Linear Arithmetic

Deepak D'Souza

Department of Computer Science and Automation
Indian Institute of Science, Bangalore.

05, 10, 12 May 2021

Outline

Linear Arithmetic (KS Ch 5)

- Boolean combinations of linear constraints of the form:

$$a_1x_1 + \cdots + a_nx_n \leq b_1$$

- Quantifier-Free fragment of $FO(+, -, <, 0, 1)$
- Interpretation of $+, -, <, 0, 1$ fixed; Domain is $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{Z}$.

Linear Arithmetic syntax

(Formula) $\varphi ::= Atom \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi$
(Atom) $Atom ::= Term < Term \mid Term = Term$
(Term) $Term ::= Var \mid Const \mid Term + Term \mid Term - Term$

Examples

Example formula φ_1

$$
\begin{aligned}
x = 19 &\implies x \leq 20 \wedge \\
x \leq 20 \wedge x \geq 10 \wedge z = -1 \wedge x' = x + z &\implies x' \leq 20 \wedge \\
x \leq 20 \wedge y = 15 \wedge \neg(x \geq 10) &\implies y \geq x'
\end{aligned}
$$

Example conjunctive formula φ_2

$$
\begin{aligned}
x + y < 1 &\wedge \\
0 < x &\wedge \\
0 < y &
\end{aligned}
$$

Question we want to answer: Satisfiability.

Importance of Linear Arithmetic

Many practical applications. In Verification:

- Loop invariants, polyhedral data-flow analysis of programs
- Compiler Optimization
- Analysis/Model-Checking of timed, hybrid, dynamical systems.
- Symbolic Execution/Simulation (representation of reachable states).
- Winning Strategies in 2-player Games, Controller Synthesis.

Example: Loop optimization (loop hoisting)

```
for (i = 1; i <= 10; i++)
  a[j+i] := a[j];
```

```
// R1 has i, R2 has j
// loop body
  1. R4 := mem[a+R2];
  2. R5 := R2 + R1;
  3. mem[a+5] := R4;
  4. R1 :-= R1 + 1;
```

Statement 1 can be hoisted out of loop if foll constraint is unsat:

$$1 \leq i \wedge i \leq 10 \wedge i + j = j$$

Checking Verification Conditions

Floyd-Hoare style verification of programs:

```
int x = 19;
int y = 15;
// inv: x <= 20
while (x >= 10) {
  int z = -1;
  x = x + z;
}
assert(y >= x);
```

Are the constraints: $\forall x, y, z, x'$:

$$x = 19 \implies x \leq 20$$

$$x \leq 20 \land x \geq 10 \land z = -1 \land x' = x + z \implies x' \leq 20$$

$$x \leq 20 \land y = 15 \land \neg(x \geq 10) \implies y \geq x'$$

valid?

Fourier-Motzkin Elimination (KS Sec 5.4, Schrijver Sec 12.2)

- Fourier 1827, Dines 1917, Motzkin 1936.
- Works for $\mathbb{R}$ and $\mathbb{Q}$ domains.
- Consider conjunctions of linear constraints
- Can check satisfiability, find a solution, eliminate variables (geometric projection, $\exists$-elimination)

General form

Suppose we want to eliminate x_1 from the system of ineqs (1):

$$a_{11}x_1 + \cdots + a_{1n}x_n \leq b_1$$
$$a_{21}x_1 + \cdots + a_{2n}x_n \leq b_2$$
$$\cdots$$
$$a_{m1}x_1 + \cdots + a_{mn}x_n \leq b_m$$

1. Make coeffs of x_1 1, -1, or 0, by scaling by a pos constant.
2. Write Ineq (1) as (2):

$$x_1 \leq b'_1 - (a'_{21}x_2 + \cdots + a'_{1n}x_n) \ (m' \text{ ineqs}) \quad (1)$$
$$\cdots$$
$$-x_1 \leq b'_{m'+1} - (a'_{m'+1,1}x_2 + \cdots + a'_{m'+1,n}x_n) \ (m'' - m' \quad (2)$$
$$a_{m''+1,2}x_2 + \cdots + a_{m''+1,n}x_n \leq b_{m''+1} \ (m - m'' \text{ ineqs}) \quad (3)$$

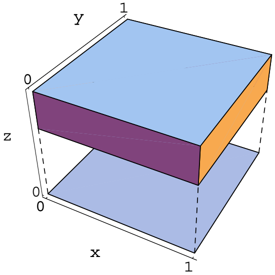
Fourier-Motzkin contd.

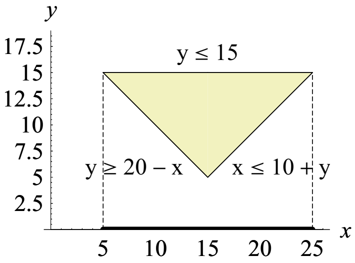
3. Remove constraints of type (1) and (2). Note that constraints of type (3) are retained.
4. Add all combinations of -RHS(2) $\leq$ RHS(1) constraints.
5. Let Ineq (3) be obtained thus.

Claim: Ineq (3) represents the projection of the solution set of Ineq (1) to the dimensions $x_2, \ldots, x_n$.

6. Repeat till we get constraints in single variable x_n. Check if the constraints are satisfiable (lower bounds $\leq$ upper bounds). If sat, output SAT; else output UNSAT.

Examples illustrating projection





$$0 \leq x \leq 1$$
$$0 \leq y \leq 1$$
$$0.75 \leq z \leq 1$$

$$y \leq 15$$
$$y \geq 20 - x$$
$$x \leq 10 + y$$

Example

Given system of ineq:

$$y \leq 15$$
$$y \geq 20 - x$$
$$x \leq 10 + y$$

Rewrite in general form:

$$y \leq 15$$
$$-y \leq x - 20$$
$$x - y \leq 10$$

Rewrite:

$$y \leq 15$$
$$-x + 20 \leq y$$
$$x - 10 \leq y$$

Eliminate y:

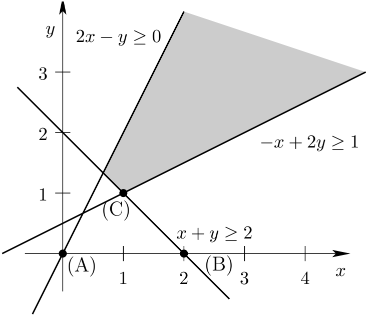
$$-x + 20 \leq 15$$
$$x - 10 \leq 15$$

That is: $5 \leq x \leq 25$. Hence original system of ineqs is satisfiable.

One solution is $x \mapsto 10, y \mapsto 12$.

Exercise

Eliminate x from the system of inequalities:



Correctness claims

The projection of a set S of n-dimension vectors to dimensions 2 to n is defined to be

$$\{(a_2, \ldots, a_n) \mid \exists a_1 \text{ such that } (a_1, a_2, \ldots, a_n) \in S\}.$$

- Ineq (3) represents the projection of the solution set of Ineq (1).
- If Algo reports SAT, then the solution set to Ineq (1) is non-empty.

Some observations on FM Elimination

- Finding a solution: substitute backwards.
- Complexity
  - Number of constraints can blow up from m to m^2 in one iteration.
  - Number of constraints can be exponential in n (See Schrijver p156)

Integer Linear Arithmetic

Given a system of linear inequalities Ineq (1):

$$
\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n &\leq b_1 \\
a_{21}x_1 + \cdots + a_{2n}x_n &\leq b_2 \\
&\cdots \\
a_{m1}x_1 + \cdots + a_{mn}x_n &\leq b_m
\end{aligned}
$$

Is there an integer-valued solution to Ineq (1)?

Integer Linear Arithmetic

Given a system of linear inequalities Ineq (1):

$$
\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n &\leq b_1 \\
a_{21}x_1 + \cdots + a_{2n}x_n &\leq b_2 \\
&\cdots \\
a_{m1}x_1 + \cdots + a_{mn}x_n &\leq b_m
\end{aligned}
$$

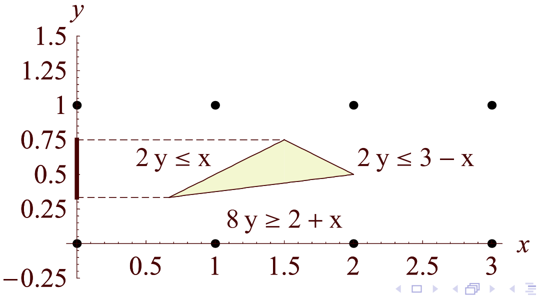
Is there an integer-valued solution to Ineq (1)?

How do we answer this?
Is the problem decidable (brute-force procedure)?

Example 1

$$2y \leq x$$
$$8y \geq 2 + x$$
$$2y \leq 3 - x$$

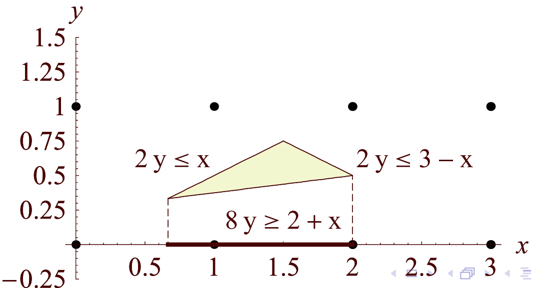
Eliminate x:



Example 1

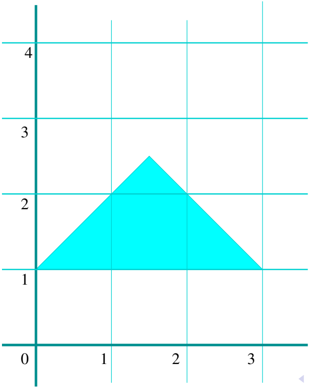
$$2y \leq x$$
$$8y \geq 2 + x$$
$$2y \leq 3 - x$$

Eliminate y:



Another example: All projections non-empty

$$y < x + 1$$
$$y > 1$$
$$y < 4 - x$$



Eliminating equality constraints

If we have a constraint

$$a_1 x_1 + \cdots + a_n x_n = b \quad (a_1 \neq 0)$$

Substitute

$$x_1 = \frac{1}{a_1}(b - a_2 x_2 - \cdots - a_n x_n)$$

in remaining constraints to get projection to $x_2, \ldots, x_n$.

Omega Test (Pugh 1991)

Adaptation of Fourier-Motzkin Elimination for integer solutions.

$OmegaTest(C)$:
    $C_R = Elim(C, v)$;
    If ($OmegaTest(C_R)$ = UNSAT)
        Return UNSAT;
    $C_D = DarkShadow(C, v)$;
    If ($OmegaTest(C_D)$ = SAT)
        Return SAT;
    If ($C_R = C_D$)
        Return UNSAT;
    $C_G^1, \ldots, C_G^k = GreyShadow(C, v)$;
    If ($OmegaTest(C_G^i)$ = SAT for any i)
        Return SAT;
    Return UNSAT;

Checking the underapproximation

Consider a pair of constraints of the form

$$\beta \leq bz$$
$$cz \leq \gamma$$

Write these as

$$c\beta \leq cbz$$
$$cbz \leq b\gamma$$

Constraint below suffices to ensure there exists an integer value (for z) between the lower and upper bounds:

$$c\beta + (cb - c - b + 1) \leq b\gamma$$

Check if Ineq (3) with these modified versions of cross constraints, has an integral solution.

If the underapproximation has no integer solution

Consider a pair of constraints of the form

$$\begin{aligned} c\beta &\leq cbz \\ cbz &\leq b\gamma \\ b\gamma &\leq c\beta + (cb - c - b) \end{aligned}$$

This implies:

$$\beta \leq bz \leq \beta + \frac{(cb - c - b)}{c}$$

Check if Ineq (3) with $bz = \beta + i$ (with $i \in 0, 1, \ldots, \frac{(cb-c-b)}{c}$) has an integer solution.

Example from [Pugh 1991]

$$3 \leq 11x + 13y \leq 21$$
$$-8 \leq 7x - 9y \leq 6$$

$$3 - 13y \leq 11x \leq 21 - 13y$$
$$9y - 8 \leq 7x \leq 9y + 6$$

P'

lower bound	upper bound	unnormalized combination
$33 - 143y \leq 121x$	$121x \leq 231 - 143y$	$198 \geq 0$
$21 - 91y \leq 77x$	$77x \leq 99y + 66$	$190y + 45 \geq 0$
$63y - 56 \leq 49x$	$49x \leq 63y + 42$	$98 \geq 0$
$99y - 88 \leq 77x$	$77x \leq 147 - 91y$	$235 \geq 190y$

P''

lower bound	upper bound	unnormalized combination
$(33 - 143y) + 100 \leq 121x$	$121x \leq 231 - 143y$	$98 \geq 0$
$(21 - 91y) + 60 \leq 77x$	$77x \leq 99y + 66$	$190y \geq 15$
$(63y - 56) + 36 \leq 49x$	$49x \leq 63y + 42$	$62 \geq 0$
$(99y - 88) + 60 \leq 77x$	$77x \leq 147 - 91y$	$175 \geq 190y$