universität innsbruck

SAT and SMT Solving

Sarah Winkler

Computational Logic Group
Department of Computer Science
University of Innsbruck

lecture 9
SS 2019

Outline

- Summary of Last Week
- Bounds for Integer Solutions
- Cutting Planes

Input to Satisfiability Problem for Equality Logic

conjunction φ of equality logic literals over set of variables V

Definitions

- $\varphi_=$ is set of positive literals (equality literals) in φ
- $\varphi_{\neq}$ is set of negative literals (inequality literals) in φ
- equality graph is undirected graph $G_=(\varphi) = (V, \varphi_=, \varphi_{\neq})$

Definitions

equality graph $G_=(\varphi) = (V, \varphi_=, \varphi_{\neq})$

- contradictory cycle is cycle with exactly one $\varphi_{\neq}$ edge
- contradictory cycle is simple if it contains no node twice

Lemma

φ is satisfiable iff $G_=(\varphi)$ contains no simple contradictory cycles

Idea (Branch and Bound)

- given $\mathbb{R}^2$ solution α, add constraints to exclude α but preserve $\mathbb{Z}^2$ solutions: if $a < \alpha(x) < a_1$, use Simplex on problems $C \wedge x \leqslant a$ and $C \wedge x \geqslant a + 1$
- might not terminate if solution space is unbounded

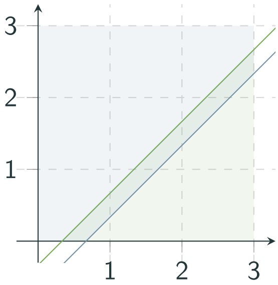
Algorithm BranchAndBound(φ)

Input: LIA constraint φ
Output: unsatisfiable, or satisfying assignment

let *res* be result of deciding φ over $\mathbb{R}$ ▷ e.g. by Simplex
if *res* is unsatisfiable **then**
    return unsatisfiable
else if *res* is solution over $\mathbb{Z}$ **then**
    return *res*
else
    let x be variable assigned non-integer value q in *res*
    res $=$ BranchAndBound($\varphi \wedge x \leqslant \lfloor q \rfloor$)
    return *res* $\neq$ unsatisfiable **?** *res* **:** BranchAndBound($\varphi \wedge x \geqslant \lceil q \rceil$)

Definition

Example



- $3x - 3y \geqslant 1 \wedge 3x - 3y \leqslant 2$
- unbounded problem
- no solution in $\mathbb{Z}^2$
- BranchAndBound does not terminate

Observation

- consider (potentially unbounded) linear arithmetic problem $A\vec{x} \leqslant \vec{b}$
- suppose we could compute bound c from A and $\vec{b}$ such that

$$\exists \vec{x} \in \mathbb{Z}^n \text{ with } A\vec{x} \leqslant \vec{b} \quad \Longrightarrow \quad \vec{x} \in \{-c, \ldots, c\}^n$$

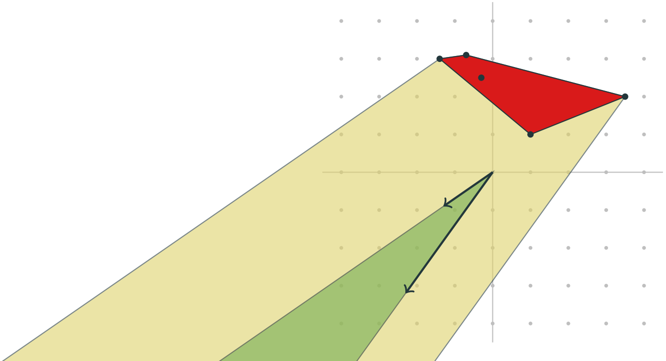
- obtain equisatisfiable bounded problem by adding $-c \leqslant x_i \leqslant c$

(material in the remainder of this section is by René Thiemann)

Definitions

- polytope: convex hull of finite set of vectors X

  smallest $V \supseteq X$ s.t. $\forall v, w \in V$, $0 \leqslant \lambda \leqslant 1$ have $v\lambda + (1-\lambda)w \in V$
- finitely generated cone: non-negative linear combinations of finite set of vectors V
- polyhedron: polytope + finitely generated cone



Roadmap

1. represent $\{\vec{x} \mid A\vec{x} \leqslant \vec{b}\}$ as $\mathit{hull}(X) + \mathit{cone}(V)$
   - using representation of $\{\vec{x} \mid A\vec{x} \leqslant \vec{0}\}$ as $\mathit{cone}(V)$
   - keep track of bounds
2. derive bound B for hull + cone representation:

$$(\mathit{hull}(X) + \mathit{cone}(V)) \cap \mathbb{Z}^n = \varnothing$$
$$\Longleftrightarrow$$
$$(\mathit{hull}(X) + \mathit{cone}(V)) \cap \{-B, \ldots, B\}^n = \varnothing$$

Integer Solutions of Polyhedra

Consider bounded set $X \subseteq \mathbb{Q}^n$ and $V \subseteq \mathbb{Z}^n$ such that $V = \{v_1, \ldots, v_n\}$

Notation

$C = \left\{ \sum_{i=1}^{n} \lambda_i \cdot v_i \mid v_i \in V \wedge 0 \leqslant \lambda_i \leqslant 1 \right\}$

yet to be proven ...

Theorem

$(Y + cone(V)) \cap \mathbb{Z}^n = \varnothing \iff (Y + C) \cap \mathbb{Z}^n = \varnothing$ *for Y convex*

Observation

- have $C \subseteq cone(V)$ by definition, so $(X + C) \subseteq (X + cone(V))$

Corollary

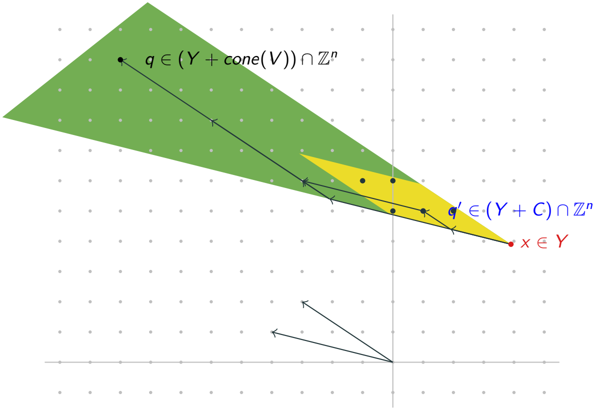
Suppose $|c| \leqslant b$ *for all coefficients* c *of vectors in* $X \cup V$.
For $B := b \cdot (1 + n)$ *have*

$$(hull(X) + cone(V)) \cap \mathbb{Z}^n = \varnothing \iff (hull(X) + C) \cap \mathbb{Z}^n = \varnothing$$
$$\iff (hull(X) + C) \cap \{-B, \ldots, B\}^n = \varnothing$$

Theorem

$(Y + cone(V)) \cap \mathbb{Z}^n = \varnothing \iff (Y + C) \cap \mathbb{Z}^n = \varnothing$ *for Y convex*

Proof (by picture).



Roadmap

1. represent $\{\vec{x} \mid A\vec{x} \leqslant \vec{b}\}$ as $hull(X) + cone(V)$
   - using representation of $\{\vec{x} \mid A\vec{x} \leqslant \vec{0}\}$ as $cone(V)$
   - keep track of bounds in this construction
2. derive bound B for hull + cone representation: ✓

$$(hull(X) + cone(V)) \cap \mathbb{Z}^n = \varnothing$$

$$\iff$$

$$(hull(X) + cone(V)) \cap \{-B, \ldots, B\}^n = \varnothing$$

Polyhedral Cones

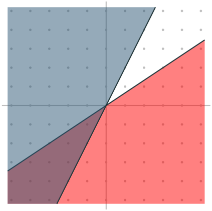
Definition

set of vectors C is polyhedral cone if $C = \{\vec{x} \mid A\vec{x} \leqslant \vec{0}\}$ for some matrix A

Lemma

C is polyhedral cone iff C is intersection of finitely many half-spaces

Example



$$A = \begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix}$$

$$2x - y \leqslant 0 \iff y \geqslant 2x$$

$$-2x + 3y \leqslant 0 \iff y \leqslant \frac{2}{3}x$$

i.e. $\exists v_1, \dots, v_m$ such that $C = cone(v_1, \dots, v_m)$

Theorem (Farkas, Minkowski, Weyl)

A cone C is polyhedral iff it is finitely generated

Aim

convert $\{\vec{x} \mid A\vec{x} \leqslant \vec{b}\}$ into $hull(X) + cone(V)$

Construction

- define polyhedral cone C

$$C = \left\{ \begin{pmatrix} \vec{x} \\ \tau \end{pmatrix} \middle| \tau \geqslant 0, A\vec{x} - \tau\vec{b} \leqslant \vec{0} \right\} = \left\{ \vec{y} \middle| \begin{pmatrix} A & -\vec{b} \\ \vec{0} & -1 \end{pmatrix} \vec{y} \leqslant \vec{0} \right\}$$

- using FMW theorem $\exists$ finite set of vectors such that

$$C = cone \left\{ \begin{pmatrix} x_1 \\ \tau_1 \end{pmatrix}, \dots, \begin{pmatrix} x_\ell \\ \tau_\ell \end{pmatrix}, \begin{pmatrix} u_1 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} u_k \\ 0 \end{pmatrix} \right\}$$

where all $\tau_i > 0$, so define $\vec{y}_i = \frac{1}{\tau_i}\vec{x}_i$ define $\vec{z}_j = |\prod \text{denominators of } \vec{u}_j| \cdot \vec{u}_j$, so z_j is integral

Claim

$\{\vec{x} \mid A\vec{x} \leqslant \vec{b}\} = hull\{\vec{y}_1, \dots, \vec{y}_\ell\} + cone\{\vec{z}_1, \dots, \vec{z}_k\}$

Claim

$\{\vec{x} \mid A\vec{x} \leqslant \vec{b}\} = \mathit{hull}\,\{\vec{y}_1, \ldots, \vec{y}_\ell\} + \mathit{cone}\,\{\vec{z}_1, \ldots, \vec{z}_k\}$

Proof.

$$C = \left\{ \begin{pmatrix} \vec{x} \\ \tau \end{pmatrix} \,\middle|\, \tau \geqslant 0, A\vec{x} - \tau\vec{b} \leqslant \vec{0} \right\} = \mathit{cone} \left\{ \begin{pmatrix} \vec{y}_1 \\ 1 \end{pmatrix}, \ldots, \begin{pmatrix} \vec{z}_1 \\ 0 \end{pmatrix}, \ldots \right\}$$

$$\begin{aligned} A\vec{x} \leqslant \vec{b} &\Longleftrightarrow \begin{pmatrix} \vec{x} \\ 1 \end{pmatrix} \in C \\ &\Longleftrightarrow \begin{pmatrix} \vec{x} \\ 1 \end{pmatrix} = \sum \lambda_i \begin{pmatrix} \vec{y}_i \\ 1 \end{pmatrix} + \sum \kappa_j \begin{pmatrix} \vec{z}_j \\ 0 \end{pmatrix} \text{ with } \lambda_1, \ldots, \kappa_1, \ldots \geqslant 0 \\ &\Longleftrightarrow \vec{x} = (\sum \lambda_i \vec{y}_i) + (\sum \kappa_j \vec{z}_j) \text{ with } \lambda_1, .. \geqslant 0,\ \sum \lambda_i = 1,\ \kappa_1, .. \geqslant 0 \\ &\Longleftrightarrow \vec{x} = \vec{y} + \vec{z} \text{ with } \vec{y} \in \mathit{hull}\,\{\vec{y}_1, \ldots\}, \vec{z} \in \mathit{cone}\,\{\vec{z}_1, \ldots\} \end{aligned}$$

∎

Roadmap

1. represent $\{\vec{x} \mid A\vec{x} \leqslant \vec{b}\}$ as $\mathit{hull}(X) + \mathit{cone}(V)$ ✓
   - using representation of $\{\vec{x} \mid A\vec{x} \leqslant \vec{0}\}$ as $\mathit{cone}(V)$
   - keep track of bounds in this construction
2. derive bound B for hull + cone representation: ✓

$$(\mathit{hull}(X) + \mathit{cone}(V)) \cap \mathbb{Z}^n = \varnothing$$

$$\iff$$

$$(\mathit{hull}(X) + \mathit{cone}(V)) \cap \{-B, \ldots, B\}^n = \varnothing$$

Bounds for FMW Theorem

Theorem (Farkas, Minkowski, Weyl)

A cone is polyhedral iff it is finitely generated.

Proof (construction)

$\Longleftarrow$: finitely generated implies polyhedral

for $\mathbb{Q}^3$ can take cross-product

- consider $cone(V)$ for $V = \{\vec{v}_1, \ldots, \vec{v}_m\} \subseteq \mathbb{Q}^n$
- for every set $W = \{\vec{w}_1, \ldots, \vec{w}_{n-1}\} \subseteq V$ of linearly independent vectors: compute vector $\vec{c}_W$ normal to hyper-space spanned by W
  - if $\vec{v}_i \cdot \vec{c}_W \leqslant 0$ for all i, then add $\vec{c}_W$ as row to A
  - if $\vec{v}_i \cdot \vec{c}_W \geqslant 0$ for all i, then add $-\vec{c}_W$ as row to A
- $cone(V) = \{\vec{x} \mid A\vec{x} \leqslant \vec{0}\}$

Theorem (Farkas, Minkowski, Weyl)

A cone is polyhedral iff it is finitely generated.

Proof (construction).

$\Longrightarrow$: polyhedral implies finitely generated

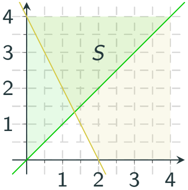
- consider $\{\vec{x} \mid A\vec{x} \leqslant \vec{0}\}$
- define W as the set of row vectors of A
- by first direction obtain B such that $cone\,(W) = \{\vec{x} \mid B\vec{x} \leqslant \vec{0}\}$
- define V as the set of row vectors of B
- $\{\vec{x} \mid A\vec{x} \leqslant \vec{0}\} = cone\,(V)$

∎

Example

- consider $x \leqslant y$ and $4 - 2x \leqslant y$

$$\underbrace{\begin{pmatrix} 1 & -1 & 0 \\ -2 & -1 & 4 \\ 0 & 0 & -1 \end{pmatrix}}_{A} \cdot \begin{pmatrix} x \\ y \\ \tau \end{pmatrix} \leqslant 0$$



- use proof of FMW theorem: compute $cone\,(W)$ for $W = \{w_1, w_2, w_3\}$

  $w_1 = (1 \quad -1 \quad 0)^T \qquad w_2 = (-2 \quad -1 \quad 4)^T \qquad w_3 = (0 \quad 0 \quad -1)^T$

  - $c_{12} = w_1 \times w_2 = (-4 \quad -4 \quad -3)$ is normal to w_1 and w_2

    $c_{12} \cdot w_1 = 0 \qquad c_{12} \cdot w_2 = 0 \qquad c_{12} \cdot w_3 = 3$
  - $c_{13} = w_1 \times w_3 = (1 \quad 1 \quad 0)$ is normal to w_1 and w_3

    $c_{13} \cdot w_1 = 0 \qquad c_{13} \cdot w_2 = -3 \qquad c_{13} \cdot w_3 = 0$
  - $c_{23} = w_2 \times w_3 = (1 \quad -2 \quad 0)$ is normal to w_2 and w_3

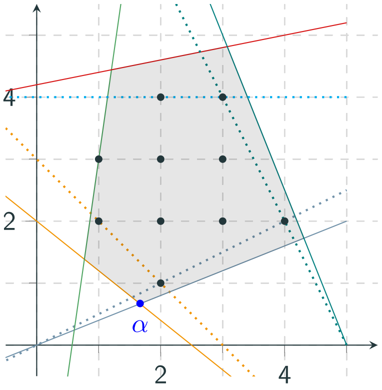
    $c_{23} \cdot w_1 = 3 \qquad c_{23} \cdot w_2 = 0 \qquad c_{23} \cdot w_3 = 0$

- for $B = \begin{pmatrix} 4 & 4 & 3 \\ 1 & 1 & 0 \\ -1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} v_1^T \\ v_2^T \\ v_3^T \end{pmatrix}$ have $cone\,(W) = \{\vec{x} \mid B\vec{x} \leqslant 0\}$
- $\{\vec{x} \mid A\vec{x} \leqslant 0\} = cone\,(\{v_1, v_2, v_3\}) = cone\,(\{(\frac{4}{3} \quad \frac{4}{3} \quad 1)^T, (1 \quad 1 \quad 0)^T, (-1 \quad 2 \quad 0)^T\})$
- $S = hull\,(\frac{4}{3} \quad \frac{4}{3})^T + cone\,\{(1 \quad 1)^T, (-1 \quad 2)^T\}$
- $S \cap \mathbb{Z}$ has bound $B := b \cdot (1 + n) = 2 \cdot 3 = 6$, where b is maximal coefficient in cone+hull

Outline

- Summary of Last Week
- Bounds for Integer Solutions
- Cutting Planes

Example



Definition (Cut)

given solution α to problem over $\mathbb{R}^n$, cut is inequality $a_1 x_1 + \cdots + a_n x_n \leqslant b$ which is not satisfied by α but by every $\mathbb{Z}^n$-solution

Method

like in BranchAndBound, keep adding cuts until integer solution found

Gomory Cuts: Assumptions

- Simplex returned solution α from final tableau A and basic B, nonbasic N

$$A\vec{x}_N = \vec{x}_B \tag{1}$$

$$-\infty \leqslant l_i \leqslant x_i \leqslant u_i \leqslant +\infty \tag{2}$$

- for some $i \in B$ variable x_i is assigned $\alpha(x_i) \notin \mathbb{Z}$
- for all $j \in N$ value $\alpha(x_j)$ is l_j or u_j

Notation

- write $c = \alpha(x_i) - \lfloor \alpha(x_i) \rfloor$
- by assumption all nonbasic variables are assigned bounds, so can split

$$L = \{ j \in N \mid \alpha(x_j) = l_j \} \qquad U = \{ j \in N \mid \alpha(x_j) = u_j \}$$

$$L^+ = \{ j \in L \mid A_{ij} \geqslant 0 \} \qquad U^+ = \{ j \in U \mid A_{ij} \geqslant 0 \}$$

$$L^- = \{ j \in L \mid A_{ij} < 0 \} \qquad U^- = \{ j \in U \mid A_{ij} < 0 \}$$

Lemma (Gomory Cut)

cut is given by inequality

$$\sum_{j \in L^+} \frac{A_{ij}}{1-c}(x_j - l_j) - \sum_{j \in U^-} \frac{A_{ij}}{1-c}(u_j - x_j) - \sum_{j \in L^-} \frac{A_{ij}}{c}(x_j - l_j) + \sum_{j \in U^+} \frac{A_{ij}}{c}(u_j - x_j) \geqslant 1$$

$$A\vec{x}_N = \vec{x}_B \tag{1}$$

$$-\infty \leqslant l_i \leqslant x_i \leqslant u_i \leqslant +\infty \tag{2}$$

Proof (1)

- consider potential integer solution $\vec{x}$ to (1) and (2)
- $\vec{x}$ satisfies i-th row of (1):

$$x_i = \sum_{j \in N} A_{ij} x_j \tag{3}$$

- because α is solution have

$$\alpha(x_i) = \sum_{j \in N} A_{ij} \alpha(x_j) \tag{4}$$

- subtract (4) from (3):

$$\begin{aligned} x_i - \alpha(x_i) &= \sum_{j \in N} A_{ij}(x_j - \alpha(x_j)) \\ &= \sum_{j \in L} A_{ij}(x_j - l_j) - \sum_{j \in U} A_{ij}(u_j - x_j) \end{aligned} \tag{5}$$

Proof (2)

- have

$$x_i - \alpha(x_i) = \underbrace{\sum_{j \in L} A_{ij}(x_j - l_j)}_{\mathcal{L}} - \underbrace{\sum_{j \in U} A_{ij}(u_j - x_j)}_{\mathcal{U}} \tag{5}$$

- for $c = \alpha(x_i) - \lfloor \alpha(x_i) \rfloor$ have $0 < c < 1$, can write $\alpha(x_i) = \lfloor \alpha(x_i) \rfloor + c$, so

$$x_i - \lfloor \alpha(x_i) \rfloor = c + \mathcal{L} - \mathcal{U} \tag{6}$$

- for integer solution $\vec{x}$ left-hand side must be integer, so also right-hand side
- abbreviate

$$\mathcal{L}^+ = \sum_{j \in L^+} A_{ij}(x_j - l_j) \qquad \mathcal{U}^+ = \sum_{j \in U^+} A_{ij}(u_j - x_j)$$
$$\mathcal{L}^- = \sum_{j \in L^-} A_{ij}(x_j - l_j) \qquad \mathcal{U}^- = \sum_{j \in U^-} A_{ij}(u_j - x_j)$$

  so $\mathcal{L} = \mathcal{L}^+ + \mathcal{L}^-$ and $\mathcal{U} = \mathcal{U}^+ + \mathcal{U}^-$

- have $\mathcal{L}^+ \geqslant 0$, $\mathcal{U}^+ \geqslant 0$ and $\mathcal{L}^- \leqslant 0$, $\mathcal{U}^- \leqslant 0$
- distinguish $\mathcal{L} \geqslant \mathcal{U}$ or $\mathcal{L} < \mathcal{U}$

Proof (3)

- both sides are integer in equation

$$x_i - \lfloor \alpha(x_i) \rfloor = c + \mathcal{L} - \mathcal{U} \tag{6}$$

since $\mathcal{L}^+ \geqslant \mathcal{L}$ and $\mathcal{U}^- \leqslant \mathcal{U}$

- if $\mathcal{L} \geqslant \mathcal{U}$
  - have $c + \mathcal{L} - \mathcal{U} \geqslant 1$ because integer, so $\mathcal{L} - \mathcal{U} \geqslant 1 - c$
  - in particular $\mathcal{L}^+ - \mathcal{U}^- \geqslant 1 - c$
  - $$\frac{1}{1-c}\left(\mathcal{L}^+ - \mathcal{U}^-\right) \geqslant 1$$

since $\mathcal{U}^+ \geqslant \mathcal{U}$ and $\mathcal{L}^- \leqslant \mathcal{L}$

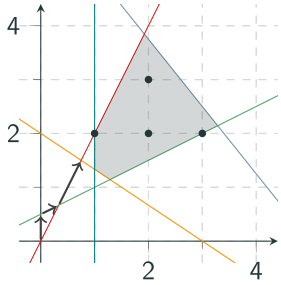
- otherwise
  - have $c + \mathcal{L} - \mathcal{U} \leqslant 0$ because integer, so $\mathcal{U} - \mathcal{L} \geqslant c$
  - in particular $\mathcal{U}^+ - \mathcal{L}^- \geqslant c$
  - $$\frac{1}{c}\left(\mathcal{U}^+ - \mathcal{L}^-\right) \geqslant 1 \tag{8}$$
- terms $\mathcal{L}^+$, $\mathcal{U}^+$, $-\mathcal{L}^-$ and $-\mathcal{U}^-$ always non-negative, as
- add (7) and (8) to obtain cut

$$\frac{1}{1-c}\left(\mathcal{L}^+ - \mathcal{U}^-\right) + \frac{1}{c}\left(\mathcal{U}^+ - \mathcal{L}^-\right) \geqslant 1$$

the desired monster inequality!

■

Example



$$-2x - 3y \leqslant -6$$
$$-2x + y \leqslant 0$$
$$x - 2y \leqslant -1$$
$$5x + 4y \leqslant 25$$

- infinite $\mathbb{R}^2$-solution space
- four solutions in $\mathbb{Z}^2$
- Simplex solution search

$$\begin{array}{c} \\ s_1 \\ s_2 \\ s_3 \\ s_4 \end{array} \begin{array}{c} \begin{array}{cc} x & y \end{array} \\ \begin{pmatrix} -2 & -3 \\ -2 & 1 \\ 1 & -2 \\ 5 & 4 \end{pmatrix} \end{array} \begin{array}{l} \\ s_1 \leqslant -6 \\ s_2 \leqslant 0 \\ s_3 \leqslant -1 \\ s_4 \leqslant 25 \end{array} \longrightarrow \begin{array}{c} \\ s_3 \\ x \\ y \\ s_4 \end{array} \begin{array}{c} \begin{array}{cc} s_2 & s_1 \end{array} \\ \begin{pmatrix} -\frac{7}{8} & \frac{3}{8} \\ -\frac{3}{8} & -\frac{1}{8} \\ \frac{1}{4} & -\frac{1}{4} \\ -\frac{7}{8} & -\frac{13}{8} \end{pmatrix} \end{array} \quad \begin{array}{ll} x = \frac{3}{4} & s_1 = -6 \\ y = \frac{3}{2} & s_2 = 0 \\ & s_3 = -2\frac{1}{4} \\ & s_4 = 9\frac{3}{4} \end{array}$$

initial tableau — final tableau — solution

- nonbasic variables $s_2 = 0$ and $s_1 = -6$ at bounds, basic x is assigned $\frac{3}{4} \notin \mathbb{Z}$
- from $c = \frac{3}{4}$ obtain Gomory cut $4(\frac{3}{8}(0 - s_2) + \frac{1}{8}(-6 - s_1)) \geqslant 1$
- corresponds to $-\frac{3}{2}(-2x + y) - \frac{1}{2}(-2x - 3y) \geqslant 4$, simplified $x \geqslant 1$

Bibliography

Daniel Kroening and Ofer Strichman
The Simplex Algorithm
Section 5.2 of Decision Procedures — An Algorithmic Point of View
Springer, 2008

Alexander Schrijver
Theory of Linear and Integer Programming
Wiley, 1998