Reasoning with Norm Models

Alberto Siena

Motivation

- Law is part of the environment, which the STS operates in
- The need to capture legal prescriptions at requirements time grows when law becomes difficult to be captured
  - Language
  - Interpretation
  - (Change)
  - Structural complexity ("Spaghetti law")
    - Applicability conditions
    - Derogations
    - Cross-references
    - Hierarchies

Objectives

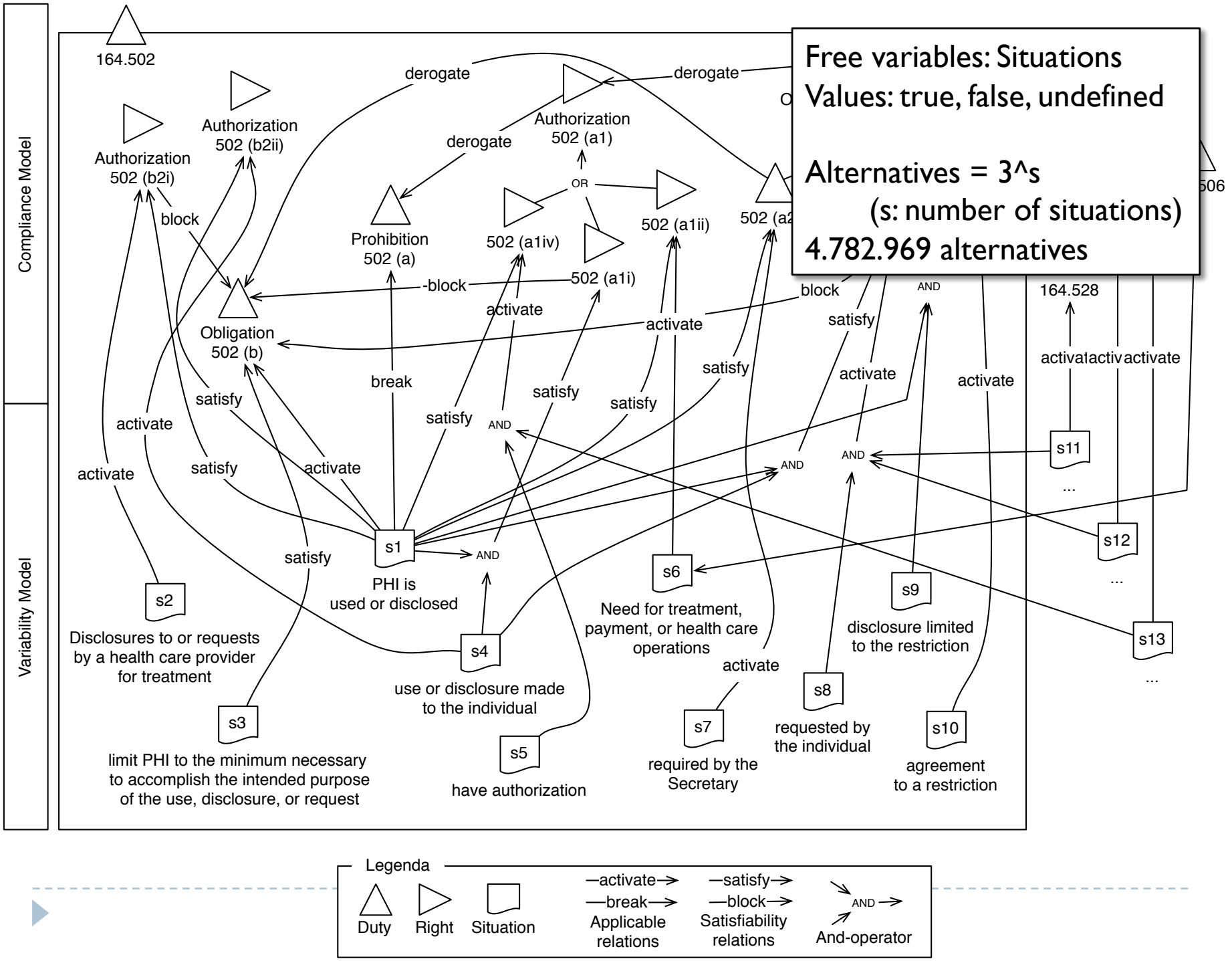
- Support requirements engineers in finding a path through the conditional elements
- No heavyweight approaches (AI)
- Rely on conceptual modeling
- Automatic reasoning
- Reduce the number of alternatives to a tractable subset
  - (Best case: 1 alternative)

Nòmos

- Framework for building conceptual models of norms
  - Vaguely based on i*
  - Adds the concepts of Norm
  - Borrows the concept of Situation
- RE language independent
  - No domain information (e.g., goals)
  - Can be attached to any other RE modeling language
  - Class-level
- Maps natural language documents onto property graphs

Nòmos

- Law as a graph L = {N, S, R, r}
- N = Norm elements: tuples (t, H, C, A, P)
  - t = Norm Type (duty, right)
  - H = Holder
  - C = Counter-part
  - A = Precedent
  - P = Consequent
- S = Situation elements
  - satisfied, not satisfied, undefined
- R = Role elements
  - Used for clustering
- r = Relations
  - Link Situations and Roles to Norms' precedents, consequents, holders and counter-parts


Compliance Model
Variability Model
164.502
Authorization 502 (b2i)
Authorization 502 (b2ii)
Authorization 502 (a1)
Prohibition 502 (a)
Obligation 502 (b)
OR
502 (a1iv)
502 (a1ii)
502 (a1i)
derogate
block
-block
activate
satisfy
break
AND
s1
PHI is used or disclosed
s2
Disclosures to or requests by a health care provider for treatment
s3
limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request
s4
use or disclosure made to the individual
s5
have authorization
s6
Need for treatment, payment, or health care operations
s7
required by the Secretary
s8
requested by the individual
s9
disclosure limited to the restriction
s10
agreement to a restriction
s11
s12
s13
164.528
...
Free variables: Situations
Values: true, false, undefined
Alternatives = 3^s
(s: number of situations)
4.782.969 alternatives
Legenda
Duty
Right
Situation
activate
break
Applicable relations
satisfy
block
Satisfiability relations
AND
And-operator

Intuition

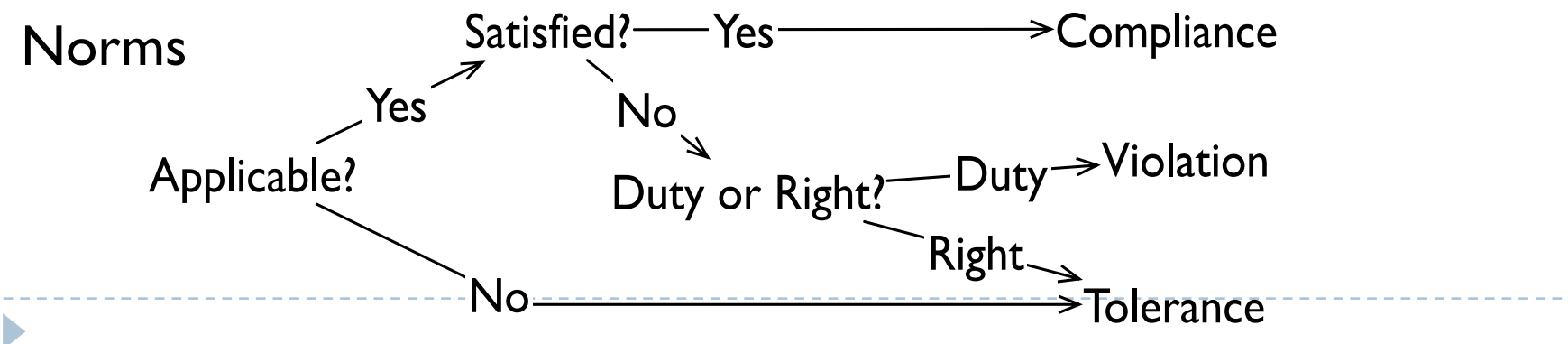
- Not all the alternative have the same properties
- Regulatory compliance engineering as a problem of alternative selection
  - **pruning unnecessary alternatives**
  - **satisfying desiderata**
- How to formalize the model?
- How to make a choice?

How to formalize the model?

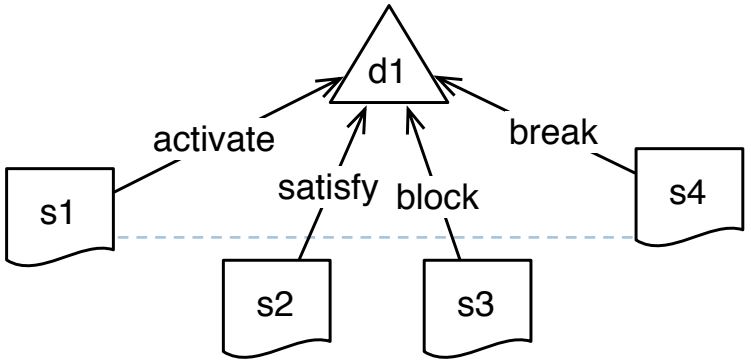
- Datalog
  - First-order logic language for deductive databases
  - Bottom-up and top-down queries
- DIv
  - Disjunctive Datalog
  - Use variables grounding to generate sets of answers
- Approach
  - Define transformation rules from Nòmos relations and axioms into Datalog predicates and rules
  - Encode a given Nòmos model as a Datalog program

Situations: satisfied, not satisfied, undefined

Relations	If source is	Target is
Activate	Satisfied	Applicable
Block	Satisfied	Not Applicable
Satisfy	Satisfied	Satisfied
Break	Satisfied	Not Satisfied
Endorse	Complied	Applicable
Derogate	Complied	Not Applicable
Imply	Complied|Violated	Complied|Violated

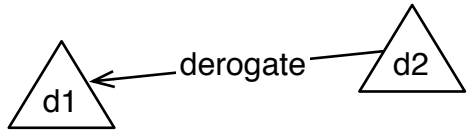


Formalization
Activate and Satisfy




```
% satisfy( d1, [s2] ).
satisfied(d1) :- satisfied(s2).
satisfied_unknown(d1) :- not satisfied(s2).

% break( d1, [s4] ).
not_satisfied(d1) :- satisfied(s4).

% activate( d1, [s1] ).
applicable(d1) :- satisfied(s1).

% block( d1, [s3] ).
not_applicable(d1) :- satisfied(s3).
```

Formalization
Derogate




```
% activate( d1, [s1] ).
applicable(d1) :- satisfied(s1), not satisfied(d1s).

% derogate( d1, [d2] ).
satisfied(d1s) :- compliant(d2).
not_applicable(d1) :- satisfied(d1s).
```

Formalization
Compliance rules

```
% Compliance rules for duty d1
compliant(d1) :- applicable(d1), satisfied(d1).
violated(d1) :- applicable(d1), not satisfied(d1).
inconclusive(d1) :- applicabile_undefined(d1).
tolerated(d1) :- not_applicable(d1).
tolerated(d1) :- compliant(d1).
conflict(d1) :- tolerated(d1), violated(d1).

% imply( d3, [d1] ).
compliant(d3) :- compliant(d1).
```

How to make a choice?

- Define properties to be verified
  - Input: a Nòmos model + desirable properties
  - Choice: properties optimization
  - Output: a subset of the alternatives space in which the properties hold
- Properties identified so far:
  - Compliance
  - Preference
  - Freedom
  - Desirability

Compliance

- Compliant solutions
  - Foreach N in L, tol(N)
- Problem: true alternatives

Example

Application must submitted through the electronic form

Application must be submitted:
a) through the electronic form
b) or, via email

- Need to structure hierarchies: use Imply relations

```
% Objectives
tol(sec502) ?
```

Preference

- Situations have cost
  - E.g.: time, money, etc.
- Cost can't be properly evaluated
- Relative cost can be estimated
  - Relative cost = "higher" or "lower"
  - Partial order over situations

```
% rankings
% rank 1: time          % rank 2: cost
:~ st(s1). [1:1]       :~ st(s1). [2:2]
:~ st(s2). [1:2]       :~ st(s2). [2:1]
```

Freedom

- Law gives explicit alternatives and rights to be discretionally exercised
- Once decided to select one alternative or to exercise one right, they become mandatory requirements
  - Changing means do again the compliance check
- The less we decide, the more we are free to do at requirements elicitation
- Operationally: use "Undefined" values

```
% Ranking
% rank 1: freedom
:~ sf(s1). [1:1]
:~ st(s1). [1:1]
```

Desiderata

- Some situations are known or desired to have certain values
  - Information arising from the domain
  - "What if" analysis
- Expressed as constraints.

```
% Scenario
st(s1) v sf(s1) v su(s1).
st(s2) v sf(s2) v su(s2).
st(s3) v sf(s3) v su(s3).
st(s4).
st(s5).
st(s0).
```

Tool support

- NRTool
- Java Wrapper on top of DLV

- Applicability analysis
  - Given a set of known situations, which norms apply?
- Compliance analysis
  - Given a set of known situations, which norms are violated?
- Compliance search
  - Given a set of known situations, which situations should be assigned to reach compliance?
  - If at least one solution is found, then compliance is ensured

```
# norms
duty sec502 a b c a2 a2i a2ii sec528 sec524
sec508 sec506
right b2i b2ii a1 a1i a1ii a1iv
```

```
# situations
situation s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12
s13 s14 always
```

```
# law structure relations
imply a1iv a1i a1ii a1 or
imply a2ii a2i a2 or
imply b2i b2ii b a a1 a2 c sec502
```

```
derogate b2i b
derogate b2ii b
derogate a2i b
derogate a2ii b
derogate a1 a
derogate a2 a
derogate a2 a1

endorse a2i b2ii
endorse a1i b2ii
```

```
# compliance relations
activate always a
activate s2 b2i
activate s4 b2ii
```

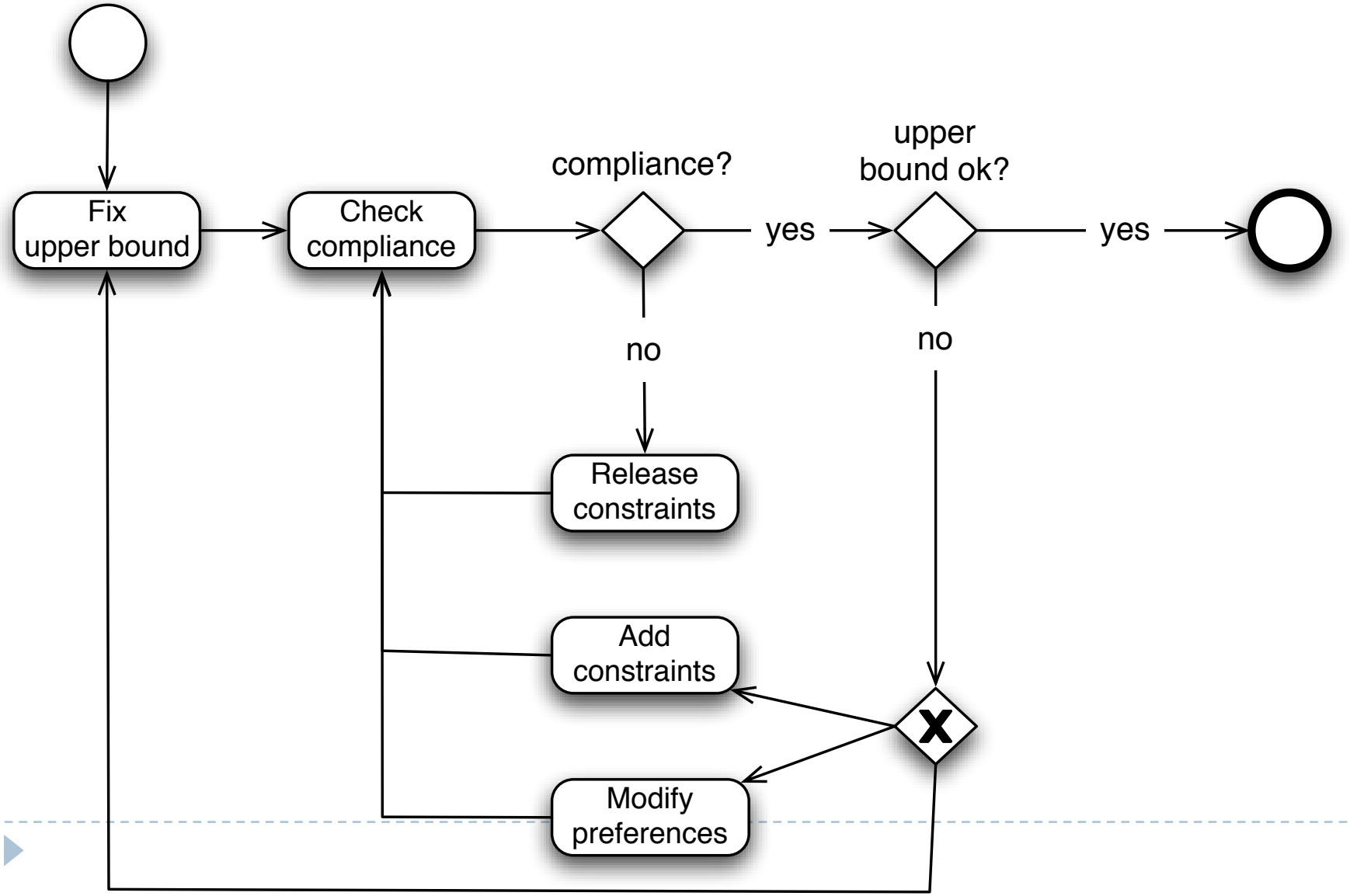
```
activate s1 b
activate s5 s13 a1iv
activate s14 a1i
activate s6 a1ii
activate s7 a2ii
activate s8 s11 s12 a2i
activate s10 c

satisfy s1 b2i
satisfy s1 b2ii
satisfy s3 b
satisfy s1 a1iv
satisfy s1 s4 a1i
satisfy s1 a1ii
satisfy s1 a2ii
satisfy s1 s4 a2i
satisfy s1 s9 c

break s1 a
```

```
value st always
```

```
rank freedom
freedom 1 st s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11
s12 s13 s14
freedom 1 sf s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11
s12 s13 s14
```

```
query tol sec502
```

Methodology



Results

- 4.782.969 → 1

  "PHI is used or disclosed
  Disclosures to or requests by a health care provider for treatment
  Use or disclosure made to the individual
  There is a request from the Secretary
  Disclosure limited to the restriction
  There is an agreement to a restriction"

- Compliant; Freedom degree: 6
- Freedom degree 7: 16 alternatives
- Freedom degree 8: 113 alternatives

Future work

- Reasoning about Roles
- Reasoning about instances
- Defining additional, significant properties
- Larger data set
- Test in other contexts
  - (not just law compliance)
- Time (sequences of situations)

Thank you