Integers

Specifications section, **Algorithms** topic, **Lecture 8**

Pavel Panchekha

CS 6110, U of Utah

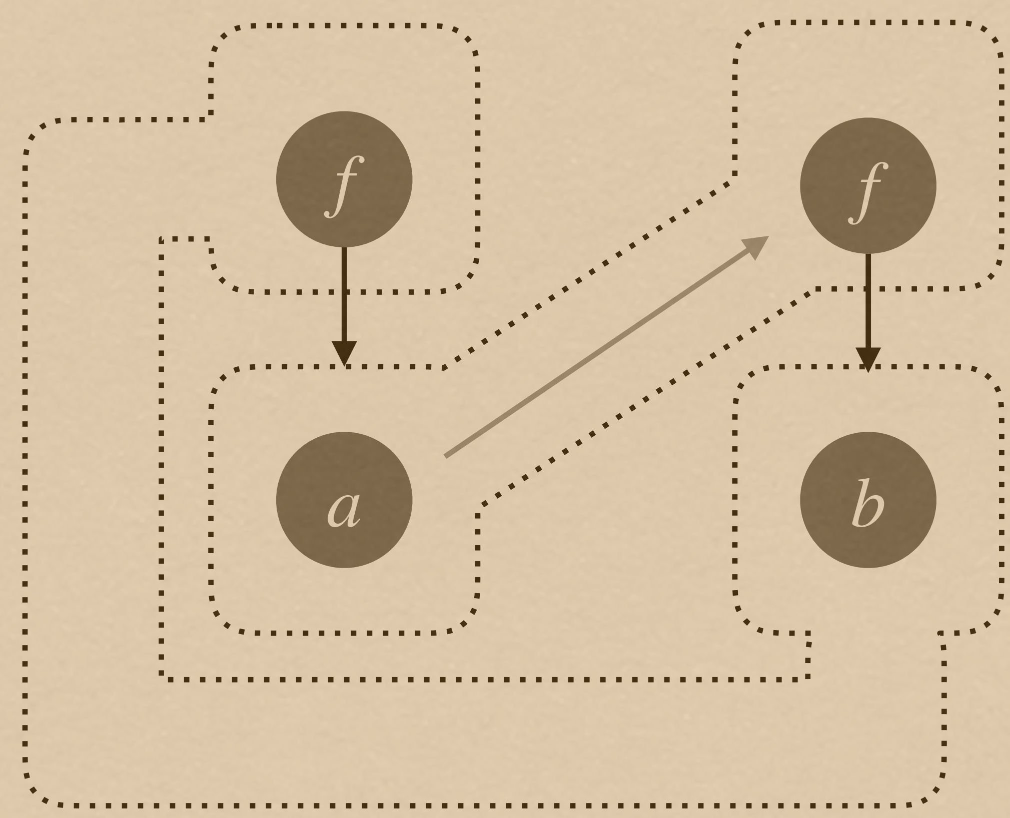
30 January 2020

Subterm Sharing

Avoid **multiple copies** of one expression

Make equal things identical to enforce equality axioms

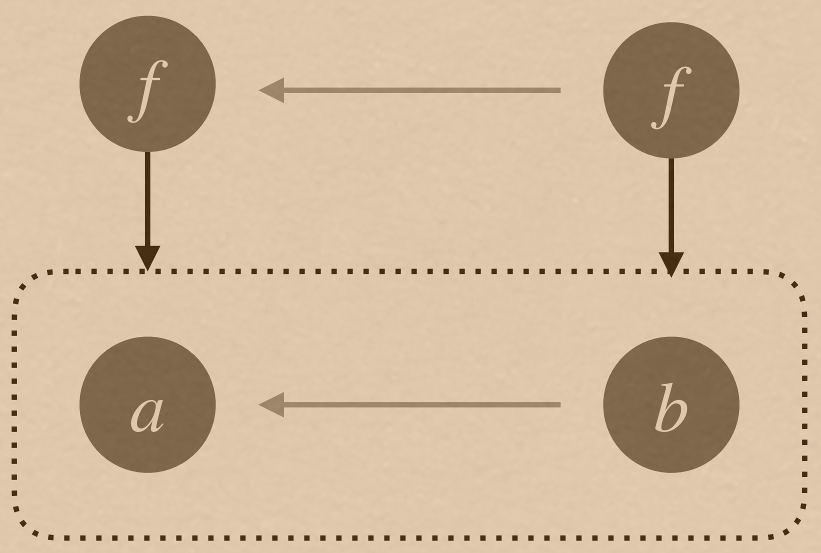
Equivalence Classes



$f(a) = b \qquad f(b) = a$

How to represent equivalence classes **in code**?

Congruence Closure




```
for (f, args), name in this.names.items():
  arg_classes = map(this.classof, args)
  name2 = this.add(f, arg_classes)
  this.eqclass[name] = name2
```

Class Progress

Logical reasoning

Program logics

Static analysis

First-order Logic

Decision Procedures

Mixing Theories

Equality

Integers

Arrays

Integers

Solving conjunctions of **integer equalities**

Back to high school with elimination and substitution

Variable elimination for integer inequalities

Combining two inequalities into one

How fast can integer reasoning be?

SAT, multiplication, and rational numbers

Systems of Equations

Flashback to high school math

The Solver Query

Statement p

$(\neg a_1 \vee a_2) \wedge (\neg b_1 \vee b_2) \wedge \ldots$

Assignment Γ

$a_1 \wedge \neg b_2 \wedge \ldots$

Today: a solver for **integer queries**

No negations!

$p := \boxed{x < y \mid x = y}$ $\qquad x, y := x + y \mid x \times n \mid v \mid n$

$\Gamma = x < 1 \wedge 0 < x$ $\qquad \Gamma = x < y \wedge y < z \wedge x + z < y$

$\Gamma = 2 \times x + 3 \times y = 5 \wedge x + 4 \times y = 0$

Standard Form

Convenient to **use** $\leq$ (in a consistent direction)

$$x < y \rightsquigarrow x \leq y - 1 \qquad\qquad x = y \rightsquigarrow x \leq y \wedge y \leq x$$

Convenient to **distribute multiplications**

$$(a + b) \times n \rightsquigarrow a \times n + b \times n$$

Convenient to **separate constants and variables**

$$1 + 2 \times (x + 3 \times y + 4) \leq y \rightsquigarrow 2 \times x + 6 \times y \leq -9$$

Result: matrix formula $Mx \leq C$

Examples

$$\Gamma = x < 1 \wedge 0 < x$$

$$\begin{vmatrix} 1 \\ -1 \end{vmatrix} \begin{vmatrix} x \end{vmatrix} \leq \begin{vmatrix} 0 \\ -1 \end{vmatrix}$$

$$\Gamma = x < y \wedge y < z \wedge x + z < y$$

$$\begin{vmatrix} 1 & -1 & \\ & 1 & -1 \\ 1 & -1 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ Z \end{vmatrix} \leq \begin{vmatrix} -1 \\ -1 \\ -1 \end{vmatrix}$$

$$\Gamma = 2 \times x + 3 \times y = 5 \wedge x + 4 \times y = 0$$

$$\begin{vmatrix} 2 & 3 \\ -2 & -3 \\ 1 & 4 \\ -1 & -4 \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} \leq \begin{vmatrix} 5 \\ -5 \\ 0 \\ 0 \end{vmatrix}$$

Equations

Restrict $Mx \leq C$ to $Mx = C$ (for now)

$$\begin{vmatrix} 1 & -1 & \\ & 1 & -1 \\ 1 & -1 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} \leqq \begin{vmatrix} -1 \\ -1 \\ -1 \end{vmatrix}$$

Equations

Restrict $Mx \leq C$ to $Mx = C$ (for now)

$$\begin{vmatrix} x \\ y \\ z \end{vmatrix} = \begin{vmatrix} 1 & -1 & \\ & 1 & -1 \\ 1 & -1 & 1 \end{vmatrix}^{\mathbf{-1}} \begin{vmatrix} -1 \\ -1 \\ -1 \end{vmatrix}$$

Matrix inverses only work for square matrices

Let's look at **two other techniques** for solving linear equations

Substitution

Solve linear equations by **eliminating variables**

$$\Gamma = 2 \times x + 3 \times y = 5 \wedge \boxed{x + 4 \times y = 0}$$

$$x = -4 \times y$$

$$2 \times (-4 \times y) + 3 \times y = 5$$

$$-5 \times y = 5$$

$$y = -1$$

Substitution

Solve linear equations by **eliminating variables**

$$\Gamma = \boxed{2 \times x + 3 \times y = 5} \wedge x + 4 \times y = 0$$

$$2 \times x = 5 - 3 \times y$$

$$2 \times x + 8 \times y = 0$$

$$(5 - 3 \times y) + 8 \times y = 0$$

$$5 + 5 \times y = 0$$

$$y = -1$$

Variable elimination is a standard logic technique

Recall **proof by resolution** in boolean logic

Elimination

Solve linear equations by **simplifying equations**

$$\Gamma = 2 \times x + 3 \times y = 5 \wedge x + 4 \times y = 0$$

$$-2 \quad \begin{vmatrix} 2 & 3 \\ 1 & 4 \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} 5 \\ 0 \end{vmatrix}$$

$$-5 \times y = 5 \quad \begin{vmatrix} 0 & -5 \\ 1 & 4 \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} 5 \\ 0 \end{vmatrix}$$

Create **row combinations** with 0 elements

Gaussian elimination algorithm does this **systematically**

Elimination

Systematic combinations of equations

$$\begin{array}{c} -b \\ a \\ \\ \\ \end{array} \left| \begin{matrix} a & ? & ? \\ b & ? & ? \\ c & ? & ? \\ d & ? & ? \end{matrix} \right| \left| \begin{matrix} x \\ y \\ z \end{matrix} \right| = \left| \begin{matrix} w \\ u \\ v \\ q \end{matrix} \right|$$

Elimination

Systematic combinations of equations

$$
\begin{array}{r}
-b \\
a \\
\\
\\
\end{array}
\left|\begin{array}{ccc}
a & ? & ? \\
0 & ? & ? \\
c & ? & ? \\
d & ? & ?
\end{array}\right|
\left|\begin{array}{c}
x \\
y \\
z
\end{array}\right|
=
\left|\begin{array}{c}
w \\
a\,u - b\,w \\
v \\
q
\end{array}\right|
$$

Elimination

Systematic combinations of equations

$$
\begin{array}{r}
\color{red}{-c} \\ \\ \color{red}{a} \\ \color{red}{\dots}
\end{array}
\begin{vmatrix} a & ? & ? \\ 0 & b & ? \\ 0 & c & ? \\ 0 & d & ? \end{vmatrix}
\begin{vmatrix} x \\ y \\ z \end{vmatrix}
=
\begin{vmatrix} w \\ a\,u - b\,w \\ a\,v - c\,w \\ a\,q - d\,w \end{vmatrix}
$$

Elimination

Systematic combinations of equations

$$\begin{array}{r} \\ -c \\ b \\ \dots \end{array} \begin{vmatrix} a & ? & c \\ 0 & a2 & b \\ 0 & 0 & a3 \\ 0 & 0 & 0 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} = \begin{vmatrix} w \\ ? \\ ? \\ ? \end{vmatrix}$$

Elimination

Systematic combinations of equations

$$\begin{array}{c} \cdots \\ \mathbf{a3} \\ \mathbf{-c} \\ \end{array} \begin{vmatrix} a & 0 & 0 \\ 0 & a2 & 0 \\ 0 & 0 & a3 \\ 0 & 0 & 0 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} = \begin{vmatrix} ? \\ ? \\ ? \\ ? \end{vmatrix}$$

Overall algorithm is $O(n^3)$ to solve n equations

Beware of a special case, pivoting, for 0 coefficients

Inequalities

Variable elimination generalizes substitution

Core Idea

Pick a variable (z) to eliminate from the inequalities

$$2x + 3y \le 7$$

$$3x - y + z \le 5 \longrightarrow z \le 5 - 3x + y$$

$$x - 2y - z \le 3 \longrightarrow x - 2y - 3 \le z$$

$$4x - 3y \le 8 \longleftarrow x - 2y - 3 \le 5 - 3x + y$$

New inequalities with **one fewer variable**

Example

$$\begin{vmatrix} 1 & -1 & \\ & 1 & -1 \\ 1 & -1 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} \leq \begin{vmatrix} -1 \\ -1 \\ -1 \end{vmatrix}$$

Eliminate the z variable from these inequalities

$$\begin{vmatrix} 1 & -1 \\ 1 & 0 \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} \leq \begin{vmatrix} -1 \\ -2 \end{vmatrix}$$

Now **eliminate the y variable**

$$\begin{vmatrix} 1 \end{vmatrix} \begin{vmatrix} x \end{vmatrix} \leq \begin{vmatrix} -2 \end{vmatrix}$$ **Satisfiable**

Multiple Variables

Group by **negative, positive, or zero** coefficient

$$-z + 2y \leq 12 \qquad z + 2x \leq 3 \qquad -y \leq 0$$
$$-z + 3y - x \leq 1 \qquad z + y - x \leq 4$$
$$2z - y \leq 6$$

Rewrite to isolate variable

$$2y - 12 \leq z \qquad z \leq 3 - 2x \qquad -y \leq 0$$
$$-1 + 3y - x \leq z \qquad z \leq 4 - y + x$$
$$2z \leq 6 - y$$

Multiple Variables

$$2y - 12 \leq z \qquad z \leq 3 - 2x \qquad -y \leq 0$$

$$-1 + 3y - x \leq z \qquad z \leq 4 - y + x$$

$$2z \leq 6 - y$$

Make left and right equal with **common multiple**:

$$4y - 24 \leq 2z \qquad 2z \leq 6 - 4x \qquad -y \leq 0$$

$$-2 + 6y - 2x \leq 2z \qquad 2z \leq 8 - 2y + 2x$$

$$2z \leq 6 - y$$

Multiple Variables

$$4y - 24 \le 2z \qquad 2z \le 6 - 4x \qquad -y \le 0$$

$$-2 + 6y - 2x \le 2z \qquad 2z \le 8 - 2y + 2x$$

$$2z \le 6 - y$$

Equivalent to one large equation:

$$\textbf{max}(4y - 24, -2 + 6y - 2x) \le 2z \le \textbf{min}(6 - 4y, 8 - 2y + 2x, 6 - y)$$

$$\downarrow$$

$$\textbf{max}(4y - 24, -2 + 6y - 2x) \le \textbf{min}(6 - 4y, 8 - 2y + 2x, 6 - y)$$

Multiple Variables

$$\textbf{max}(4y - 24, -2 + 6y - 2x) \leq \textbf{min}(6 - 4y, 8 - 2y + 2x, 6 - y)$$

Equivalent to **pairwise inequalities**:

$$4y - 24 \leq 6 - 4y \qquad -2 + 6y - 2x \leq 6 - 4y$$

$$4y - 24 \leq 8 - 2y + 2x \qquad -2 + 6y - 2x \leq 8 - 2y + 2x$$

$$4y - 24 \leq 6 - y \qquad -2 + 6y - 2x \leq 6 - y$$

Add back equations **without** z:

$$-y \leq 0$$

Multiple Variables

Eventually, we eliminate down to **1 variable**

$$\begin{aligned} x &\leq 2 \\ 2x &\leq 3 \\ 3x &\leq 4 \end{aligned} \qquad 1 \leq x \qquad\qquad 0 \leq 1$$

Resulting equations are easy to check:

$$\begin{aligned} 1 &\leq 2 \\ 2 &\leq 3 \\ 3 &\leq 4 \end{aligned} \qquad 0 \leq 1$$

Course Updates

Project Proposals

Project Ideas

Some **memorable projects** from past years

— Verifying a neural network using SMT

— Verifying Rust code with a model checker

— SMT for type checking ("Liquid Types")

— Finding math counterexamples with SMT

Project Proposals

1 page **Project Proposals due** in a week

You've been **assigned a group**, unless you wanted solo project

Make sure to **check the rubrik** for what to include:

Group Project

User need

Goal

Technical approach

Per-milestone plan

Solo Assignment

Language design

Example code

Likely complications

Per-milestone plan

Alternative Assignment

The solo assignment is **verifying quicksort**:

- Implement a new programming language
- Add annotations for verification
- Generate verification conditions to SMT
- Verify and test a quicksort implementation

Complexity

Why integer equations are hard

Speed

Algorithm works but produces **a lot of inequalities**

Group n inequalities into $n_+ + n_- + n_0$ inequalities

Form $n_+ n_-$ new inequalities, plus n_0 old ones

If $n_+ = n_- = n/2$ and $n_0 = 0$, takes n to $n^2/4$

After all k variables eliminated, $n^{2^k}/4^k$ **equations**

There are tricks to skip **redundant equations**…

In practice, variants of linear programming are used

Linear optimization

Finds $x_1, \ldots, x_n$ that form a vector **x**:

$$\left.\begin{array}{r}\text{Maximize } \mathbf{c}^{\mathbf{T}}\mathbf{x} \\ \text{Given } \mathbf{M}\ \mathbf{x} \le \mathbf{b}\end{array}\right\} \textbf{For real x}$$

Efficient algorithms exist for linear optimization

Simplex Algorithm	1947	Average O(n^3), worst-case O(2^n)
Ellipsoid Algorithm	1979	Worst-case O(n^4)
Karmarkar's Algorithm	1984	Worst-case O(n^3.5)
Path-following	2018	Worst-case O(n^2.372), practical sizes O(n^3)

Non-integers

Rationals and reals are **less complex** than integers

- Linear optimization efficiently solves linear real inequalities
- Tarsi’s algorithm eliminates variables even with multiplication
- Multiplication queries relatively efficient (doubly exponential)

Luckily, **real-world** integer queries tend to be simple

- Multiplication and divisibility reasoning rare
- Real solutions can **guide search** for integer solutions

SAT in Integers

SAT problems can be **rephrased as integer** problems

$$x, y := v \mid -x \mid x \vee y \mid x \wedge y$$

v	a	a	a
$0 \leq v$ $v \leq 1$	$a \leq 1 - x$ $1 - x \leq a$	$x \leq a$ $y \leq a$ $a \leq x + y$	$a \leq x$ $a \leq y$ $x + y \leq a + 1$

So solving **integer inequalities is as hard as SAT**.

Quantifiers

What about **quantified** linear equations?

Quantifier Elimination $\exists x, P(x) \Leftrightarrow Q$

Is it **always possible**?

$$\exists x, x < y \land -y < x \qquad\qquad \exists x, 2x = y$$

$$0 < y \qquad\qquad ?$$

Adding $n \mid x$ relation **makes elimination possible**

Quantifiers

What about **quantified** linear equations?

$$cx < E_1 \qquad E_2 < cx \qquad n \mid cx + E_3 \qquad n \nmid cx + E_4$$

- Rewrite cx as quotient, remainder of ns
- Test all possible remainders
- Combine remaining inequalities
- Result is formula without x

Details in Chapter 7 of textbook

Multiplication

For **any program** P, consider $\exists x, P(x) = y$.

There is a polynomial $Q(y, x_1, \ldots, x_{11})$ so that

$$\exists x, P(x) = y \Leftrightarrow \exists x_1 \cdots \exists x_{11}, Q(y, x_1, \ldots, x_{11}) = 0$$

Fact about programs

Fact about integer polynomial

Facts about multiplication **as hard as any fact** at all!

That said, heuristics can handle some simple cases…

Examples

This is true **only** when n is prime:

$$\exists a \exists b \forall (i \leq \bar{n}) \exists s \exists w \exists p \exists q \forall j \forall v \exists e \exists g$$
$$\{(s+w)^2 + 3w + s = 2i \wedge ([j = w \wedge v = q] \vee [j = 3i \wedge v = p + q]$$
$$\vee [j = s \wedge (v = p \vee (i = \bar{n} \wedge v = q + \bar{n}))] \vee [j = 3i + l \wedge v = pq]$$
$$\rightarrow a = v + e + ejb \wedge v + g = jb)\}.$$

There's an n for which this **cannot** be proven or disproven:

$$\exists ab \forall i_{\leqq \bar{n}} \exists swpq \forall jv \exists eg \{(s+w)^2 + 3w + s = 2i \wedge ([j = w \wedge v = q] \vee [j = 3i \wedge v = p + q]$$
$$\vee [j = s \wedge (v = p \vee (i = \bar{n} \wedge v = q + \bar{n}))] \vee [j = 3i + 1 \wedge v = pq] \rightarrow a = v + e + ejb$$
$$\wedge v + g = jb)\}.$$

Next class:

Integers

To do:

- ☐ Course feedback
- ☐ Read Chapter 8
- ☐ Assignment 2

Integers

Solving conjunctions of **integer equalities**

Back to high school with elimination and substitution

Variable elimination for integer inequalities

Combining two inequalities into one

How fast can integer reasoning be?

SAT, multiplication, and rational numbers

THEORIES

INDICIES

VARIABLES

DECOMPOSITION

READ OVER

WRITE

FRAGMENT

ARRAY

PROPERTIES

Next class:

Integers

To do:

- ☐ Course feedback
- ☐ Read Chapter 8
- ☐ Assignment 2