Quantifier Elimination for Presburger Arithmetic

- We used DFAs as data structures to manipulate $Sol(\varphi)$ and thus decide satisfiability of φ
- We will see now an alternative proof obtained using tools from Logics. This proof will offer new insights on PA.
- Consider a closed formula $\varphi \in PA[<, =, \equiv_k]$. The difficult part in deciding satisfiability of φ is finding witnesses in $\mathbb{N}$ for the existentially quantified variables.
- On the other hand, if φ is quantifier-free, deciding satisfiability is easy: no variables, just check numerical constraints.
- APPROACH: show that existential quantifiers can be replaced by checking the constraints on some finite set of possible witnesses.
Roughly speaking we can always find a finite set of 'candidate witnesses' $W \subseteq \mathbb{N}$ such that $\exists x: \psi \equiv \bigvee_{n \in W} \psi[^n/_x]$. Using the result, we can decide sat. of φ by obtaining an equivalent quantifier-free formula φ' on which sat. is easily checked.

Theorem (Presburger 1929)

For each formula $\varphi(\vec{z}) \in PA[<, =, \equiv_k]$ we can effectively construct $\psi(\vec{z}) \in PA[<, =, \equiv_k]$ that is quantifier-free and logically equivalent to $\varphi(\vec{z})$.

The proof is by showing that from formula $\exists x: \varphi(x, \vec{z})$, where φ is quantifier free, we can obtain an equivalent quant-free formula $\psi(\vec{z})$. Then by induction on quantifier depth we obtain the result.

Proof (of Presburger's theorem):

Consider formula $\exists x : \varphi(x, \bar{y})$,

where $\varphi(x, \bar{y})$ is quantifier-free.

Step 1: Normalize formula

↳ Transform $\varphi(x, \bar{y})$ into negation normal form (NNF), where negation only applies to atomic propositions.

↳ Eliminate negation:

$$\neg(t_1 = t_2) \quad \text{iff} \quad t_1 < t_2 \lor t_2 < t_1$$

$$\neg(t_1 < t_2) \quad \text{iff} \quad t_1 = t_2 \lor t_2 < t_1$$

$$\neg(t_1 \equiv_m t_2) \quad \text{iff} \quad t_1 \equiv_m t_2 + 1 \lor t_1 \equiv_m t_2 + 2 \lor \ldots \lor t_1 \equiv_m t_2 + (m-1)$$

↳ Compute DNF of the resulting formula:

$\exists x : \gamma_1 \lor \ldots \lor \gamma_n$ where γ_i = conjunction of atomic formulas.

$\equiv \exists x : \gamma_1 \lor \ldots \lor \exists x : \gamma_n.$

$\boxed{\text{From now on, focus on a single } \exists x\, \gamma}$

↳ Let $\exists x : \gamma = \exists x : \alpha_1 \land \ldots \land \alpha_n$

where each α_i is atomic.

↳ Wlog. assume x occurs in each α_i, and each α_i has one of the following forms

$$nx + t = u$$

$$nx + t \equiv_m u$$

$$nx + t < u$$

$$u < nx + t,$$

where $n \geq 1$ and u, t terms (that may be 0) that do not contain x.

As in the construction of Presburger automata, add subtraction and write

$$\begin{aligned} nx &= u-t \\ nx &\equiv_m u-t \\ nx &< u-t \\ u-t &< nx \end{aligned}$$

(Shortcuts for the formulas where the terms are on the correct side)

Step 2: Uniformize and eliminate coefficients on x:

↳ We have

$$\exists x: \alpha_1 \wedge \dots \wedge \alpha_n$$

with coefficients $n_1, \dots, n_n$ on x

↳ Compute

$$p := \text{lcm}(n_1, \dots, n_n).$$

least common multiple

↳ Transform each α_i so that coefficient of x is p:

$$nx = u - t$$

$$\text{iff} \quad \frac{p}{n} nx = \frac{p}{n} u - \frac{p}{n} t$$

integer since $n \mid p$.

For modulo:

$$nx \equiv_m u - t$$

$$\text{iff} \quad \frac{p}{n} nx \equiv_{(\frac{p}{n} \cdot m)} \frac{p}{n} u - \frac{p}{n} t$$

↳ Replace px by new variable y and add $y \equiv_p 0$:

$$px = u' - t'$$

is replaced by

$$y = u' - t'$$

$$\wedge \ y \equiv_p 0.$$

<u>Intuition</u> We obtain a formula that uses x only in terms px so we can give px a name $y = px$ and require the existence of y instead of x. But to recover the existence of x from the existence of y we need to find a witness for y that is a multiple of p:

$$\exists x : 5x = t \wedge 5x < t' \rightsquigarrow \exists y : y = t \wedge y < t' \wedge y \equiv_5 0$$

Overall, we transformed

$$\exists x : \alpha_1 \wedge \ldots \wedge \alpha_m \quad \text{into} \quad \exists y : \alpha_1' \wedge \ldots \wedge \alpha_m' \wedge \overbrace{y \equiv_p 0}^{\alpha_{m+1}'}$$

The formula is now in the form, for some finite sets of indices

$I_< \uplus I_> \uplus I_= \uplus I_\equiv = \{1, \ldots, m+1\}$:

$$\exists y : \bigwedge_{i \in I_<} L_i < y \text{ (lower bounds)}$$

$$\wedge \bigwedge_{i \in I_>} y < U_i \text{ (upper bounds)}$$

$$\wedge \bigwedge_{i \in I_\equiv} y \equiv_{k_i} V_i \text{ (congruences)}$$

$$\wedge \bigwedge_{i \in I_=} y = T_i \text{ (equalities)}$$

where $L_i = r_i' - s_i'$, $U_i = t_i' - u_i'$, $V_i = v_i' - w_i'$, $T_i = q_i' - p_i'$

terms that may only reference the free variables of the original formu[la] but not y

Case (a) $\exists j \in I_=$ i.e. there is a $y = T_j$

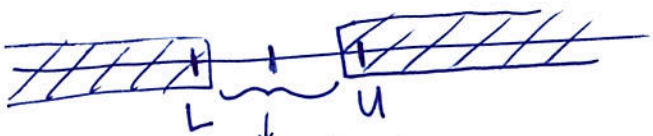
Then we can apply the substitution $[T_j/y]$ in all clauses and replace α_j' with $p_j' \leqslant q_j'$ to ensure that $y = T_j$ could be sat by some positive natural

The formula we obtain does not contain y anymore so we can remove the existential quantifier $\exists y$ DONE ✓

Case (b) $I_= = \emptyset$ i.e. there are no equalities.

Case $\boxed{b.1}$ $I_\equiv = \emptyset$ i.e. there are no congruences neither:

we only need to ensure that the lower and upper bounds can be satisfied, namely that for each $L \in \{L_i\}_{i \in I_<}$ and $U \in \{U_i\}_{i \in I_>}$



there is at least one number $\in \mathbb{N}$ in here

We can require that using the quantifier free formula

$$\bigwedge_{i \in I_<} \bigwedge_{j \in I_>} L_i + 1 < U_j \wedge \bigwedge_{j \in I_>} 0 < U_j$$

Case $\boxed{b.2}$ $I_{\equiv} \neq \emptyset$ we have to find witnesses within the bounds that also satisfy some congruences.

i) Compute $M = lcm\{k_i\}_{i \in I_{\equiv}}$ the least common multiplier of all the congruences $\equiv_{k_i}$

ii) This M satisfies

$$a + M \equiv_{k_i} a \quad \text{for all } a \in \mathbb{N} \text{ and all } k_i \quad i \in I_{\equiv}$$

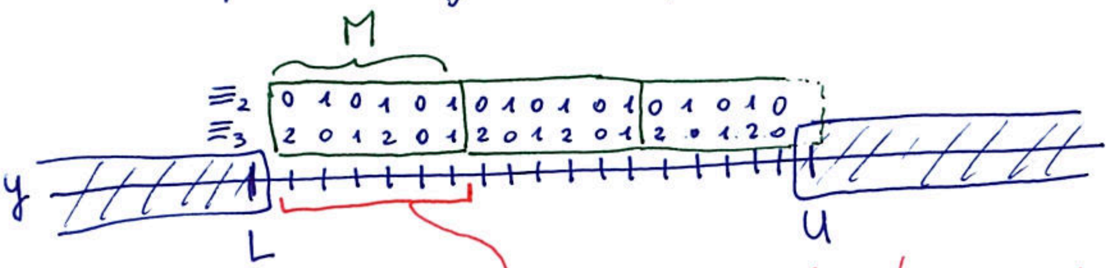
that is, M identifies the length after which the congruences see a repeating pattern, for example with $\equiv_2$ and $\equiv_3$

$M = 6$:

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$\equiv_2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	...
$\equiv_3$	0	1	2	0	1	2	0	1	2	0	1	2	0	1	...

recurring pattern of length M

iii) We need to stipulate the existence of a natural number within all bounds L and U (in $\{L_i\}_{i \in I_<}$ and $\{U_i\}_{i \in I_>}$ resp.) that satisfies some congruences with period M:



(I) If there is a witness, there is a small witness (close to L)

(II) If there is a witness sat. the congruence you can find it also within M steps from L

CAVEAT: To handle the case when $L_i + M$ is negative for all i we add $L' = r' - s'$ with $r' = 0$ $s' = 1$ (i.e. injecting $-1 < y$) without altering the truth value of the formula

Now we can replace the $\exists y$ quantifier by some tests to look for witnesses around the lower bounds, i.e. in the finite set $L_i + q$ with $i \in I_<$ and $q \in \{1, \dots, M\}$ transforming $\exists y : \alpha_1' \wedge \dots \wedge \alpha_{m+1}'$ into

$$\bigvee_{i \in I_<} \bigvee_{q=1}^{M} \Big[\bigwedge_{j \in I_<} L_j < \overbrace{L_i + q}^{\text{one of the possible witnesses}}$$

$$\wedge \bigwedge_{j \in I_>} L_i + q < U_j$$

witness satisfies all the bounds

$$\wedge \bigwedge_{j \in I_\equiv} L_i + q \equiv_{k_i} V_i \Big]$$

witness satisfies congruences

$\square$

<u>Example</u>: $\varphi(z) = \forall x : (2x < z+1 \to x = 0) \wedge z > 0$

$\equiv \neg \exists x : \neg (\neg 2x < z+1 \vee x = 0) \wedge z > 0$ NNF inside $\exists x$

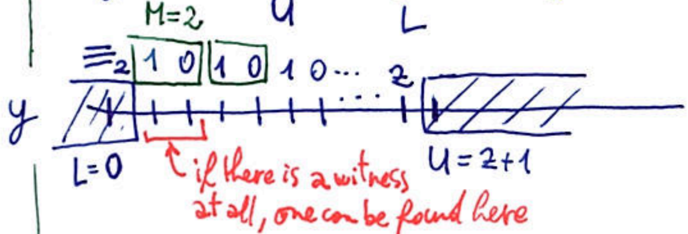
$\equiv \neg \exists x : 2x < z+1 \wedge \neg(x=0) \wedge z > 0$ REMOVE Negation around atomic form

$\equiv \neg \exists x : 2x < z+1 \wedge (x > 0 \vee \underbrace{x < 0}_{\text{false}}) \wedge z > 0$

$\equiv \neg \exists x : (2x < z+1 \wedge 1 \cdot x > 0) \wedge z > 0$ APPLY PRESBURGER THEOREM

$\exists x : \; 2x < z+1 \wedge 0 < 1 \cdot x \quad p = lcm(2,1) = 2 \quad y = 2x$

$\equiv \exists y : \; y < \underbrace{z+1}_{U} \wedge \underbrace{0}_{L} < y \wedge y \equiv_2 0$



$\equiv (0 < 0+1 \wedge 0+1 < z+1 \wedge \overbrace{0+1 \equiv_2 0}^{\text{false}})$

$\vee (\underbrace{0 < 0+2}_{\text{true}} \wedge 0+2 < z+1 \wedge \underbrace{0+2 \equiv_2 0}_{\text{true}})$

$\equiv 2 < z+1 \equiv 1 < z$

So overall

$\varphi(z) \equiv \neg(1 < z) \wedge z > 0$

$\equiv (z = 1 \vee z < 1) \wedge z > 0$

$\equiv z = 1$ which is quantifier free! ✓

Examples:

1.) $\exists y : (1 < y \wedge y < 100 \wedge y \equiv_2 1 \wedge y \equiv_3 2)$

↳ is in required form

↳ Coefficients 1

↳ There is no $=$ on y

↳ There are congruences

Case 3.b.2:

· Compute

$$M := \mathrm{lcm}(2,3) = 6$$

· Replace $\exists$-quantified formula by

$$\bigvee_{q=0}^{5} (1 < 1+q \wedge 1+q < 100 \wedge 1+q \equiv_2 1 \wedge 1+q \equiv_3 2)$$

$$\boxed{\begin{array}{l} \underline{q = 4} \\ 1 < 5 \wedge 5 < 100 \wedge 5 \equiv_2 1 \wedge 5 \equiv_3 2 \end{array}}$$

2.) $\exists x : (w < 4x \wedge 2x < u \wedge 3x < v \wedge x \equiv_3 t)$

where w, u, v, t terms without x.

↳ is in the required form

Step 2: Uniformize and eliminate coefficients:

· Compute $p := \mathrm{lcm}(4,2,3) = 12$

$$\cdot\ \exists x : \Big(\tfrac{12}{4} w < \tfrac{12}{4} 4x \wedge \tfrac{12}{2} 2x < \tfrac{12}{2} u \wedge \tfrac{12}{3} 3x < \tfrac{12}{3} v \wedge \tfrac{12}{1} x \equiv_{\frac{12}{1}\cdot 3} \tfrac{12}{1} t$$

$$= \exists x : (3w < 12x \wedge 12x < 6u \wedge 12x < 4v \wedge 12x \equiv_{36} 12t)$$

Replace $12x$ by variable y:

$$\exists y : (3w < y \wedge y < 6u \wedge y < 4v \wedge y \equiv_{36} 12t \wedge y \equiv_{12} 0)$$

↳ There is no $=$ on y

<u>Case 3.5.2</u>: <u>There are congruences</u>:

- Compute
  $$M := \mathrm{lcm}(36, 12) = 36.$$
- Add lower bound
  $$\exists y : (3w < y \wedge 0-1 < y \wedge y < 6u \wedge y < 4v \wedge y \equiv_{36} 12t \wedge y \equiv_{12} 0)$$
- <u>Replace</u> <u>quantifier on y</u>:

$$\bigvee_{q=0}^{35} (3w < 3w+q \wedge 0-1 < 3w+q \wedge 3w+q < 6u \wedge 3w+q < 4v \wedge 3w+q \equiv_{36} 12t \wedge 3w+q \equiv_{12} 0)$$

$$\vee \bigvee_{q=0}^{35} (3w < (0-1)+q \wedge 0-1 < (0-1)+q \wedge (0-1)+q < 6u \wedge (0-1)+q < 4v \wedge (0-1)+q \equiv_{36} 12t \wedge (0-1)+q \equiv_{12} 0)$$