# General overview of a $T$-Solver for Difference Logic

Albert Oliveras and Enric Rodríguez-Carbonell

Deduction and Verification Techniques
Session 3
Fall 2009, Barcelona

Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITECNICA DE CATALUNYA

# Difference logic

- Literals in Difference Logic are of the form $a - b \bowtie k$, where
  - $\bowtie \in \{\leq, \geq, <, >, =, \neq\}$
  - $a$ and $b$ are integer/real variables
  - $k$ is an integer/real
- At the formula level,
  $a{=}b$ is replaced by $p$ and $p \quad \leftrightarrow \quad a \leq b \; \wedge \; b \leq a$ is added
- If domain is $\mathbb{Z}$ then $a - b < k$ is replaced by $a - b \leq k - 1$
- If domain is $\mathbb{Z}$ then $a - b < k$ is replaced by $a - b \leq k - \delta$
  - $\delta$ is a sufficiently small real
  - $\delta$ is not computed but used symbolically
    (i.e. numbers are pairs $(k, \delta)$)
- Hence we can assume all literals are $a - b \leq k$

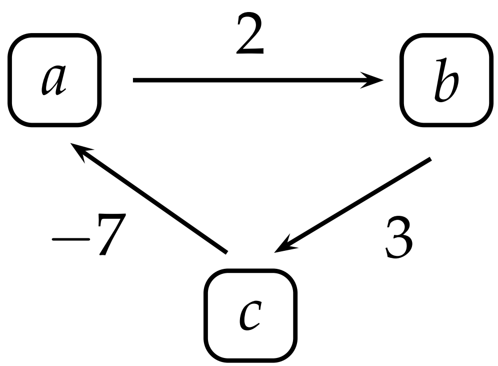
UPC
Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITECNICA DE CATALUNYA

# Difference Logic - Remarks

- Note any solution to a set of DL literals can be shifted (i.e. if $\sigma$ is a solution then $\sigma'(x) = \sigma(x) + k$ also is a solution)
- This allows one to process bounds $x \leq k$
  - Introduce fresh variable *zero*
  - Convert all bounds $x \leq k$ into $k - zero \leq k$
  - Given a solution $\sigma$, shift it so that $\sigma(zero) = 0$
- If we allow (dis)equalities as literals, then:
  - If domain is $\mathbb{R}$ consistency check is polynomial
  - If domain is $\mathbb{Z}$ consistency check is NP-hard ($k$-colorability)
    - $1 \leq c_i \leq k$ with $i = 1 \ldots \#verts$ encodes $k$ colors available
    - $c_i \neq c_j$ if $i$ and $j$ adjacents encode proper assignment

# Difference Logic as a Graph Problem

- Given $M = \{a - b \leq 2,\ b - c \leq 3,\ c - a \leq -7\}$, construct weighted graph $\mathcal{G}(M)$




- **Theorem:**

  $M$ is $T$-inconsistent iff $\mathcal{G}(M)$ has a negative cycle


UPC
Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITECNICA DE CATALUNYA

# Difference Logic as a Graph Problem (2)

**Theorem:**

$M$ is $T$-inconsistent iff $\mathcal{G}(M)$ has a negative cycle

$\Leftarrow$)

Any negative cycle $a_1 \xrightarrow{k_1} a_2 \xrightarrow{k_2} a_3 \longrightarrow \ldots \longrightarrow a_n \xrightarrow{k_n} a_1$ corresponds to a set of literals:

$a_1 - a_2 \leq k_1$
$a_2 - a_3 \leq k_2$
$\ldots$
$a_n - a_1 \leq k_n$

If we add them all, we get $0 \leq k_1 + k_2 + \ldots + k_n$, which is inconsistent since neg. cycle implies $k_1 + k_2 + \ldots + k_n < 0$

# Difference Logic as a Graph Problem (3)

**Theorem:**

$M$ is $T$-inconsistent iff $\mathcal{G}(M)$ has a negative cycle

$\Rightarrow)$
Let us assume that there is no negative cycle.

1. Consider additional vertex $o$ with edges $o \xrightarrow{0} v$ for all verts. $v$
2. For each variable $x$, let $\sigma(x) = -dist(o, x)$
   [exists because there is no negative cycle]
3. $\sigma$ is a model of $M$
   - If $sigma \not\models x - y \leq k$ then $-dist(o, x) + dist(o, y) > k$
   - Hence, $dist(o, y) > dist(o, x) + k$
   - But $k = weight(x \longrightarrow y)$!!!

UPC
Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITECNICA DE CATALUNYA

# Bellman-Ford: negative cycle detection

**forall** $v \in V$ **do** $d[v] := \infty$ **endfor**
**forall** $i = 1$ **to** $|V| - 1$ **do**
  **forall** $(u, v) \in E$ **do**
    **if** `d[v] > d[u] + weight(u,v)` **then**
      `d[v]:= d[u] + weight(u,v)`
      `p[v]:= u`
    **endif**
  **endfor**
**endfor**

**forall** $(u, v) \in E$ **do**
  **if** $d[v] > d[u] + weight(u, v)$ **then**
    `Negative cycle detected`
    `Cycle reconstructed following` $p$
  **endif**
**endfor**

UPC
Departament de Llenguatges i Sistemes Informàtics
UNIVERSITAT POLITÈCNICA DE CATALUNYA

# Consistency checks

- Consistency checks can be performed using Bellman-Ford in time ($O(|V| \cdot |E|)$)
- Other more efficient variants exists
- Incrementality easy:
  - Upon arrival of new literal $a \xrightarrow{k} b$ process graph from $u$
- Solutions can be kept after backtracking
- Inconsistency explanations are negative cycles
  (irredundant but not minimal explanations)

UPC
Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITECNICA DE CATALUNYA

# Theory propagation

- Addition of $a \xrightarrow{k} b$ entails $c - d \leq k'$ only if

$$c \underbrace{\longrightarrow^{*} \; \overbrace{a \xrightarrow{k} b}^{}}_{shortest} \longrightarrow^{*} d \quad \text{with } \overbrace{a \xrightarrow{k} b \longrightarrow^{*} d}^{shortest}$$

- Each edge $a \xrightarrow{k} b$ has its reduced cost $k - \sigma(a) + \sigma(b) \leq 0$
- Shortest path computation more efficient using reduced costs, since they are non-negative [Dijkstra's algorithm]
- Theory propagation $\approx$ shortest-path computations
- Explanations are the shortest paths

Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITECNICA DE CATALUNYA