Satisfiability Procedures Based on Congruence Closure

- Consider the theory of arrays with McCarthy's axioms
  - symbols: sel, upd, =, ≠
    - add uninterp. function symbols since we are going to extend congruence closure
  - axioms

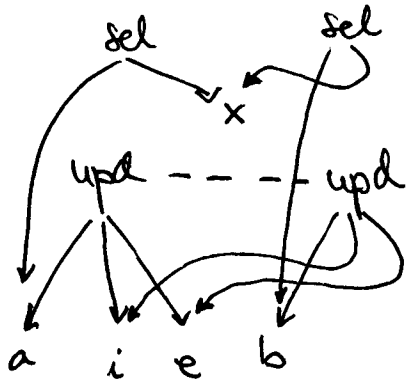
$$\forall a i e \quad sel(upd(a,i,e),i) = e \qquad (1)$$

$$\forall a i j e \quad i \neq j \Rightarrow sel(upd(a,i,e),j) = sel(a,j) \qquad (2)$$

- example of a theorem

$$upd(a,i,e) = upd(b,i,e) \wedge sel(a,x) \neq sel(b,x) \Rightarrow x = i$$

- again, like for lists just doing closure for equivalence and axioms is not enough.



← closed for Eq, Ax but seems satisfiable

Again, like for lists we look at two possible solutions.

1) extend the set of axioms
2) add more nodes to the graph

Try 2.

- we have an E-DAG that denotes a partial interpretation ψ_G
  - universe is the set of representatives
  - if t is represented then $\psi_G(t) = t^*$
  - ψ_G satisfies Eq, Ax
  - but is partial
  - Everything is Ok if we can extend ψ_G to be total without running into contradictions.
- This is tricky. E.g, the graph before we cannot define

  $\psi(sel(upd(a,i,e),x))$

  because it would have to be equal with

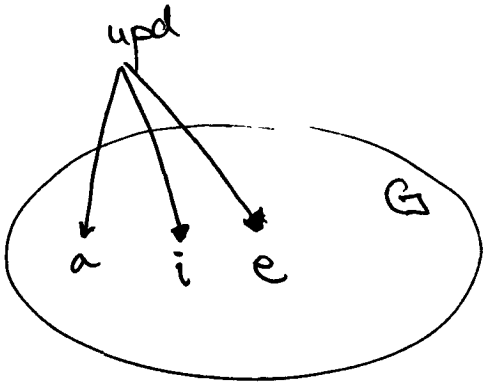
  $\psi(sel(a,x))$ and

  $\psi(sel(upd(b,i,e),x)$ and

  $\psi(sel(b,x))$. Impossible, contradicts $sel(a,x) \neq sel(b,x)$.
- See, we will have to add nodes (or axioms for solution 1

· Incremental extension

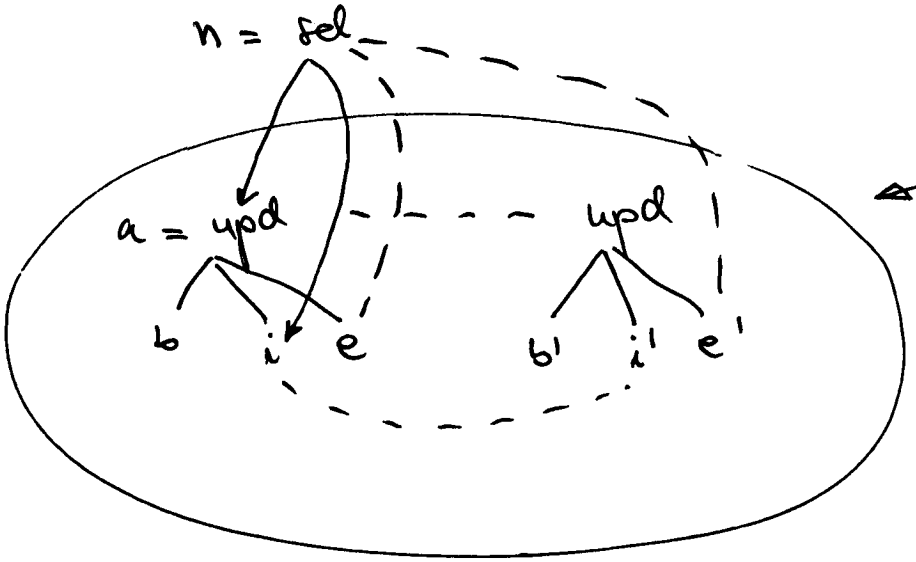
· assume upd(a, i, e) is not represented, but a and i, e are represented



· There are no new instantiations of the axioms

· We can assign any value to $\psi(upd(a,i,e))$ without violating any of the axioms

· assume sel(a, i) is not represented but a and i are represented



we could violate axiom 1

Since

$n = e$ and $n = e'$

but

$e^* \neq e'^*$

This suggest adding the axiom

$$\forall b b' i e e'.\ upd(a,i,e) = upd(b',i,e') \Rightarrow e = e'$$

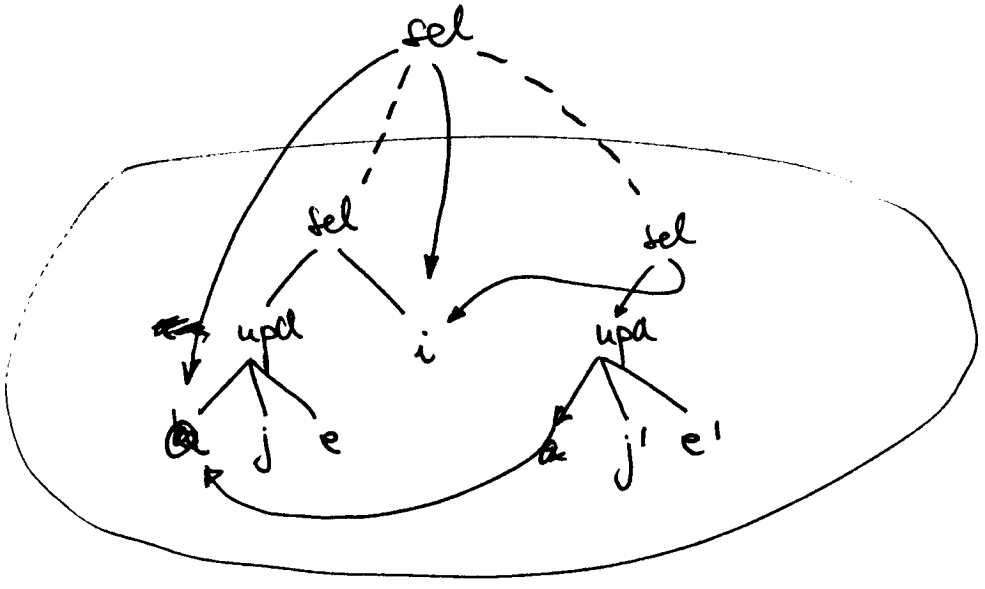
Another way to fix this problem is to ensure that

Rule 1

> Whenever $upd(b,i,e)$ is represented
> $sel(upd(b,i,e),i)$ is also represented

- this can be achieved by adding one sel node for each upd node
- this will prevent the scenario above.

- again, $sel(a,i)$ is not represented, but a and i are represented



- This contradicts axiom 2

This can be fixed with axiom

$$i \neq j \wedge i \neq j' \Rightarrow sel(upd(a,j,e),i) = sel(upd(a,j',e'),i)$$

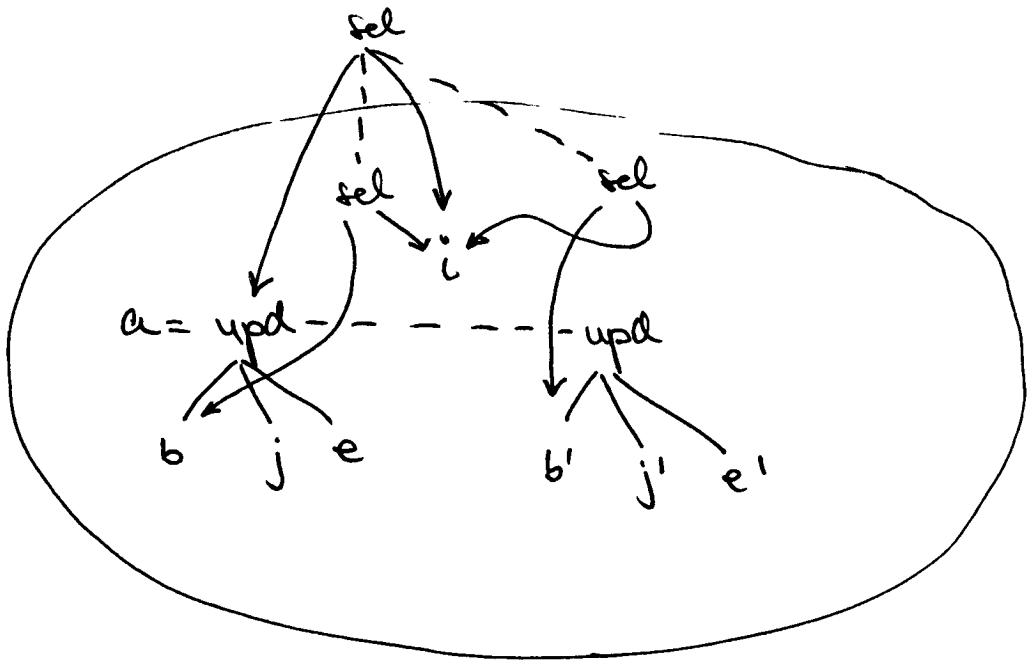
Another way to fix this problem is to ensure that

Rule 2

> whenever $sel(upd(a,j,e),i)$ is represented and $i^* \neq j^*$ then $sel(a,i)$ is also represented

- for each sel adds at most one other sel

- yet another possible problem when adding $sel(a,i)$



To fix this we can add the axiom

$$upd(b,j,e) = upd(b',j',e') \wedge i \neq j \wedge i \neq j'$$

$$\Rightarrow sel(b,i) = sel(b',i)$$

Again, we can fix this problem by adding nodes to ensure that

Rule 3

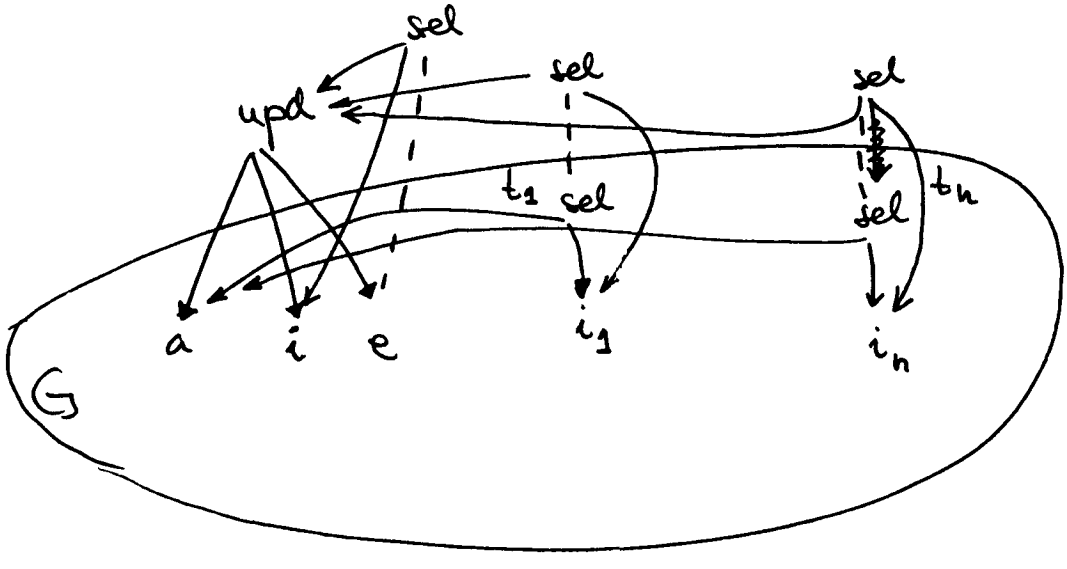
> whenever $upd(b,j,e)$ and $sel(b,i)$ are represented and $i^* \neq j^*$ then
>
> $sel(upd(b,j,e), i)$ is also represented.

We can now show that if we have enough nodes (as specified above) then we can extend Ψ_G on unrepresented nodes:

- to add $upd(a,i,e)$
  - Let $t_1, \ldots, t_n$ be the nodes labelled sel and first successors equivalent to a and second successors not equivalent to i

    Rule 1 $\Rightarrow$ · add $sel(upd(a,i,e), i) = e$

    Rule 3 $\Rightarrow$ · add $sel(upd(a,i,e), i_k) = sel(a, i_k)$



- to add $sel(a, i)$
  - no Rule 1 extensions
  - we will add a bunch of $sel(b, i)$
  - Rule 3 extensions cannot trigger Rule 2 extensions
- do Rule 2 extensions first

$$sel(upd(upd(\dots upd(a, i_1, e_1), i_2, e_2)\dots), i_n, e_n), i)$$

add

$sel(a, i)$

$sel(upd(a, i_1, e_1), i)$

$\vdots$

$sel(upd(upd(\dots)), i$

} n new sel nodes

- do Rule 3 extensions now

~~This is a convex ~~sets~~ theory~~
~~can be seen already from Axiom 2~~
~~$\Rightarrow i = j \vee sel(upd(a, i, e), j) = sel(a, j)$~~

- The max number of sel nodes added is $O(n^2)$
- for each $upd(a, j, e)$ and $sel(a, i)$ add

$$sel(upd(\mathbb{a}, j, e), i)$$

The theory of arrays is non-convex

- can be seen already from Axiom 2
  - $\Rightarrow i = j \vee sel(upd(a,i,e),j) = sel(a,j)$
- Consider also

$$upd(upd(\ldots upd(a,i_1,x),i_2,x)\ldots,i_n,x) = upd(upd(\ldots upd(a,j_1,x),j_2,x)\ldots,j_{n-1},x) \wedge$$

~~This literal implies~~

$$sel(a,i_1) \neq x \wedge \ldots \wedge sel(a,i_n) \neq x$$

This literal implies

$$\bigvee_{k \neq l} i_k = i_l$$

Since the array on the right of equality differs from a in $n-1$ places only.

- Thus a literal of length n might cause $O(n^2)$ splits
- Algorithm
  - add nodes to graph $O(n^2)$ nodes
  - will have $O(n^2)$ disequalities to consider
  - consider all combinations of disequalities
    - if a disequality is assumed to hold then the added sel nodes in Rule 2 and 3 are merged with the sel node that triggered the rule

$\Rightarrow O(2^{n^2})$ ← Bad