An Abstract Domain Extending Difference-Bound Matrices with Disequality Constraints

Mathias Péron and Nicolas Halbwachs

Grenoble – France

Motivations

Our belief

integer variables are used to address objects in many situations

- array indexes
- memory addresses and pointers (`C` style)
- addressing of devices (in SoCs)

▶ usefulness of the invariant $x \neq y$

- for alias phenomena: `A`$[x]$ and `A`$[y]$
- for other analyses: *e.g.* independence analysis

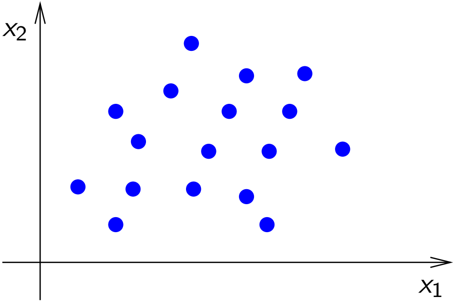
Framework abstract interpretation theory

Goal a new abstract domain handling disequalities

Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains

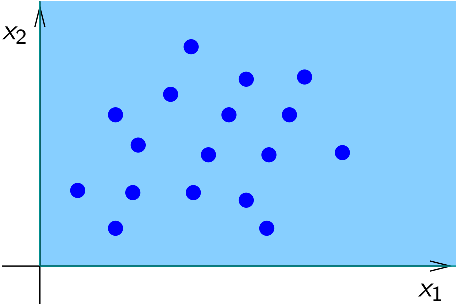


Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains

non-relational domains



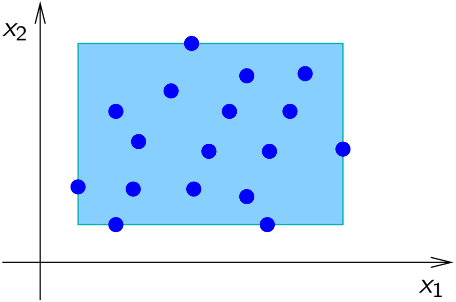
signs $0 \leq x_i$

Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains

non-relational domains



signs

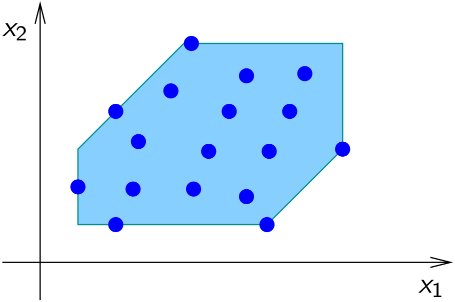
intervals $c_1 \leq x_i \leq c_2$

Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains

2-relational domains



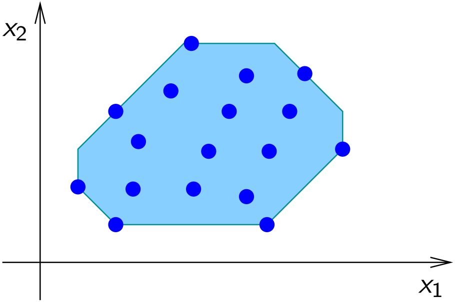
signs
intervals
zones (DBMs) $x_i - x_j \leq c$

Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains

2-relational domains



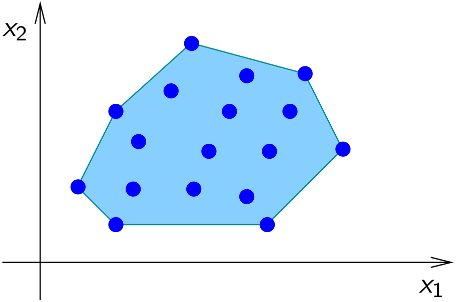
signs
intervals
zones (DBMs)
octagons $\pm x_i \pm x_j \leq c$

Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains

n-relational domains

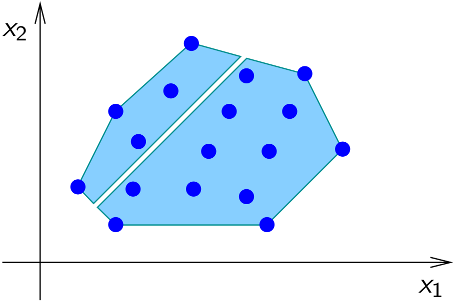


signs
intervals
zones (DBMs)
octagons
convex polyedra $\sum \alpha_i x_i \leq c$

Abstract Interpretation

Abstraction of a set of states:

- by classical (convex) numerical abstract domains



signs
intervals
zones (DBMs)
octagons
convex polyedra

with disequality invariants $x_i \neq x_j$

Which Domain for Disequalities ? (1/2)

Disequalities + equalities a too poor analysis

- trivial deductions
  - $(x = y \land y = z) \Rightarrow x = z$
  - $(x = y \land x \neq z) \Rightarrow y \neq z$

Disequalities + ordering relations a fruitful combination

- deduction power enriched
  - $(x \leq y + c \land c < 0) \Rightarrow x \neq y$
  - $(x \leq y \leq z \land x \neq y) \Rightarrow x \neq z$

Goal

To extend an existing domain without increasing its complexity

Which Domain for Disequalities ? (2/2)

DBM is a good candidate

- simple
  $c_1 \leq x \leq c_2$
  $x - y \leq c$
- and cheap
  emptiness testing, normal form computing, usual operations
  $\rightarrow O(n^3)$

Which Domain for Disequalities ? (2/2)

DBM is a good candidate

- simple

  $c_1 \leq x \leq c_2 \quad + \quad x \neq 0$

  $x - y \leq c \quad + \quad x \neq y$

- and cheap

  emptiness testing, normal form computing, usual operations $\rightarrow O(n^3)$

Other disequalities Why not $x - y \neq c$?

```
x := 0; y := 2
while ( y < 100 and ? )  {
  y := y + 2
}
```

▶ impose an unbounded representation for the constraint set
do not respect our goal (complexity)

Which Domain for Disequalities ? (2/2)

DBM is a good candidate

- simple

  $c_1 \leq x \leq c_2 \quad + \quad x \neq 0$

  $x - y \leq c \quad + \quad x \neq y$

- and cheap

  emptiness testing, normal form computing, usual operations $\rightarrow O(n^3)$

Other disequalities Why not $x - y \neq c$?

```
x := 0; y := 2
while ( y < 100 and ? )  {
  y := y + 2
}
```

$y - x \neq 1$

$y - x \neq 1, y - x \neq 3, \ldots, y - x \neq 99$

▶ impose an unbounded representation for the constraint set do not respect our goal (complexity)

Outline

- Introduction
- Difference-Bound Matrices
  a short reminder
- *disequalities* Difference-Bound Matrices
  definition of the domain
- Application to Program Analysis
- Conclusion

Difference-Bound Matrices *(Dill 89)*

Var: a finite set of variables $\{x_0, x_1, \ldots, x_{n-1}\}$
$\mathcal{V}$: the variables domain, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$
$\overline{\mathcal{V}}$: the extension of $\mathcal{V}$ with $+\infty$

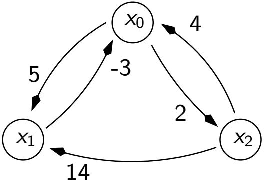
Potential constraints ($c \in \mathcal{V}$)

$x_i - x_j \leq c$

Representations

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \end{cases}$$

$$\begin{array}{c c} & \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} & \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 14 \\ 2 & +\infty & 0 \end{pmatrix} \end{array}$$



- set of constraints
- DBM
- potential graph

Difference-Bound Matrices *(Dill 89)*

Var: a finite set of variables $\{x_0, x_1, \ldots, x_{n-1}\}$
$\mathcal{V}$: the variables domain, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$
$\overline{\mathcal{V}}$: the extension of $\mathcal{V}$ with $+\infty$

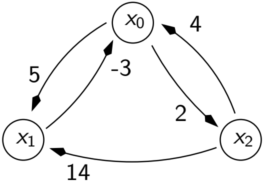
Potential constraints ($c \in \mathcal{V}$)

$x_i - x_j \leq c \mid x_i \leq c \mid -x_i \leq c$

Representations

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \end{cases}$$

$$\begin{array}{cc} & \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} & \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 14 \\ 2 & +\infty & 0 \end{pmatrix} \end{array}$$



- set of constraints
- DBM
- potential graph

Difference-Bound Matrices *(Dill 89)*

Var: a finite set of variables $\{x_0, x_1, ..., x_{n-1}\}$
$\mathcal{V}$: the variables domain, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$
$\overline{\mathcal{V}}$: the extension of $\mathcal{V}$ with $+\infty$

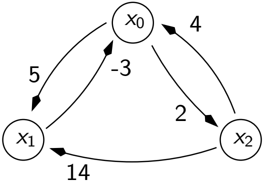
Potential constraints ($c \in \mathcal{V}$)

$$x_i - x_j \leq c \mid x_i - x_0 \leq c \mid x_0 - x_i \leq c \qquad \textit{with } x_0 = 0$$

Representations

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \end{cases}$$

$$\begin{array}{c} \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 14 \\ 2 & +\infty & 0 \end{pmatrix} \end{array}$$



- set of constraints
- DBM
- potential graph

Difference-Bound Matrices *(Dill 89)*

Var: a finite set of variables $\{x_0, x_1, ..., x_{n-1}\}$
$\mathcal{V}$: the variables domain, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$
$\overline{\mathcal{V}}$: the extension of $\mathcal{V}$ with $+\infty$

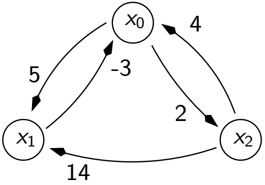
Potential constraints ($c \in \mathcal{V}$)

$x_i - x_j \leq c \mid x_i \leq c \mid -x_i \leq c$

Representations

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \end{cases}$$

$$\begin{array}{cc} & \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} & \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 14 \\ 2 & +\infty & 0 \end{pmatrix} \end{array}$$



- set of constraints
- DBM
- potential graph

Testing Emptiness, Closure

Emptiness Test

- checking for the existence of negative cycles

Closure *(for non-empty DBMs)*

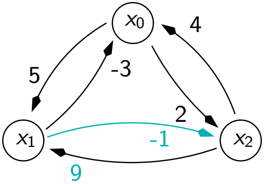
- infering implicit constraints

shortest-path closure is well defined

the closure leads to a normal form

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \end{cases}$$

$$\begin{array}{c} \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 9 \\ 2 & -1 & 0 \end{pmatrix} \end{array}$$



- set of constraints
- *closed* DBM
- potential graph

Outline

- Introduction
- Difference-Bound Matrices

  a short reminder
- *disequalities* Difference-Bound Matrices

  definition of the domain
- Application to Program Analysis
- Conclusion

disequalities Difference-Bound Matrices

Constraints $(c \in \mathcal{V})$

$x_i - x_j \leq c \mid \pm x_i \leq c$

Representations

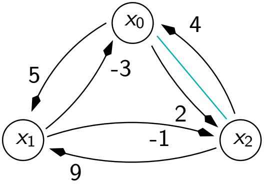
- a *d*DBM is a pair of matrices $(M^{\leq}, M^{\neq})$

$M^{\leq}$ is a classical DBM

$M^{\neq}$ is a symmetric boolean matrix

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \\ x_2 \neq 0 \end{cases}$$

$$\begin{array}{cc} & \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} & \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 9 \\ 2 & -1 & 0 \end{pmatrix}^{\leq} \\ \begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} & \begin{pmatrix} F & F & T \\ F & F & F \\ T & F & F \end{pmatrix}^{\neq} \end{array}$$



- set of constraints
- *d*DBM
- disequal potential graph

disequalities Difference-Bound Matrices

Constraints $(c \in \mathcal{V})$

$x_i - x_j \leq c \mid \pm x_i \leq c \mid x_i - x_j \neq 0$

Representations

- a *d*DBM is a pair of matrices $(M^{\leq}, M^{\neq})$

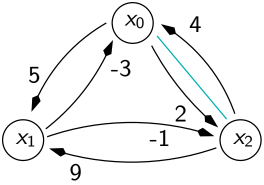
$M^{\leq}$ is a classical DBM

$M^{\neq}$ is a symmetric boolean matrix

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \\ x_2 \neq 0 \end{cases}$$

$$\begin{array}{c} \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 9 \\ 2 & -1 & 0 \end{pmatrix}^{\leq} \end{array}$$

$$\begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{pmatrix} F & F & T \\ F & F & F \\ T & F & F \end{pmatrix}^{\neq}$$



- set of constraints
- *d*DBM
- disequal potential graph

disequalities Difference-Bound Matrices

Constraints $(c \in \mathcal{V})$

$$x_i - x_j \leq c \mid \pm x_i \leq c \mid x_i - x_j \neq 0 \mid x_i \neq 0$$

Representations

- a dDBM is a pair of matrices $(M^{\leq}, M^{\neq})$

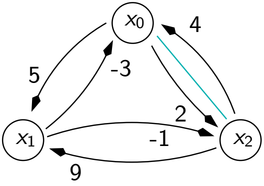
$M^{\leq}$ is a classical DBM

$M^{\neq}$ is a symmetric boolean matrix

$$\left\{ \begin{array}{l} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \\ x_2 \neq 0 \end{array} \right.$$

$$\begin{array}{c} \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 9 \\ 2 & -1 & 0 \end{pmatrix}^{\leq} \end{array}$$

$$\begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{pmatrix} F & F & T \\ F & F & F \\ T & F & F \end{pmatrix}^{\neq}$$



- set of constraints
- dDBM
- disequal potential graph

disequalities Difference-Bound Matrices

Constraints $(c \in \mathcal{V})$

$$x_i - x_j \leq c \mid \pm x_i \leq c \mid x_i - x_j \neq 0 \mid x_i - x_0 \neq 0 \qquad \textit{with } x_0 = 0$$

Representations

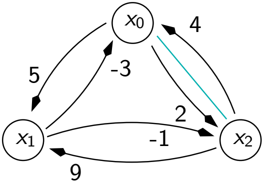
- a dDBM is a pair of matrices $(M^{\leq}, M^{\neq})$

$M^{\leq}$ is a classical DBM

$M^{\neq}$ is a symmetric boolean matrix

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \\ x_2 \neq 0 \end{cases}$$

$$\begin{array}{c} \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 9 \\ 2 & -1 & 0 \end{pmatrix}^{\leq} \\ \begin{pmatrix} F & F & T \\ F & F & F \\ T & F & F \end{pmatrix}^{\neq} \end{array}$$



- set of constraints
- dDBM
- disequal potential graph

disequalities Difference-Bound Matrices

Constraints $(c \in \mathcal{V})$

$$x_i - x_j \leq c \mid \pm x_i \leq c \mid x_i - x_j \neq 0 \mid x_i \neq 0$$

Representations

- a *d*DBM is a pair of matrices $(M^{\leq}, M^{\neq})$

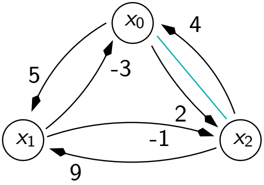
$M^{\leq}$ is a classical DBM

$M^{\neq}$ is a symmetric boolean matrix

$$\begin{cases} 3 \leq x_1 \leq 5 \\ -4 \leq x_2 \leq 2 \\ x_1 - x_2 \leq 14 \\ x_2 \neq 0 \end{cases}$$

$$\begin{array}{c} \\ \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{x}_0 & \mathbf{x}_1 & \mathbf{x}_2 \end{array} \\ \begin{pmatrix} 0 & -3 & 4 \\ 5 & 0 & 9 \\ 2 & -1 & 0 \end{pmatrix}^{\leq} \end{array}$$

$$\begin{array}{c} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{array} \begin{pmatrix} F & F & T \\ F & F & F \\ T & F & F \end{pmatrix}^{\neq}$$



- set of constraints
- *d*DBM
- disequal potential graph

Domain, Order and Normal Form

Domain noted $\mathcal{D}(M)$

- all the possible valuations of the variables represented by the *d*DBM M

Order

- $M \trianglelefteq M' \iff \forall i, j\ M_{ij} \leq M'_{ij}\ \wedge\ {M'}^{\neq}_{ij} \Rightarrow M^{\neq}_{ij}$

"smaller" has *tightest bounds* and *more disequalities*

  - property : $M \trianglelefteq M' \Rightarrow \mathcal{D}(M) \subseteq \mathcal{D}(M')$

Normal form *(for non-empty dDBMs)*

- $\overline{M} = \inf_{\trianglelefteq} \{M' \mid \mathcal{D}(M') = \mathcal{D}(M)\}$

Outline

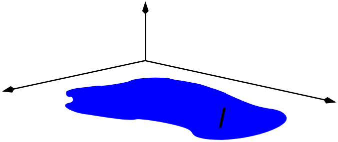
- Introduction
- Difference-Bound Matrices
  a short reminder
- *disequalities* Difference-Bound Matrices
  definition of the domain
  - Dense Case
    where $\mathcal{V} = \mathbb{Q}$, $\mathbb{R}$. Testing emptiness, closure
  - Arithmetic Case
    where $\mathcal{V} = \mathbb{Z}$. Testing emptiness, closure
- Application to Program Analysis
- Conclusion

Dense Case | Testing Emptiness

Independence of disequalities

Theorem (Lassez *et al.* 1992)

Let I be a system of linear inequalities, and D be a finite set of linear disequalities. Then the conjunction of I and D is feasible if and only if, for each single disequality $d \in D$, the conjunction of I and $\{d\}$ is feasible.



Emptiness test

- check there is no pair of variables given equal and disequal

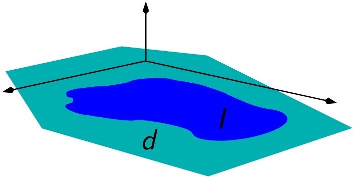
$\rightarrow O(n^2)$ on the closed dDBM

Dense Case | Testing Emptiness

Independence of disequalities

Theorem (Lassez *et al.* 1992)

Let I be a system of linear inequalities, and D be a finite set of linear disequalities. Then the conjunction of I and D is feasible if and only if, for each single disequality $d \in D$, the conjunction of I and $\{d\}$ is feasible.



Emptiness test

- check there is no pair of variables given equal and disequal

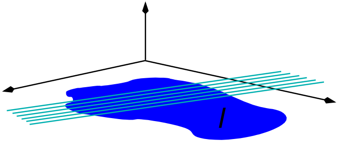
$\rightarrow O(n^2)$ on the closed dDBM

Dense Case | Testing Emptiness

Independence of disequalities

Theorem (Lassez *et al.* 1992)

Let I be a system of linear inequalities, and D be a finite set of linear disequalities. Then the conjunction of I and D is feasible if and only if, for each single disequality $d \in D$, the conjunction of I and $\{d\}$ is feasible.



Emptiness test

- check there is no pair of variables given equal and disequal

$\rightarrow O(n^2)$ on the closed dDBM

Dense Case | Closure (1/2)

Inequalities

- independence always hold: apply DBM closure

Disequalities

- deduction rules
  - (1) $(x \leq y + c \wedge c < 0) \Rightarrow x \neq y$
  - (2) $(x = y \wedge x \neq z) \Rightarrow y \neq z$
  - (3) $(x \leq y \leq z \wedge x \neq y) \Rightarrow x \neq z$

Closure algorithm *(first stage)*

- close $M^{\leq}$
- apply rules (1) and (2)

$\rightarrow O(n^3)$

Dense Case | Closure (2/2)

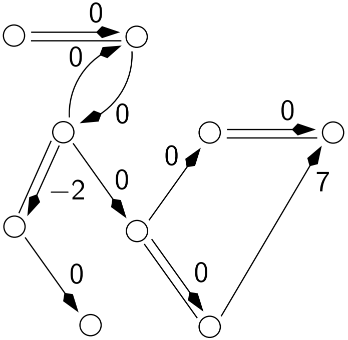
Rule (3)

a "disequal potential graph view" of the rule:

Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

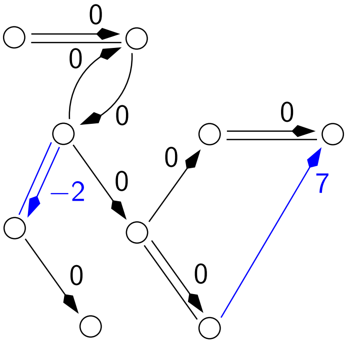
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\rightarrow O(n^3)$

Closure algorithm *(second stage)*

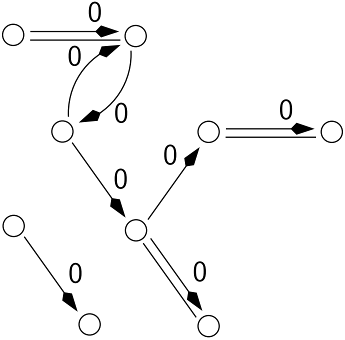


Dense Case] Closure (2/2)

Rule (3)

a kind of transitive closure $\longrightarrow O(n^3)$

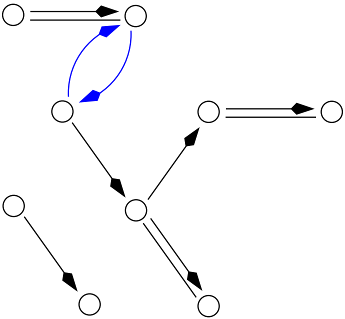
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

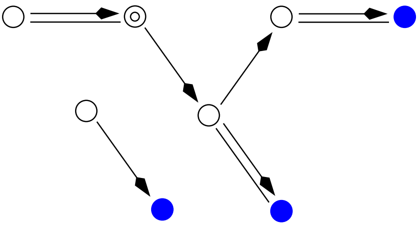
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

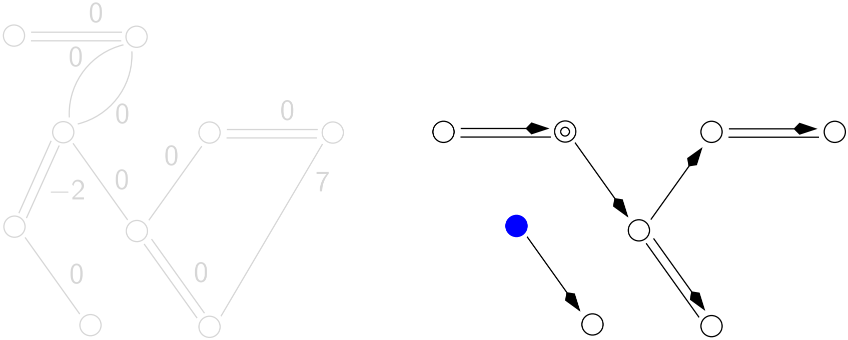
Closure algorithm *(second stage)*



Dense Case] Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

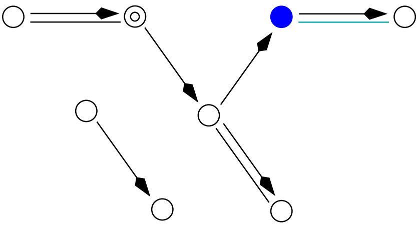
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

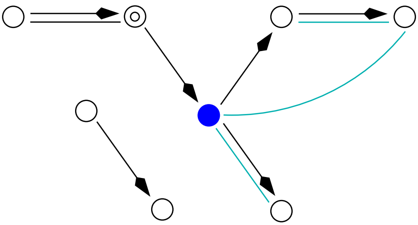
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

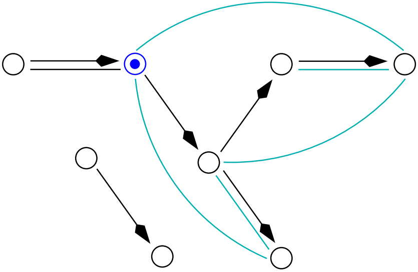
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

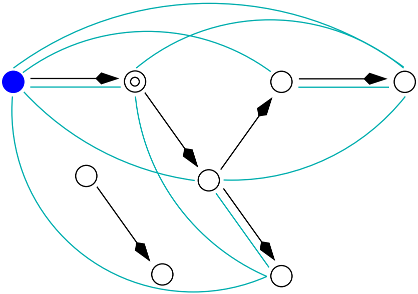
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

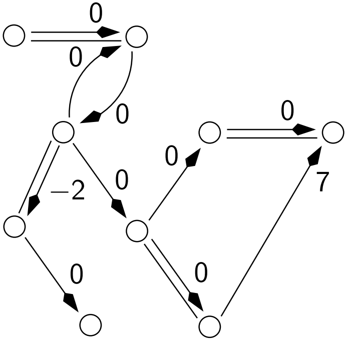
Closure algorithm *(second stage)*

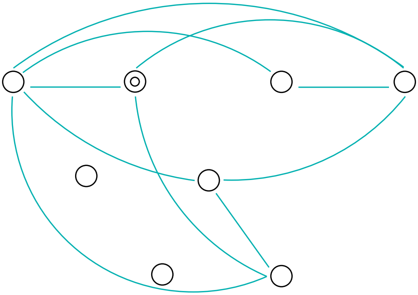


Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

Closure algorithm *(second stage)*



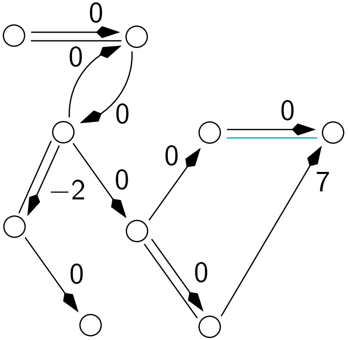


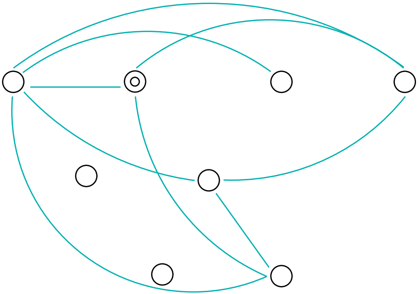
Dense Case | Closure (2/2)

Rule (3)

a kind of transitive closure $\longrightarrow O(n^3)$

Closure algorithm *(second stage)*

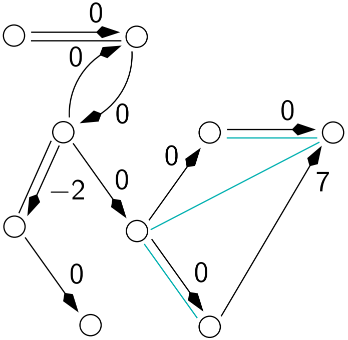


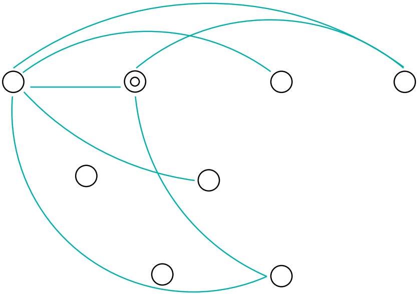


Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

Closure algorithm *(second stage)*

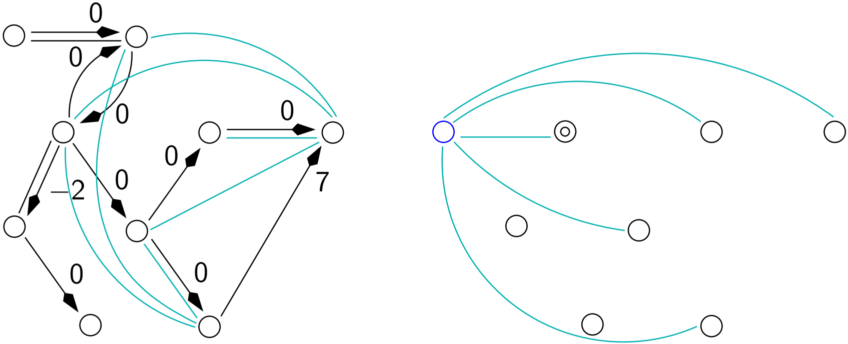




Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure → $O(n^3)$

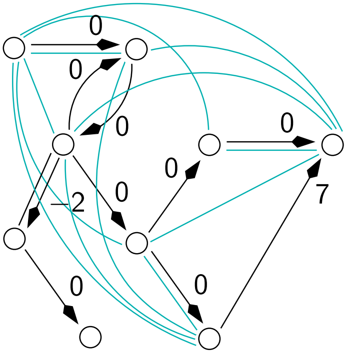
Closure algorithm *(second stage)*



Dense Case | Closure (2/2)

Rule (3)
a kind of transitive closure $\longrightarrow O(n^3)$

Closure algorithm *(second stage)*



Outline

- Introduction
- Difference-Bound Matrices

  a short reminder
- *disequalities* Difference-Bound Matrices

  definition of the domain
  - Dense Case

    where $\mathcal{V} = \mathbb{Q}, \mathbb{R}$. Testing emptiness, closure
  - Arithmetic Case

    where $\mathcal{V} = \mathbb{Z}$. Testing emptiness, closure
- Application to Program Analysis
- Conclusion

Arithmetic Case | Testing Emptiness

NP-completeness

Theorem (Hunt 1980)

The satisfiability problem of a set of potential constraints in presence of disequations is NP-complete

$$\begin{cases} 1 \leq x_1, x_2, x_3 \leq 2 \\ x_1 \neq x_2 \\ x_1 \neq x_3 \\ x_2 \neq x_3 \end{cases}$$

Emptiness test

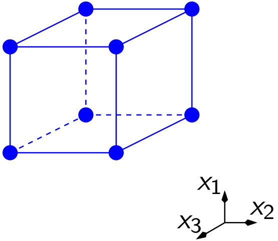
- brute force: consider for each disequality cases $x - y \leq -1$ and $x - y \geq 1$
  - leads to 2^d emptiness tests on DBMs
- dense approximation is safe !
- in the middle: heuristics

Arithmetic Case | Testing Emptiness

NP-completeness

Theorem (Hunt 1980)

The satisfiability problem of a set of potential constraints in presence of disequations is NP-complete



Emptiness test

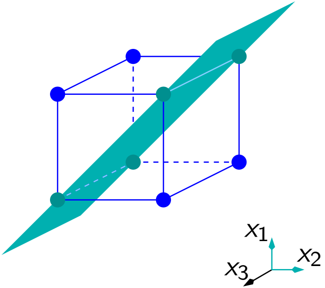
- brute force: consider for each disequality cases $x - y \leq -1$ and $x - y \geq 1$
  - leads to 2^d emptiness tests on DBMs
- dense approximation is safe !
- in the middle: heuristics

Arithmetic Case | Testing Emptiness

NP-completeness

Theorem (Hunt 1980)

The satisfiability problem of a set of potential constraints in presence of disequations is NP-complete



Emptiness test

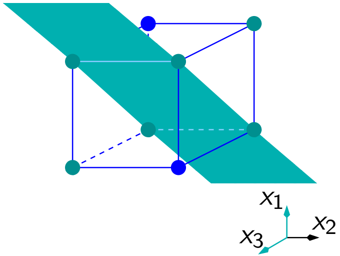
- brute force: consider for each disequality cases $x - y \leq -1$ and $x - y \geq 1$
  - ▶ leads to 2^d emptiness tests on DBMs
- dense approximation is safe !
- in the middle: heuristics

Arithmetic Case | Testing Emptiness

NP-completeness

Theorem (Hunt 1980)

The satisfiability problem of a set of potential constraints in presence of disequations is NP-complete



Emptiness test

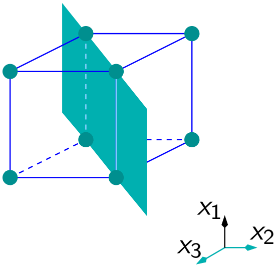
- brute force: consider for each disequality cases $x - y \leq -1$ and $x - y \geq 1$
  - leads to 2^d emptiness tests on DBMs
- dense approximation is safe !
- in the middle: heuristics

Arithmetic Case | Testing Emptiness

NP-completeness

Theorem (Hunt 1980)

The satisfiability problem of a set of potential constraints in presence of disequations is NP-complete



Emptiness test

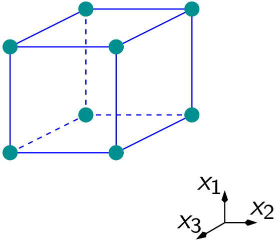
- brute force: consider for each disequality cases $x - y \leq -1$ and $x - y \geq 1$
  - leads to 2^d emptiness tests on DBMs
- dense approximation is safe !
- in the middle: heuristics

Arithmetic Case | Testing Emptiness

NP-completeness

Theorem (Hunt 1980)

The satisfiability problem of a set of potential constraints in presence of disequations is NP-complete



Emptiness test

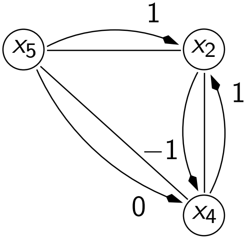
- brute force: consider for each disequality cases $x - y \leq -1$ and $x - y \geq 1$
  - leads to 2^d emptiness tests on DBMs
- dense approximation is safe !
- in the middle: heuristics

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

- an iterative process



iterations of

- shortest-path closure + rules (1)(2)

narrowing

Closure algorithm

- iterations include the application of rule (3)

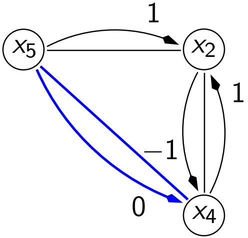
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

▶ an iterative process



iterations of
shortest-path closure + rules (1)(2)

▶ narrowing

Closure algorithm

- iterations include the application of rule (3)

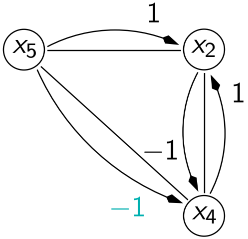
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

▶ an iterative process



iterations of
shortest-path closure + rules (1)(2)
▶ narrowing

Closure algorithm

- iterations include the application of rule (3)

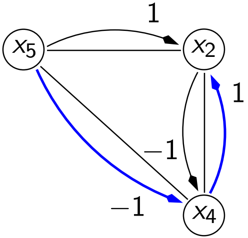
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

- an iterative process



iterations of

- shortest-path closure + rules (1)(2)

narrowing

Closure algorithm

- iterations include the application of rule (3)

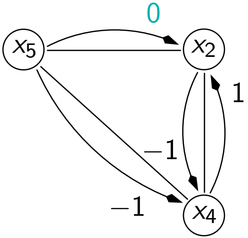
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

- an iterative process



iterations of

- shortest-path closure + rules (1)(2)

narrowing

Closure algorithm

- iterations include the application of rule (3)

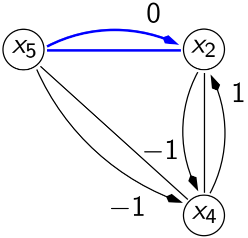
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

▶ an iterative process



iterations of
shortest-path closure + rules (1)(2)

▶ narrowing

Closure algorithm

- iterations include the application of rule (3)

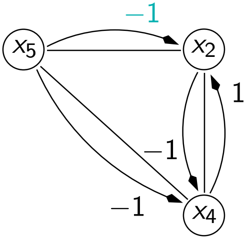
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

▶ an iterative process



iterations of
shortest-path closure + rules (1)(2)

▶ narrowing

Closure algorithm

- iterations include the application of rule (3)

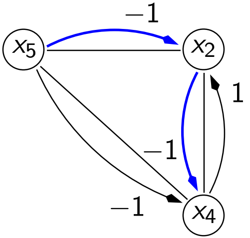
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

▶ an iterative process



iterations of

▶ shortest-path closure + rules (1)(2)

narrowing

Closure algorithm

- iterations include the application of rule (3)

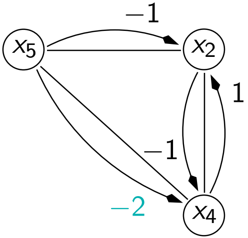
$\rightarrow O(n^5)$

Arithmetic Case | Closure

Narrowing of the bounds

$(x - y \leq 0 \ \wedge \ x \neq y) \Rightarrow (x - y \leq -1)$

▶ an iterative process



iterations of

▶ shortest-path closure + rules (1)(2)

narrowing

Closure algorithm

- iterations include the application of rule (3)

$\rightarrow O(n^5)$

Outline

- Introduction
- Difference-Bound Matrices

  a short reminder
- *disequalities* Difference-Bound Matrices

  definition of the domain
  - Dense Case

    where $\mathcal{V} = \mathbb{Q}, \mathbb{R}$. Testing emptiness, closure
  - Arithmetic Case

    where $\mathcal{V} = \mathbb{Z}$. Testing emptiness, closure
- Application to Program Analysis
- Conclusion

Lattice of *d*DBMs, Operators

Lattice

with classical lattice operators + a widening

- $\sqcup = (\max, \vee)$, $\sqcap = (\min, \wedge)$

Other operators

existential quantification and projection

post-condition of an assignment

abstraction of conditions

```
x := x + w
```

Implementation

- a prototype has been implemented and simple ad hoc examples analysed.

Lattice of *d*DBMs, Operators

Lattice

with classical lattice operators + a widening

- $\sqcup = (\max, \vee)$, $\sqcap = (\min, \wedge)$

Other operators

existential quantification and projection

post-condition of an assignment

abstraction of conditions

$\quad x = y,\ w \neq 0$

```
x := x + w
```

$x \neq y$

Implementation

- a prototype has been implemented and simple ad hoc examples analysed.

Conclusion

Achievements

▶ a new numerical abstract domain dealing with both potential constraints and disequalities

- complexity is $O(n^3)$ when variables take values in a dense set
- in the arithmetic case, apart from the emptiness problem which is exponential (may be aprroximate), operations are in $O(n^5)$

Ongoing work

- implementation of dDBMs in the APRON interface
- extend the work to octagons (expressing $x \neq -y$)
- propose a domain expressing disequalities of the form $x - y \neq c$