{i+1} \cdots b_{n+1})^\mathsf{T}$

Example

- $L(A_{x+2y=3}) = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}^*$
- $L(\mathrm{C}_3(A_{x+2y=3})) = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\} \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}^*$

Lemma

if $R \subseteq \Sigma_n^*$ is regular then $\mathrm{C}_i(R) \subseteq \Sigma_{n+1}^*$ is regular for every $1 \leqslant i \leqslant n+1$

Remark

- drop_i is homomorphism from Σ_{n+1}^* to Σ_n^*
- $\mathrm{C}_i(R) = \mathrm{drop}_i^{-1}(R)$

Outline

Definition (Projection)

$\Pi_i(R) \subseteq \Sigma_n^*$ is defined for $R \subseteq \Sigma_{n+1}^*$ and index $1 \leqslant i \leqslant n+1$ as

$$\Pi_i(R) = \{\mathrm{drop}_i(x_1) \cdots \mathrm{drop}_i(x_m) \in \Sigma_n^* \mid x_1 \cdots x_m \in R\}$$

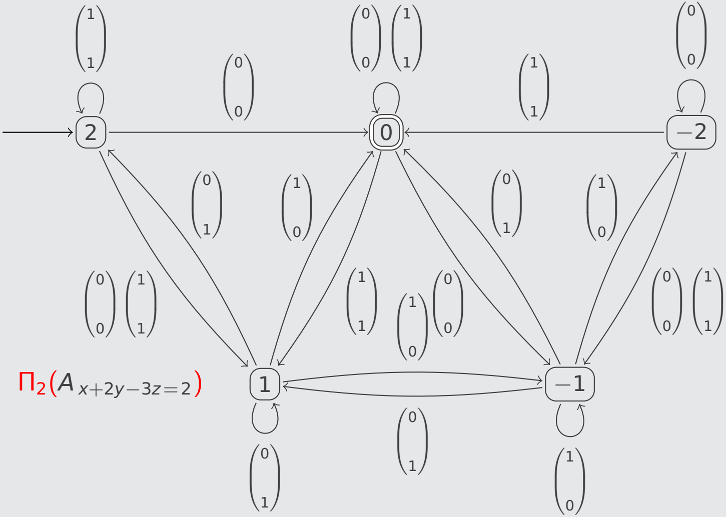
Lemma

if $R \subseteq \Sigma_{n+1}^*$ is regular then $\Pi_i(R) \subseteq \Sigma_n^*$ is regular for every $1 \leqslant i \leqslant n+1$

Example

1. solutions of $\exists\, y.\, x + 2y - 3z = 2$ correspond to $\mathrm{stz}(\Pi_2(A_{x+2y-3z=2}))$
2. solutions of $\forall\, y.\, x + 2y - 3z = 2$ correspond to $\mathrm{C}(\mathrm{stz}(\Pi_2(\mathrm{C}(A_{x+2y-3z=2}))))$

Example



$\Pi_2(A_{x+2y-3z=2})$

Outline

Theorem (Presburger 1929)

Presburger arithmetic is decidable

Decision Procedures

- quantifier elimination
- automata techniques
- translation to WMSO

Procedure

- map variables in Presburger arithmetic formula to second-order variables in WMSO
- n is represented as set of "1" positions in reverse binary notation of n
- 0 and 1 in Presburger arithmetic formulas are translated into ZERO and ONE with

$$\forall x.\, \neg \mathrm{ZERO}(x) \qquad\qquad \forall x.\, \mathrm{ONE}(x) \leftrightarrow x = 0$$

- $+$ in Presburger arithmetic formula is translated into ternary predicate P_+ with

$$\begin{aligned} P_+(X,Y,Z) \; := \exists\, C.\, \neg C(0) \wedge \big(\forall\, x.\, C(x+1) \leftrightarrow X(x) \wedge Y(x) \vee X(x) \wedge C(x) \vee Y(x) \wedge C(x)\big) \wedge \\ \big(\forall\, x.\, Z(x) \leftrightarrow X(x) \wedge Y(x) \wedge C(x) \vee X(x) \wedge \neg Y(x) \wedge \neg C(x) \vee \\ \neg X(x) \wedge Y(x) \wedge \neg C(x) \vee \neg X(x) \wedge \neg Y(x) \wedge C(x)\big) \end{aligned}$$

Example

26 is represented by $\{1,3,4\}$ since $(26)_2 = 11010$

Example

Presburger arithmetic formula $\exists\, y.\, x = y + y + 1$ is transformed into WMSO formula

$$\big(\forall\, x.\, \mathrm{ONE}(x) \leftrightarrow x = 0\big) \;\wedge\; \exists\, Y.\, \exists\, Z.\, P_+(Y, Y, Z) \wedge P_+(Z, \mathrm{ONE}, X)$$

Corollary

Presburger arithmetic is decidable

Outline

1. **Summary of Previous Lecture**
2. **Presburger Arithmetic**
3. **Intermezzo**
4. **Presburger Arithmetic**
5. **WMSO**
6. **Further Reading**

Boudet and Comon

- Diophantine Equations, Presburger Arithmetic and Finite Automata, Proc. 21st International Colloquium on Trees in Algebra and Programming, LNCS 1059, pp. 30–43, 1996

Esparza and Blondin

- Chapter 9 of Automata Theory: An Algorithmic Approach (MIT Press 2023)

Important Concepts

- A_φ
- $L(\varphi)$
- cylindrification
- projection
- Presburger arithmetic

homework for November 22