# Decision Procedures

## An Algorithmic Point of View

## Linear Arithmetic

D. Kroening O. Strichman

ETH/Technion

Version 1.0, 2007

Part V

# Linear Arithmetic

# Fourier-Motzkin Variable Elimination

- Goal: decide satisfiability of conjunction of linear constraints over reals

$$\bigwedge_{1 \leq i \leq m} \sum_{1 \leq j \leq n} a_{i,j} x_j \leq b_i$$

# Fourier-Motzkin Variable Elimination

- Goal: decide satisfiability of conjunction of linear constraints over reals

$$\bigwedge_{1 \leq i \leq m} \sum_{1 \leq j \leq n} a_{i,j} x_j \leq b_i$$

- Earliest method for solving linear inequalities
- Discovered in 1826 by Fourier, re-discovered by Motzkin in 1936

# Fourier-Motzkin Variable Elimination

- Goal: decide satisfiability of conjunction of linear constraints over reals

$$\bigwedge_{1 \leq i \leq m} \sum_{1 \leq j \leq n} a_{i,j} x_j \leq b_i$$

- Earliest method for solving linear inequalities
- Discovered in 1826 by Fourier, re-discovered by Motzkin in 1936

- Basic idea of variable elimination:
  - Pick one variable and eliminate it
  - Continue until all variables but one are eliminated

Input: A system of conjoined linear inequalities $A\overline{x} \leq \overline{b}$

$m$ constraints

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ a_{m1} & a_{22} & \cdots & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \end{pmatrix} \leq \begin{pmatrix} b_1 \\ \vdots \\ \vdots \\ b_n \end{pmatrix}$$

$n$ variables

# Removing unbounded variables

- Iteratively remove variables that are not bounded in both ways (and all the constraints that use them)
- The new problem has a solution iff the old problem has one!

$$\begin{array}{rcl} 8x & \geq & 7y \\ x & \geq & 3 \\ y & \geq & z \\ z & \geq & 10 \\ 20 & \geq & z \end{array}$$

# Removing unbounded variables

- Iteratively remove variables that are not bounded in both ways (and all the constraints that use them)
- The new problem has a solution iff the old problem has one!

$$
\begin{array}{rcl}
\cancel{8x} & \cancel{\geq} & \cancel{7y} \\
\cancel{x} & \cancel{\geq} & \cancel{3} \\
y & \geq & z \\
z & \geq & 10 \\
20 & \geq & z
\end{array}
$$

# Removing unbounded variables

- Iteratively remove variables that are not bounded in both ways (and all the constraints that use them)
- The new problem has a solution iff the old problem has one!

$$
\begin{array}{rcl}
\cancel{8x} & \cancel{\geq} & \cancel{7y} \\
\cancel{x} & \cancel{\geq} & \cancel{3} \\
y & \geq & z \\
z & \geq & 10 \\
20 & \geq & z
\end{array}
\quad \longrightarrow \quad
\begin{array}{rcl}
y & \geq & z \\
z & \geq & 10 \\
20 & \geq & z
\end{array}
$$

# Removing unbounded variables

- Iteratively remove variables that are not bounded in both ways (and all the constraints that use them)
- The new problem has a solution iff the old problem has one!

$$
\begin{array}{rcl}
\cancel{8x} & \cancel{\geq} & \cancel{7y} \\
\cancel{x} & \cancel{\geq} & \cancel{3} \\
y & \geq & z \\
z & \geq & 10 \\
20 & \geq & z
\end{array}
\quad \longrightarrow \quad
\begin{array}{rcl}
\cancel{y} & \cancel{\geq} & \cancel{z} \\
z & \geq & 10 \\
20 & \geq & z
\end{array}
$$

# Removing unbounded variables

- Iteratively remove variables that are not bounded in both ways (and all the constraints that use them)
- The new problem has a solution iff the old problem has one!

$$\begin{array}{rcl} \cancel{8x} & \cancel{\geq} & \cancel{7y} \\ \cancel{x} & \cancel{\geq} & \cancel{3} \\ y & \geq & z \\ z & \geq & 10 \\ 20 & \geq & z \end{array} \longrightarrow \begin{array}{rcl} \cancel{y} & \cancel{\geq} & \cancel{z} \\ z & \geq & 10 \\ 20 & \geq & z \end{array} \longrightarrow \begin{array}{rcl} z & \geq & 10 \\ 20 & \geq & z \end{array}$$

# Partitioning the Constraints

1. When eliminating $x_n$, partition the constraints according to the coefficient $a_{in}$:
   - $a_{i,n} > 0$: upper bound $\beta_i$
   - $a_{i,n} < 0$: lower bound $\beta_i$

# Partitioning the Constraints

1. When eliminating $x_n$, partition the constraints according to the coefficient $a_{in}$:
   - $a_{i,n} > 0$: upper bound $\beta_i$
   - $a_{i,n} < 0$: lower bound $\beta_i$

$$\sum_{j=1}^{n} a_{i,j} \cdot x_j \leq b_i$$

# Partitioning the Constraints

1. When eliminating $x_n$, partition the constraints according to the coefficient $a_{in}$:
   - $a_{i,n} > 0$: upper bound $\beta_i$
   - $a_{i,n} < 0$: lower bound $\beta_i$

$$\sum_{j=1}^{n} a_{i,j} \cdot x_j \leq b_i$$

$$\Rightarrow \quad a_{i,n} \cdot x_n \leq b_i - \sum_{j=1}^{n-1} a_{i,j} \cdot x_j$$

# Partitioning the Constraints

1. When eliminating $x_n$, partition the constraints according to the coefficient $a_{in}$:
   - $a_{i,n} > 0$: upper bound $\beta_i$
   - $a_{i,n} < 0$: lower bound $\beta_i$

$$\sum_{j=1}^{n} a_{i,j} \cdot x_j \leq b_i$$

$$\Rightarrow \quad a_{i,n} \cdot x_n \leq b_i - \sum_{j=1}^{n-1} a_{i,j} \cdot x_j$$

$$\Rightarrow \quad x_n \leq \frac{b_i}{a_{i,n}} - \sum_{j=1}^{n-1} \frac{a_{i,j}}{a_{i,n}} \cdot x_j \quad =: \beta_i$$

# Example for Upper and Lower Bounds

Category?

$$
\begin{array}{ll}
(1) & x_1 - x_2 \leq 0 \\
(2) & x_1 - x_3 \leq 0 \\
(3) & -x_1 + x_2 + 2x_3 \leq 0 \\
(4) & -x_3 \leq -1
\end{array}
$$

Assume we eliminate $x_1$.

# Example for Upper and Lower Bounds

Category?

(1) $x_1 - x_2 \leq 0$ Upper bound

(2) $x_1 - x_3 \leq 0$

(3) $-x_1 + x_2 + 2x_3 \leq 0$

(4) $-x_3 \leq -1$

Assume we eliminate $x_1$.

# Example for Upper and Lower Bounds

| | | Category? |
|---|---|---|
| (1) | $x_1 - x_2 \leq 0$ | Upper bound |
| (2) | $x_1 - x_3 \leq 0$ | Upper bound |
| (3) | $-x_1 + x_2 + 2x_3 \leq 0$ | |
| (4) | $-x_3 \leq -1$ | |

Assume we eliminate $x_1$.

# Example for Upper and Lower Bounds

| | | Category? |
|---|---|---|
| (1) | $x_1 - x_2 \leq 0$ | Upper bound |
| (2) | $x_1 - x_3 \leq 0$ | Upper bound |
| (3) | $-x_1 + x_2 + 2x_3 \leq 0$ | Lower bound |
| (4) | $-x_3 \leq -1$ | |

Assume we eliminate $x_1$.

# Adding the constraints

2. For each pair of a lower bound $a_{l,n} < 0$ and upper bound $a_{u,n} > 0$, we have

$$\beta_l \quad \leq \quad x_n \quad \leq \quad \beta_u$$

3. For each such pair, add the constraint

$$\beta_l \quad \leq \quad \beta_u$$

# Fourier-Motzkin: Example

Category?

(1) $x_1 - x_2 \leq 0$
(2) $x_1 - x_3 \leq 0$
(3) $-x_1 + x_2 + 2x_3 \leq 0$
(4) $-x_3 \leq -1$

# Fourier-Motzkin: Example

$$
\begin{array}{ll}
(1) & x_1 - x_2 \leq 0 \\
(2) & x_1 - x_3 \leq 0 \\
(3) & -x_1 + x_2 + 2x_3 \leq 0 \\
(4) & -x_3 \leq -1
\end{array}
$$

---

Category?

Upper bound

Upper bound

Lower bound

we eliminate $x_1$

# Fourier-Motzkin: Example

| | | Category? |
|---|---|---|
| (1) | $x_1 - x_2 \leq 0$ | Upper bound |
| (2) | $x_1 - x_3 \leq 0$ | Upper bound |
| (3) | $-x_1 + x_2 + 2x_3 \leq 0$ | Lower bound |
| (4) | $-x_3 \leq -1$ | |
| | | we eliminate $x_1$ |
| (5) | $2x_3 \leq 0$ (from 1,3) | |

# Fourier-Motzkin: Example

| | | | Category? |
|---|---|---|---|
| (1) | $x_1 - x_2 \leq 0$ | | Upper bound |
| (2) | $x_1 - x_3 \leq 0$ | | Upper bound |
| (3) | $-x_1 + x_2 + 2x_3 \leq 0$ | | Lower bound |
| (4) | $-x_3 \leq -1$ | | |
| | | | we eliminate $x_1$ |
| (5) | $2x_3 \leq 0$ | (from 1,3) | |
| (6) | $x_2 + x_3 \leq 0$ | (from 2,3) | |

# Fourier-Motzkin: Example

Category?

(1) ~~$x_1 \quad x_2 \leq 0$~~

(2) ~~$x_1 \quad x_3 \leq 0$~~

(3) ~~$x_1 + x_2 + 2x_3 \leq 0$~~

(4) $-x_3 \leq -1$

---

we eliminate $x_1$

(5) $2x_3 \leq 0$ (from 1,3)

(6) $x_2 + x_3 \leq 0$ (from 2,3)

# Fourier-Motzkin: Example

Category?

(1) ~~$x_1 \quad x_2 \leq 0$~~

(2) ~~$x_1 \quad x_3 \leq 0$~~

(3) ~~$x_1 + x_2 + 2x_3 \leq 0$~~

(4) $-x_3 \leq -1$

---

we eliminate $x_1$

(5) $2x_3 \leq 0$ (from 1,3)

(6) $x_2 + x_3 \leq 0$ (from 2,3)

---

we eliminate $x_3$

# Fourier-Motzkin: Example

Category?

~~(1) $x_1 \quad x_2 \leq 0$~~

~~(2) $x_1 \quad x_3 \leq 0$~~

~~(3) $x_1 + x_2 + 2x_3 \leq 0$~~

(4) $-x_3 \leq -1$ — Lower bound

---

we eliminate $x_1$

(5) $2x_3 \leq 0$ (from 1,3) — Upper bound

(6) $x_2 + x_3 \leq 0$ (from 2,3) — Upper bound

---

we eliminate $x_3$

# Fourier-Motzkin: Example

Category?

(1) ~~$x_1 \quad x_2 \leq 0$~~

(2) ~~$x_1 \quad x_3 \leq 0$~~

(3) ~~$x_1 + x_2 + 2x_3 \leq 0$~~

(4) $-x_3 \leq -1$ — Lower bound

we eliminate $x_1$

(5) $2x_3 \leq 0$ (from 1,3) — Upper bound

(6) $x_2 + x_3 \leq 0$ (from 2,3) — Upper bound

we eliminate $x_3$

(7) $0 \leq -1$ (from 4,5)

$\rightarrow$ Contradiction (the system is UNSAT)

# Complexity

- Worst-case complexity:

$$m \longrightarrow m^2$$

# Complexity

- Worst-case complexity:

$$m \rightarrow m^2 \rightarrow (m^2)^2$$

# Complexity

- Worst-case complexity:

$$m \rightarrow m^2 \rightarrow (m^2)^2 \rightarrow \ldots \rightarrow m^{2^n}$$

# Complexity

- Worst-case complexity:

$$m \rightarrow m^2 \rightarrow (m^2)^2 \rightarrow \ldots \rightarrow m^{2^n}$$

- Heavy! So why is it so popular in verification?

# Complexity

- Worst-case complexity:

$$m \rightarrow m^2 \rightarrow (m^2)^2 \rightarrow \ldots \rightarrow m^{2^n}$$

- Heavy! So why is it so popular in verification?

- The bottleneck: case-splitting