Shostak's Generalization to $ax+by \leq c$

- Create a node in a graph for each variable
- For each constraint $ax+by \leq c$ create an <u>undirected</u> edge labelled with the constraint
- A path is admissible if adjacent edges

  $ax+by \leq c$ and $dy+ez \leq f$

  have $\text{sign}(b) \neq \text{sign}(d)$
- The residue of a path is obtained by applying transitivity to the path.

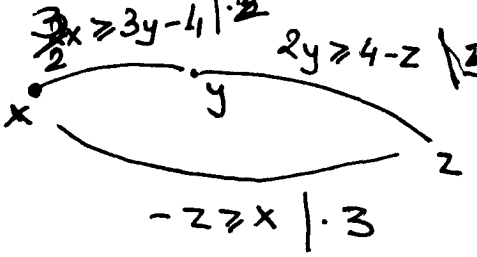
  e.g.
  $$\begin{array}{rl} ax+by \leq c & \mid \cdot\,|d| \\ dy+ez \leq f & \mid \cdot\,|b| \\ \hline a\cdot|d|\cdot x + e\cdot|b|\,z \leq c\cdot|d| + f\cdot|b| & \end{array}$$

  (since $b\cdot|d| + d\cdot|b| = 0$)

- If a simple loop (one with distinct nodes) has the residue

  $0 \leq n$ where $n < 0$

  then the set of constraints is not satisf.

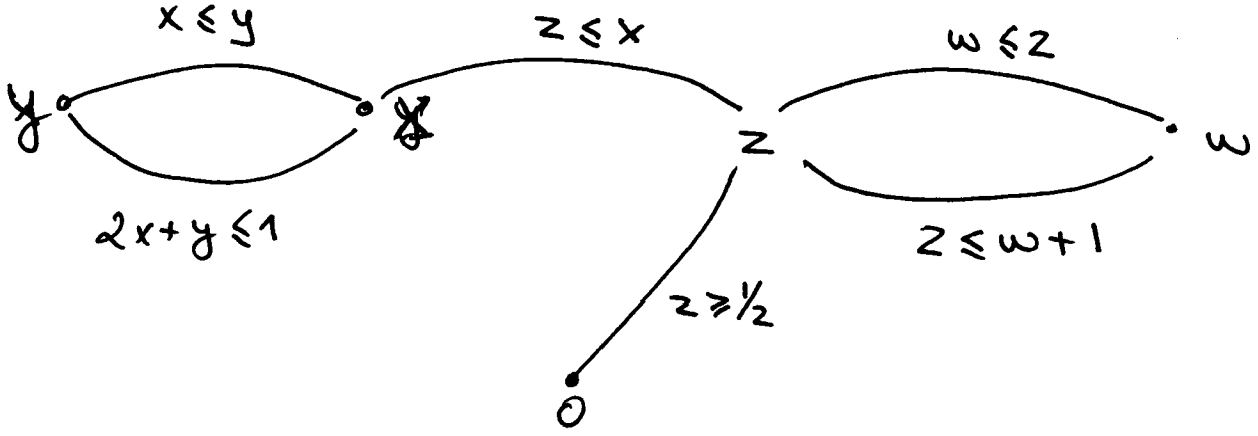


Residue of loop

$0 \geq 4$

Converse is not true

- there are graphs with no infeasible loops but that are unsatisfiable nevertheless



But ~~$w \leq z \wedge z \leq w+1$~~

$x \leq y \wedge 2x+y \leq 1 \Rightarrow 3x \leq 1$

$\Leftrightarrow$

$3z \leq 1$

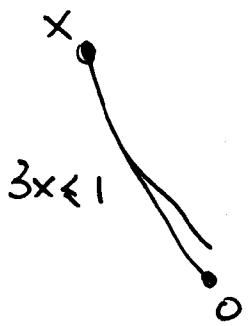
$\Leftrightarrow$

$z \leq \frac{1}{3}$ Contra with $z \geq \frac{1}{2}$

Idea

Augment the graph with the residues of all admissible loops.

Above residue for $x \supset y$ is $3x \leq 1$



This creates an infeasible loop.

Algorithm

- find simple admissible loops. For each.
  if feasible add an edge with its residue.
  otherwise answer unsat

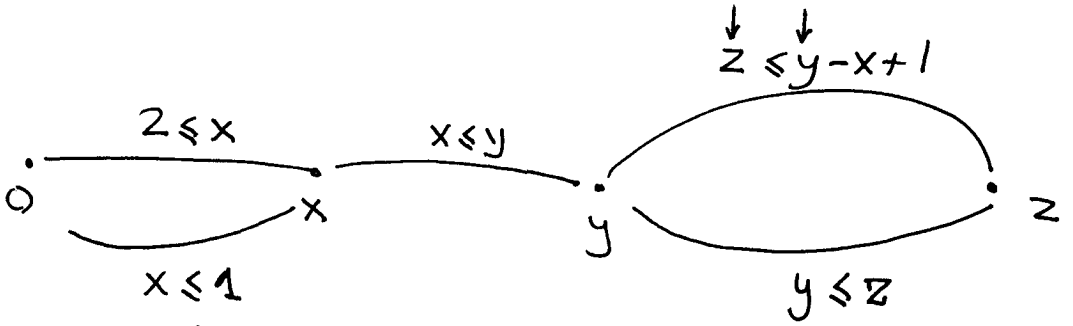
Theorem this alg. is sound and complete.
See Shostak, "Deciding Linear Inequalities by Computing Loop Residues"
JACM vol 28/4 10/81 p. 769-779

Notes

- In the case when all constraints are $x - y \leq c$
  - admissible loops are those in the directed graph of Pratt's alg.
  - no new residue edges need to be added
- Complexity is that of finding loops.
  $$O(e \cdot (n+m))$$
  - e is exponential in worst case
- There is a modification due to Asprall and Shiloach that avoids considering all cycles. Resulting complexity is $O(n^3 \cdot m^2 \cdot$ [illegible]$)$

Extension of Shostak to ~~three variables~~ more than two variables per constraint.

- Pick an ordering of variables.
- In each constraint pick the "~~first~~" two "smaller" variables as primary
- Compute the loop residues as before



residue of $y \leq z$ $2 \leq y - x + 1$

$2 \leq 1$ is the residue of $2 \leq x$ and $x \leq 1$

- Any set of inequalities can be reduced polynomially to a set of inequalities with at most 3 variables / inequality

The SUP-INF satisfiability procedure

- Only sketch here

  See · Bledsoe, "The SUP-INF method in Presburger arithmetic"
  (Tech. Rept. ATP-18, Math, U.T. Austin, 74

  · Shostak, "On the SUP-INF Method for Presburger Formulas"
  JACM 24/4 10/1977, pp 529--543

- Idea

  · Given a set of linear inequality constraints S

  · For each variable x compute

  $SUP_S(x)$ - the maximal value taken by x on all interpretations that satisfy S

  $INF_S(x)$ - the minimal value ...

  SUP/INF are computed recursively

  · Separate S as following

  $$x \geq A_i \cdot \bar{x} + b_i \qquad x \leq B_j \cdot \bar{x} + c_j$$

  Define $SUP(x) = SUP(\min_j (B_j \cdot \bar{x} + c_j))$

  $$= \min_j (SUP(B_j \cdot \bar{x} + c_j))$$

  · Check that $\lceil INF(x) \rceil \leq \lfloor SUP(x) \rfloor$

  If not, then unsatisfiable.

Intuition of SUP-INF

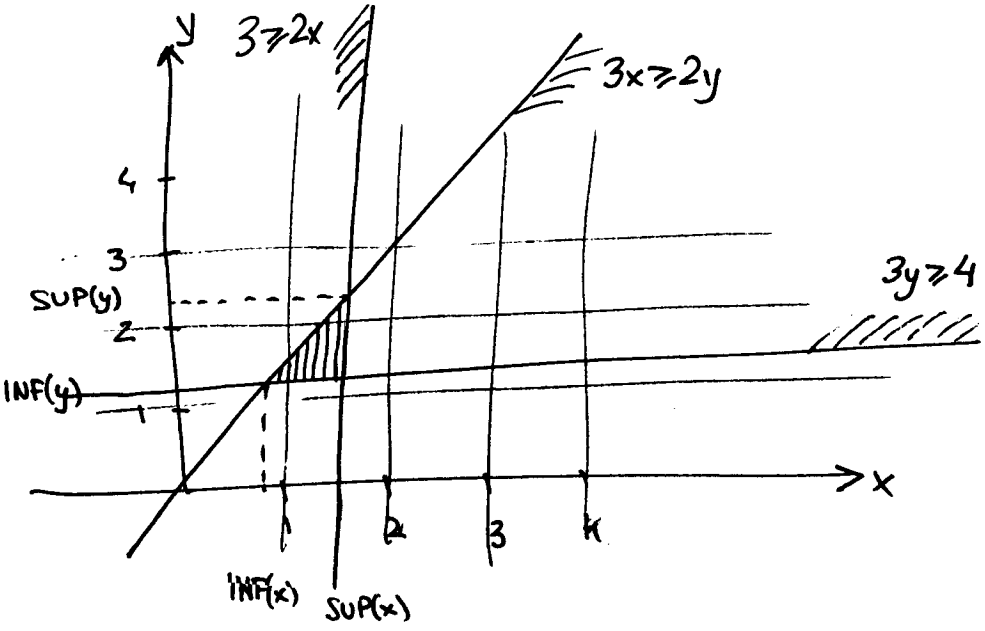
- a set of inequality constraints with n variable denotes a convex polyhedron in $\mathbb{R}^n$
- $[INF(x_k), SUP(x_k)]$ is the projection on the x_k axis of the polyhedron
- If some projection does not contain integer points there could be no satisfiable assignments

Example

$3x \geq 2y$

$3y \geq 4$

$3 \geq 2x$



$SUP(x) = SUP\left(\frac{3}{2}\right) = \frac{3}{2}$ $\quad (2x \leq 3 \in S)$

$INF(x) = INF\left(\frac{2y}{3}\right) = \frac{2}{3} \cdot INF(y) = \frac{2}{3} \cdot INF\left(\frac{4}{3}\right) = \frac{8}{9}$ $\quad (3y \geq 4)$

$SUP(y) = SUP\left(\frac{3}{2} \cdot x\right) = \frac{3}{2} \cdot SUP(x) = \frac{9}{4}$

$INF(y) = \frac{4}{3}$

$\lceil INF(x) \rceil = 1 \leq 1 = \lfloor SUP(x) \rfloor \Rightarrow x \in \{1\}$

$\lceil INF(y) \rceil = 2 \leq 2 = \lfloor SUP(y) \rfloor \Rightarrow y \in \{2\}$

Seems satisfiable

- But it is not
- SUP-INF is also not complete for $\mathbb{Z}$
- Shostak's improvement
  - if $\lceil INF(x) \rceil = \lfloor SUP(x) \rfloor$
    replace x by $\lceil INF(x) \rceil$
- Example: $x \rightarrow 1$

$3 \cdot 1 \geq 2y$ $\quad INF(y) = \frac{4}{3}$

$3y \geq 4$

~~$3 \geq 2 \cdot 1$~~ $\quad SUP(y) = \frac{3}{2}$

$\Rightarrow$ No integer solution

- However this does not guarantee completeness for $\mathbb{Z}$
  - But makes it less likely we are going to be hitting the incompleteness.

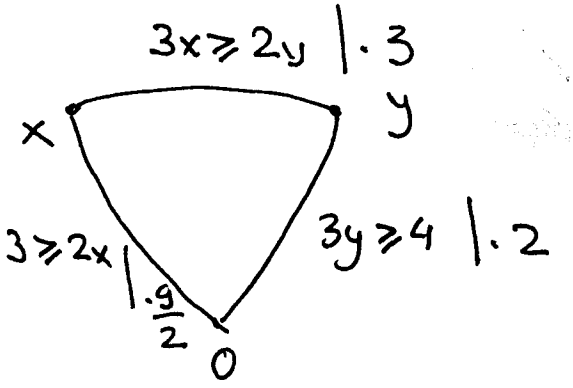
An Example (Same as before)

$3x \geq 2y$

$3y \geq 4$

$3 \geq 2x$

Shostak



- cycle is admissible
- residue $3 \cdot (3x \geq 2y) + 2 \cdot (3y \geq 4) + \frac{9}{2} \cdot (3 \geq 2x)$

$$= \frac{27}{2} \geq 8$$

⇒ system is satisfiable.

But not in $\mathbb{Z}$!!

⇒ Shostak is not complete for $\mathbb{Z}$

It is sound: If C is not sat in R then it is not sat in $\mathbb{Z}$.

Conclusion

- Most efficient sat. proc. for arithmetic are not complete for $\mathbb{Z}$
- Not surprising, since IP is NP-complete
- It is rare in practice to hit on a problem that is sat. in $\mathbb{R}$ but not in $\mathbb{Z}$
- Easy remedies to help
  - $ax > b \longrightarrow x \geq \lceil \frac{b}{a} \rceil$ (a is > 0)

This strengthens the constraint!

If it was not sat in $\mathbb{Z}$ it might make it unsat in $\mathbb{R}$

Fourier-Motzkin Elimination

(Fourier 1824, Motzkin 1936)

Consider a set of linear inequalities.
Pick a variable x and let the rest be $\bar{x}$
Partition the set of inequalities according to the sign of x:

$$x - A_i \bar{x} \geq 0 \qquad i = 1, \ldots, m$$
$$-x + B_j \cdot \bar{x} \geq 0 \qquad j = 1, \ldots, n$$
$$C_k \cdot \bar{x} \geq 0 \qquad k = 1, \ldots, p$$

This set of inequality is satisfiable iff

$$(B_j - A_i)\,\bar{x} \geq 0 \qquad \begin{matrix} i = 1, \ldots, m \\ j = 1, \ldots, n \end{matrix}$$
$$C_k \cdot \bar{x} \geq 0$$

is satisfiable.

Proof The only interesting part is "if"

Since $(B_j - A_j)\,\bar{x} \geq 0$ means that

$$\max_i A_i \cdot \bar{x} \leq \min_j B_j \cdot \bar{x} \qquad (*)$$

Pick $x = \min_j B_j \cdot \bar{x}$

Then $\min_j B_j \cdot \bar{x} \geq A_i \cdot \bar{x}$ for all $i = 1, \ldots, m$

And $\min_j B_j \cdot \bar{x} \leq B_j \cdot \bar{x}$ for all $j = 1, \ldots, n$

Fourier-Motzkin is not used in practice because it leads to an exponential growth in the number of inequalities.

Fourier-Motzkin Elimination Example

(Postpone after discussing FMElim)

eliminate x

$$3y \geq 4$$
$$9 \geq 6x \geq 4y$$

eliminate y : $27 \geq 16$ ✓ $\Rightarrow$ satisfiable

- Just as before.
  Because FM can be seen as eliminating nodes and replacing all 2-edge ~~path~~ admissible paths through the node with their resolves.

$\Rightarrow$ FM is also not complete for $\mathbb{Z}$

~~Furthermore~~

Feasability Theorem

$A\bar{x} \geq \bar{b}$ is unsatisfiable iff there exists $\bar{c} \geq 0$ such that

$$A\bar{c} = 0 \quad \text{and} \quad \bar{c} \cdot \bar{b} > 0$$

(there exists a non-negative linear combination of input constraints that cancels all variables and produces a positive constant)

Proof

- "if" is simple
- "only if" $A\bar{x} \geq \bar{b}$ is unsat then
  - after every Fourier-Motzkin elimination step the system remains unsat.
  - eventualy we find an inequation

$$0 \geq c \quad \text{where} \quad c > 0.$$

But every inequation in a Fourier-Motzkin elim process is a non-negative linear combination of input inequalities.

□

The Fecsability theorem suggest a simple proof system for systems of linear inequalities

Given a set of linear inequalities $\sum_j a_{ij} \cdot x_j \geq b_i$ they entail false if there is a set of non-negative coefficients c_i such that

$$\sum_i c_i \cdot \left(\sum_j a_{ij} \cdot x_j - b_i \right) < 0$$

$$\sum_i c_i \cdot a_{ij} = 0 \quad \text{for all } j$$

$$\sum_i c_i \cdot b_i > 0$$

This is easy to check.

Thus the job of the satisfiability procedure is to select the input ineq. that multiplied by some coefficients leads to $0 < 0$.

Corrolary

To show that $\overline{C} \Rightarrow I$ need a set of positive coefficients a_i and d such that

$$\sum a_i C_i - d \cdot I \quad \text{simplifies to} \quad n \geq 0 \quad \text{for } n < 0$$

Back to proof generation for Pratt

- Recall the invariant

  if $\delta_{ij} < \infty$ then

  $P_{ij} = (x_k - x_\ell \le a, prf)$ such that

  $\delta_{ij} = \delta_{ik} + a + \delta_{\ell j}$

  and $prf : pf\,(x_k - x_\ell \le a)$

- $mkGeqProof(i, j) : pf\,(x_i - x_j \le \delta_{ij})$

  (if $\delta_{ij} < \infty$)

  - builds a list of inequalities along with positive coefficients that when added result in $x_i - x_j \le \delta_{ij}$

  if $i = j$ then $[]$ (and $\delta_{ii} = 0$)

  else

  let $(x_k - x_\ell \le a, prf) = P_{ij}$

  $(1, x_k - x_\ell \le a, prf) :: (mkGeqProof(i,k) \;@\; mkGeqProof(\ell, j))$

  list cons — list append

- coefficients will always ≥ 1 for Pratt

Proof generation for Shostak

Each loop residue is a positive linear combination of the loop inequalities

Shostak detects contradiction when a loop residue reduces to $n \geq 0$ for some $n < 0$

Need only keep track of what loop is the residue for.