Lecture 10

- EUF
- Theory combination with the Nelson Oppen algorithm

$(\exists x_1\ x_2\ x_3)$ | $x_1 = x_2$ and $(x_2 = x_3$ or $x_3 \neq x_1)$

$\mathbb{Z}/\mathbb{R}$
$\mathbb{Q}/\ldots$

Skeleton → SAT

Theory

$[x_1 = x_2$ and $x_2 = x_3$ and $x_3 \neq x_1]$

① Construct the equality graph:

$x_1 \text{ —— } x_2 \text{ —— } x_3$

Claim: Two variables are in the same SCC iff the equality constraints force them to be equal.

② Check if ∃ inequality constraint which is in conflict with the equality graph.

Unsat if yes. Sat if no.

```
int cube (int x) {
    int ans = (x * x) * x;
    return ans;
}
```

(x + x) + x

```
int cube' (int x) {
    int ans = x;
    for (i=0; i<2; i++)
        ans = ans * x;
                ans + x
    return ans;
}
```

$\exists x \in \mathbb{Z} \cdot (x \oplus x) \oplus x \neq a_3$

$a_1\ a_2\ a_3$

and $a_1 = x$ and

$a_2 = a_1 \oplus x$ and

$a_3 = a_2 \oplus x$

a_1 ans = x

a_2 ans = ans * x ← x * x

a_3 ans = ans * x ← (x * x) * x

```
int f1 (int x) {
    int ans = (x ⊕ x) ⊕ x;
    return ans;
}
```

```
int f2 (int x) {
    int ans = x;
    for (i = 0; i < 2; i++)
        ans = ans ⊕ x;
    return ans;
}
```

$\exists f \; \exists x \quad f(x) = x$

f

Input	Output
—	—
—	—
—	—

Claim: If a formula is satisfiable,

we can demonstrate satisfiability

by only filling in finitely many entries in the table

Ex :

```
(set-logic ALL)
(set-option :produce-models true)

(declare-const x Int)
(declare-const y Int)
(declare-fun f (Int) Int)

(assert (not (= (f x) (f y))))

(check-sat)
(get-model)
```

Let x = 0
Let y = 1
Let f in = { 0, if in = 1
           { -1, otherwise

Interpretation of f

```
sat
(
(define-fun x () Int 0)
(define-fun y () Int 1)
(define-fun f ((BOUND_VARIABLE_401 Int)) Int (ite (= BOUND_VARIABLE_401 1) 0 (- 1)))
)
```

in in

Syntax of EUF constraints

EUF constraint ::= $lit_1 \wedge lit_2 \wedge \cdots \wedge lit_k$

EUF Literal ::= $Term_1 = Term_2 \mid Term_1 \neq Term_2$

Term ::= Var x, y, z, ...

| Function application f(Term)

Ex:

$(\exists f)_{\mathbb{Z}\to\mathbb{Z}}\ (\exists x)_{\mathbb{Z}}\cdot\ f(x)=x$ and $f(f(x))\neq f(x)$

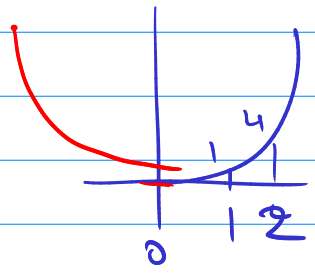
$f(x)\neq x$

Question: How to describe $f(x)=x^2$?

- $\exists f \cdot \forall x,\ f(x)=x*x$.

- $\exists f \cdot \forall x\ \ f(x+1)=f(x)+x+x+1$

  and $f(0)=0$



$f(0)=f(-1)-2+1$

$f(-1)=1$

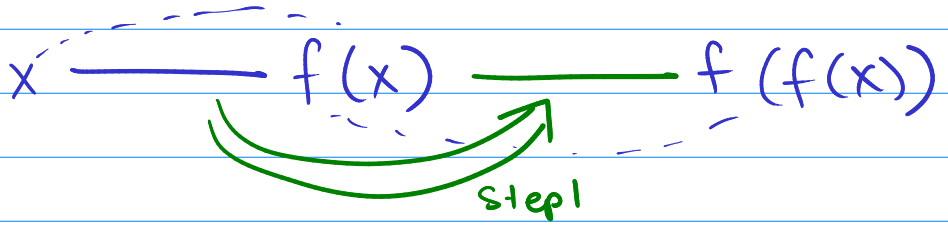
Congruence Closure Algorithm (4.3.1 of K+S)

Ex:

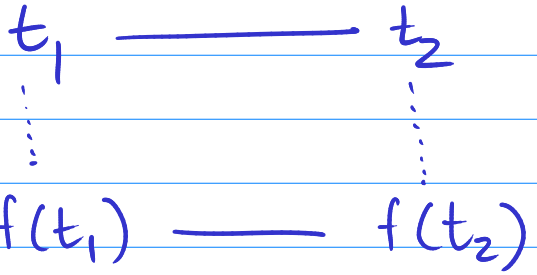
$(\exists f : \mathbb{Z} \to \mathbb{Z})(\exists x \in \mathbb{Z}) \cdot f(x) = x$ and $f(f(x)) \neq f(x)$

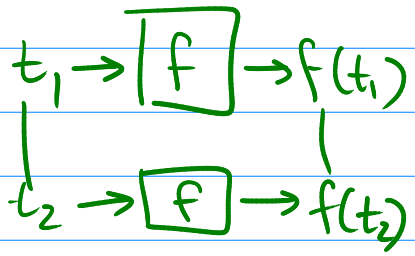
$f(x) \neq x$

Step 0: Enumerate all terms in the constraint.



Step 1: Add equality constraints, one at a time





Also perform congruence closure of constraints:

If we just added a $t_1 \text{---} t_2$ edge

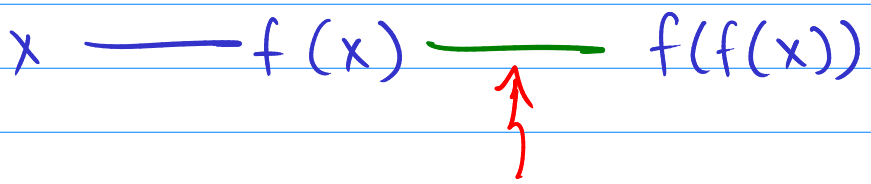
& $f(t_1)$ & $f(t_2)$ both occur in the formula,

add $f(t_1) \text{---} f(t_2)$ edge.

Step 3: Check if ∃ inequality constraint

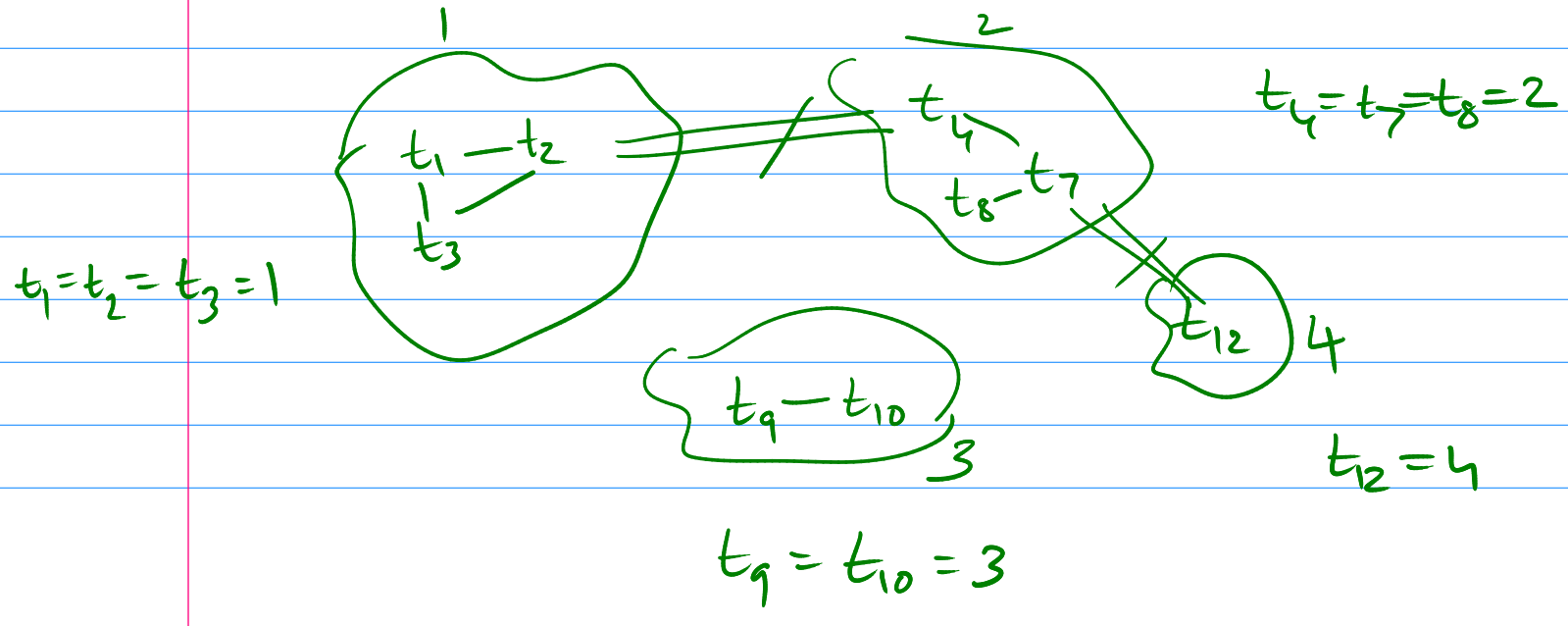
$$t_1 \neq t_2$$

which is in conflict with the saturated equality graph.



$f(f(x)) \neq f(x)$

But both $f(x)$ & $f(f(x))$ occur in the same SCC. So unsat.



Quantified formulas which are decidable

- EPR (Effectively Propositional Logic)

  Bernays - Schonfinkel class

  Frank Ramsey

$\exists\exists\exists\exists\ \forall\forall\forall\forall\forall$

$\exists^*\ \forall^*$

$\leq$

$x_1 = x_2,\ x_1 \neq x_2,$

$R(x_1, x_2),\ R(x_1, x_3, x_4)$

...

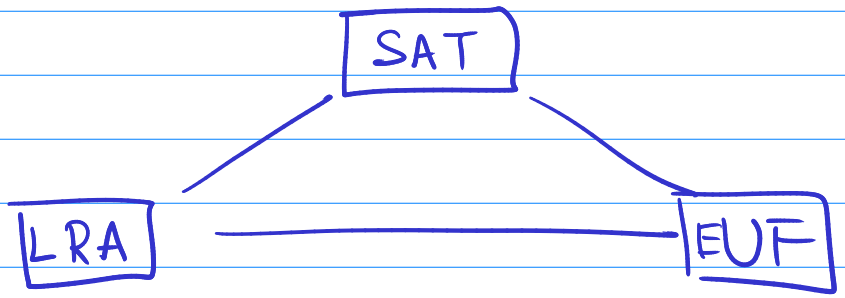
How to combine theories?

Ex: $(x_2 \geq x_1)$ and

$(x_1 - x_3 \geq x_2)$ and

$(x_3 \geq 0)$ and

$(f(f(x_1) - f(x_2)) \neq f(x_3))$



UFLRA

All have equality

Given: Theory solvers for T_1 T_2 ... T_n

Apart from $=$, no common function symbols relation

$+ \in$ LRA

$+ \notin$ EUF

all interpreted over infinite domains, &

all theories convex,

then Nelson-Oppen procedure gives a solver for combined theory $T_1 \cup T_2 \cup \cdots \cup T_n$.

Example of Nelson Oppen

Ex: $f(x_1, 0) \geq x_3$ and

$f(x_2, 0) \leq x_3$ and

$\therefore x_1 \geq x_2$ and

$x_2 \geq x_1$ and

$x_3 - f(x_1\ 0) \geq 1$

Step 0: "Purify" the formula.

$a_1 = f(x_1, 0)$ and $a_1 \geq x_3$ and

$a_2 = f(x_2\ 0)$ and $a_2 \leq x_3$ and

$x_1 \geq x_2$ and

$x_2 \geq x_1$ and

$x_3 - a_1 \geq 1$

LRA	EUF
$a_1 \geq x_3$	$a_1 = f(x_1, 0)$
$a_2 \leq x_3$	$a_2 = f(x_2, 0)$
$\begin{cases} x_1 \geq x_2 \\ x_2 \geq x_1 \end{cases}$	
$x_3 - a_1 \geq 1$	
$\Rightarrow \quad x_1 = x_2$	$(x_1 = x_2)$!!!

$(a_1 = a_2)$!!! $\Rightarrow a_1 = a_2$

$\Rightarrow a_1 = x_3, \; a_2 = x_3$

$\Rightarrow a_1 - a_1 \geq 1$

$0 \geq 1$! Contradiction !

Unsat !