Little Engines of Proof: Arithmetic Inequalities

N. Shankar, L. de Moura, H. Ruess, A. Tiwari
shankar@csl.sri.com
URL: http://www.csl.sri.com/~shankar/LEP.html

Computer Science Laboratory
SRI International
Menlo Park, CA

Overview

We examine the Dantzig's Simplex method as the basis for solving linear inequalities.

Simplex is typically used as an optimization method for linear programming, but it can be easily adapted to theorem proving.

Though simplex is, in principle, an exponential algorithm, it rarely exhibits super-polynomial behavior in practice.

The treatment here is based on Vanderbei's *Linear Programming: Foundations and Extensions*, and the work of Nelson, Badros and Borning, and Rueß and Shankar (forthcoming).

Linear Programming

A factory with m machines makes n products. The unit profit margin on item j is c_j and its manufacture requires a_{ij} units of resource (machine) i per unit of product j. There is a limit of b_i units of resource i. Maximize the profit margin.

LP: Example

A factory produces shirts, shorts, and skirts, with unit profits of \$5, \$3, and \$4, respectively, are produced using sewing machines, embroidery, and button stitching machines. There are 20 sewing machines, and each can do 4 shirts/hour, or 6 shorts/hour, or 3 skirts/hour. There are 10 embroidery machines, and each can do 5 shirts/hour, 8 shorts/hour, and 6 skirts/hour. There are 12 button-stitching machines, and each can do 8 shirts/hour, 5 shorts/hour, and 10 skirts/hour. Maximize profit.

Maximize $5x + 3y + 4z$, given

$$\begin{aligned}
(1/4)x + (1/6)y + (1/3)z &\leq 20 \\
(1/5)x + (1/8)y + (1/6)z &\leq 10 \\
(1/8)x + (1/5)y + (1/10)z &\leq 12
\end{aligned}$$

Linear Programming

Primal form: Maximize $\vec{c}^T\vec{x}$ given $A\vec{x} \leq \vec{b}$, where $\vec{b}$ and $\vec{c}$ are m-vectors, A is an $m \times n$ matrix, and $\vec{x} \geq 0$.

Equivalent dual form: Minimize $\vec{u}^T b$ given $\vec{u}^T A = \vec{c}^T$ and $\vec{u} \geq 0$.

Note that $\vec{c}^T\vec{x} \leq d$ iff for some $\vec{u}$, $\vec{u} \geq 0$, $\vec{c}^T\vec{x} = \vec{u}^T A\vec{x} \leq \vec{u}^T\vec{b} \leq d$ (Farkas Lemma).

The maximal primal solution $\vec{x}$ yields a $\vec{u}$ such that $\vec{c}^T\vec{x} = \vec{u}^T\vec{b}$ which is the minimal dual solution.

So, if primal form has a feasible solution $\vec{x}$, then this yields a minimal feasible solution $\vec{u}$ to the dual form.

Simplex [Dantzig]

Introduce slack variables through m-vector $\vec{k}$ so that $\vec{k} = \vec{b} - A\vec{x}$, with the restriction that in the solution $\vec{k} \geq 0$ and $\vec{x} \geq 0$.

The equality $\vec{k} = \vec{b} - A\vec{x}$ is the *simplex tableau* S.

Each k_i is a *dependent* variable (in the tableau) and each x_j is an *independent* variable (out of the tableau).

If $\vec{b} \geq 0$, then S is manifestly feasible (i.e., satisfiable), and has a basic feasible solution: Let $\vec{x} = 0$.

A dependent variable k_i is maximized (minimized) at b_i if $k_i = b_i - a_i^T x$ in S where all the entries in a_i are non-negative (non-positive).

An independent variable x_j is unbounded if for each i, a_{ij} is non-positive in the tableau.

Obtaining Optimality

Given objective function $\vec{c}^T\vec{x}$ and simplex tableau S of the form $\vec{k} = \vec{b} - A\vec{x}$, we need to

1. Convert S into an equivalent feasible tableau S_0, otherwise, there are no solutions, optimal or otherwise.

2. Starting with $C_0 = \vec{c}^T\vec{x}$ and feasible tableau S_0, transform $C_0; S_0$ to an equivalent form $C'; S'$ where C' is maximized or unbounded.

An expression C of the form $c_0 + \Sigma_{i=1}^n c_i x_i$ is maximized when all coefficients c_i are non-positive, and unbounded if for some i, $c_i \geq 0$ and x_i is unbounded in S.

Pivoting

Pivoting is the operation of swapping a dependent variable with an independent variable, so that the latter *enters* the tableau while the former *leaves* it.

Given

$$\begin{aligned} k_1 &= -2 + 3x_1 - 2x_2 \\ k_2 &= 1 - 2x_1 + 4x_2 \end{aligned}$$

If we pivot x_1 with k_2, we get

$$\begin{aligned} k_1 &= -1/2 - (3/2)k_2 + 4x_2 \\ x_1 &= 1/2 - (1/2)k_2 + 2x_2 \end{aligned}$$

Pivoting

Define $solve(x)(s = s')$ to return a solution of the form $x = t$, when x occurs with distinct coefficients in s and s'.

If S is a solution set containing $k = s$, then pivoting x with k, $pivot(x, k)(S)$, is just the operation $S \circ solve(x)(k = s)$.

Note that $S \iff pivot(x, k)(S)$.

For example $pivot(x, k)(S)$, where $k = d - a * x + s \in S$ is $S \circ \{x = d/a - (1/a)k + (1/a)s\}$.

The gain for the pivot $g(x, k)(S)$ is then d/a.

If k_i is such that for all i', $g(x_j, k_{i'})(S) \geq g(x_j, k_i)(S)$, then we say that $pivotable(x_j, k_i)(S)$ holds.

Pivoting

Given an expression C of the form $c_0 + c_1 x_1 + \ldots c_n x_n$ where $|C| = c_0$, and a feasible simplex tableau S, we can pivot *up* to increase $|C|$ while preserving the feasibility of S.

To pivot up: Find an x_j such c_j is positive and $pivotable(x_j, k_i)(S)$ holds. (If there is no such x_j, C is maximized.)

Let $S' = pivot(x_j, k_i)(S)$ and $C' = S'[C]$.

Note that $c'_0 = c_0 + c_j * g(x_j, k_i)$ so $|C'| \geq |C|$.

Check that S' is also feasible.

Simplex Inference

The state consists of an objective function C and a feasible simplex tableau S.

$$\frac{C; S}{C'; S'} \quad \begin{array}{l} C \text{ not maximized or unbounded} \\ c_j > 0, pivotable(x_j, k_i)(S) \\ S' = pivot(x_j, k_i)(S), C' = S'[C] \end{array}$$

Check that $S' \iff S$ and $S[C'] = C$.

But does it terminate? Depends. Pivoting cycles are possible, but also avoidable.

Note the nondeterminism in the choice of x_j and k_i.

Incremental Inequality Solving with Simplex

Input inequalities contain unrestricted variables.

The state consists of $G; S$, where G is the set of input inequalities, and the solution state S is further divided as $S_R; S_T$, where S_R is the solution set for unrestricted variables and S_T is the simplex tableau for restricted (≥ 0) variables.

Canonization $S[e]$ is as before: substitute solutions from S and put the result in canonical form.

We assume that there is a infinite supply of slack variables $k_0, k_1, \ldots$.

Adding an Inequality Incrementally

Given a feasible $m \times n$ tableau S of the form $\vec{k} = \vec{b} - A\vec{x}$, let $m' = m + 1$, we can add a new inequality $e \geq 0$ as follows.

$$\frac{e \geq 0, G; S}{G; S'} \text{ if } S' = addineq(k_{m'} = S[e]; S)$$

$addineq(k_{m'} = S[e]; S)$ is implemented in the following (deterministic) inference system.

$$\frac{k = C; S}{\bot} \text{ if } C \text{ is maximized}, |C| < 0$$

$$\frac{k = C; S}{S} \text{ if } C \text{ is minimized}, |C| \geq 0$$

$$\frac{k = C; S}{S \circ R} \quad \begin{array}{l} \text{if } solve(y)(k = C) = R \\ \text{for some unrestricted } y \in C \end{array}$$

$$\frac{k = C; S}{S \circ \{k = C\}} \quad \begin{array}{l} \text{if } |C| \geq 0, \\ C \text{ is not minimized} \end{array}$$

$$\frac{k = C; S}{S \circ R} \quad \begin{array}{l} \text{if } |C| < 0, \\ k' \in C, k' \text{ is unbounded in } S \\ solve(k')(k = C) = R \end{array}$$

$$\frac{k = C; S}{k = S'[C]; S'} \quad \begin{array}{l} |C| < 0, C \text{ is not unbounded in } S \\ c_j > 0, pivotable(x_j, k_i)(S) \\ S' = pivot(x_j, k_i)(S) \end{array}$$

Example

$$\{x_1 \geq 0, x_2 \geq 0, 2 - x_1 - x_2 \geq 0, -9 + 2x_1 + 2x_2 \geq 0\}; (\emptyset; \emptyset)$$
$$\overline{\{x_2 \geq 0, 2 - x_1 - x_2 \geq 0, -9 + 2x_1 + 2x_2 \geq 0\}; (\{x_1 = k_1\}; \emptyset)}$$
$$\overline{\{2 - x_1 - x_2 \geq 0, -9 + 2x_1 + 2x_2 \geq 0\}; (\{x_1 = k_1, x_2 = k_2\}; \emptyset)}$$
$$\overline{\{-9 + 2x_1 + 2x_2 \geq 0\}; (\{x_1 = k_1, x_2 = k_2\}; \{k_3 = 2 - k_1 - k_2\})}$$
$$\overline{k_4 = -9 + 2k_1 + 2k_2; (\{x_1 = k_1, x_2 = k_2\}; \{k_3 = 2 - k_1 - k_2\})}$$
$$\overline{k_4 = -5 - 2k_3; (\{x_1 = k_1, x_2 = k_2\}; \{k_1 = 2 - k_2 - k_3\})}$$
$$\overline{\bot}$$
$$\overline{\bot}$$

Correctness

Termination: We have already noted that nontermination is possible, but there are terminating pivoting strategies.

Each non-$\bot$ state is of the form $k = C; S$ or $\emptyset; S$, where S is feasible and C is canonical with respect to S.

Each step is model-preserving: both pivoting and canonization are.

A feasible tableau is trivially satisfiable.

Adding Equalities

There are two choices for adding equality $s=t$: either add $s-t\geq 0$ and $t-s\geq 0$, or process as follows.

$$\frac{s=t,G;S}{G;S\circ R}\quad \text{if } y\in S[t-s], y \text{ unrestricted} \quad solve(y)(S[s=t])=R$$

$$\frac{s=t,G;S}{G;S'}\quad \text{if } S'=addineq(k^0_{m'}=C;S), C=S[t-s], |C|\leq 0$$

C contains no unrestricted variables.

$addineq(k^0_{m'}=C;S)$ is given by the following (deterministic) inference system.

$k^0_{m'}$ is a 0-slack variable that is restricted to being equal to 0.

Addeq

$$\frac{k^0_{m'}=C;S}{\bot}\quad \text{if } |C|<0, C \text{ is maximized}$$

$$\frac{k^0_{m'}=C;S}{\bot}\quad \text{if } |C|>0, C \text{ is minimized}$$

$$\frac{k^0_{m'}=C;S}{S\circ R\triangleright\{k^0_{m'}=0\}}\quad \text{if } k' \text{ unbounded in } C \quad |C|<0, R=solve(k')(k^0_{m'}=C)$$

$$\frac{k^0_{m'}=C;S}{k^0_{m'}=S'[C];S'}\quad \text{if } |C|<0, c_j>0, pivotable(x_j,k_i)(S), \quad S'=pivot(x_j,k_i)(S)$$

$$\frac{k^0_{m'}=C;S}{k^0_{m'}=S'[C];S'}\quad \text{if } |C|>0, c_j<0, pivotable(x_j,k_i)(S), \quad g(x_j,k_i)(S)<g(x_j,k^0_{m'})(\{k^0_{m'}=C\}) \quad S'=pivot(x_j,k_i)(S)$$

$$\frac{k^0_{m'}=C;S}{S\circ R\triangleright\{k^0_{m'}=0\}}\quad \text{if } |C|>0, c_j<0, pivotable(x_j,k_i)(S), \quad g(x_j,k_i)(S)\geq g(x_j,k^0_{m'})(\{k^0_{m'}=C\}) \quad R=pivot(x_j,k^0_{m'})(\{k^0_{m'}=C\})$$

Example

$$\{x\geq 0, y\geq 0, 2-2x-y\geq 0, y=-3+3x\};(\emptyset;\emptyset)$$

$$\{y\geq 0, 2-2x-y\geq 0, y=-3+3x\};(\{x=k_1\};\emptyset)$$

$$\{2-2x-y\geq 0, y=-3+3x\};(\{x=k_1, y=k_2\};\emptyset)$$

$$\{y=-3+3x\};(\{x=k_1, y=k_2\};\{k_3=2-2k_1-k_2\})$$

$$k^0_4=-3+3k_1-k_2;(\{x=k_1, y=k_2\};\{k_3=2-2k_1-k_2\})$$

$$k^0_4=-(5/2)k_2-(3/2)k_3;(\{x=k_1, y=k_2\};\{k_1=1-(1/2)k_2-(1/2)k_3\})$$

$$\emptyset;(\{x=k_1, y=k_2\};\{k_1=1-(1/2)k_2-(1/2)k_3, k_2=-(3/5)k_3\})$$

$$(\{x=k_1, y=k_2\};\{k_1=1-(1/2)k_2-(1/2)k_3, k_2=-(3/5)k_3\})$$

It is easy to see that $y=k2=k3=0$ and $x=k_1=1$.