CS 433 Automated Reasoning 2022

Lecture 18: Difference and Octagonal logic

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2022-10-13

Topic 18.1

Difference logic

Logic vs. theory

- theory = FOL + axioms
- logic = theory+syntactic restrictions

Example 18.1

LRA is a theory
QF_LRA is a logic that has only quantifier free LRA formulas

Difference Logic

Difference Logic over reals(QF_RDL): Boolean combinations of atoms of the form $x - y \leq b$, where x and y are real variables and b is a real constant.

Difference Logic over integers(QF_IDL): Boolean combinations of atoms of the form $x - y \leq b$, where x and y are integer variables and b is an integer constant.

Widely used in analysis of timed systems for comparing clocks.

Commentary: Lecture is based on: The octagon abstract domain.Antoine Miné. In Higher-Order and Symbolic Computation (HOSC), 19(1), 31-100, 2006. Springer.

Difference Graph

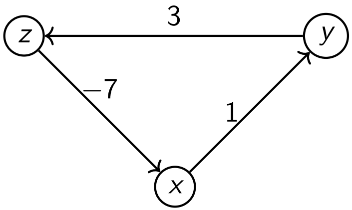
We may view $x - y \leq b$ as a weighted directed edge between nodes x and y with weight b in a directed graph, which is called difference graph.

Theorem 18.1

A conjunction of difference inequalities is unsatisfiable iff the corresponding difference graph has negative cycles.

Example 18.2

$$x - y \leq 1 \wedge y - z \leq 3 \wedge z - x \leq -7$$



Difference bound matrix

Another view of difference graph.

Definition 18.1

Let F be conjunction of difference inequalities over rational variables $\{x_1, \dots, x_n\}$. The difference bound matrix(DBM) A is defined as follows.

$$A_{ij} = \begin{cases} 0 & i = j \\ b & x_i - x_j \leq b \in F \\ \infty & otherwise \end{cases}$$

Let $F[A] \triangleq \bigwedge_{i,j \in 1..n} x_i - x_j \leq A_{ij}$.

Let $A_{i_0 \dots i_m} \triangleq \sum_{k=1}^{m} A_{i_{k-1} i_k}$.

Example: DBM

Example 18.3

Consider: $x_2 - x_1 \leq 4 \wedge x_1 - x_2 \leq -1 \wedge x_3 - x_1 \leq 3 \wedge x_1 - x_3 \leq -1 \wedge x_2 - x_3 \leq 1$

Constraints has three variables x_1, x_2, *and* x_3.

The corresponding DBM is

$$\begin{bmatrix} 0 & -1 & -1 \\ 4 & 0 & \_\_\_ \\ 3 & \_\_\_ & 0 \end{bmatrix}$$

Exercise 18.1

Fill the blanks

Shortest path closure and satisfiability

Definition 18.2

The *shortest path closure* $A^\bullet$ *of* A *is defined as follows.*

$$(A^\bullet)_{ij} = \min_{i=i_0,i_1,\ldots,i_m=j \text{ and } m\leq n} A_{i_0\ldots i_m}$$

Theorem 18.2

F *is unsatisfiable iff* $\exists i \in 1..n.\ A^\bullet_{ii} < 0$

Proof.

($\Leftarrow$) If RHS holds, trivially unsat.(why?)

($\Rightarrow$) if LHS holds,

due to Farkas lemma, $0 \leq -k$ is a positive integral linear combination of difference inequalities for some $k > 0$. ...

Shortest path closure: there is a negative loop

Proof(contd.)

claim: there is $A_{i_0,.....,i_m} < 0$ and $i_0 = i_m$.

Let $G = (\{x_1, ..., x_n\}, E)$ be a weighted directed graph such that

- $E = \{\underbrace{(x_i, b, x_j), .., (x_i, b, x_j)}_{\lambda \text{ times}} | x_i - x_j \leq b$ has λ coefficient in the proof $\}$

Since each x_i cancels out in the proof, x_i has equal in and out degree in G.

Therefore, each SCC of G has a Eulerian cycle (full traversal without repeating an edge). (why?)

The sum along the cycle must be negative.(why?) ...

Exercise 18.2

Prove that if a directed graph is a strongly connected component(scc), and each node has equal in and out degree, there is a Eulerian cycle in the graph.

Shortest path closure(contd.)

Proof.

claim: Shortest loop with negative sum has no repeated node

For $0 < p < q < m$, lets suppose $i_0 = i_m$ and $i_p = i_q$ in $A_{i_0,....,i_m}$.

$$\begin{tikzcd} x_{i_0} \arrow[r, bend left, "A_{i_0..i_p}"] & x_{i_p} \arrow[l, bend left, "A_{i_q..i_m}"] \arrow[loop right, "A_{i_p,...,i_q}"] \end{tikzcd}$$

Since $A_{i_0..i_m} = \underbrace{A_{i_p..i_q}}_{\text{loop}} + \underbrace{(A_{i_q..i_m} + A_{i_m..i_p})}_{\text{loop}}$, one of the two sub-loops is negative.

Therefore, shorter loops exist with negative sum. Therefore, there is a negative simple loop. □

Exercise 18.3

If F is sat, $A^{\bullet}_{ij} \leq A^{\bullet}_{ikj}$.

Floyd-Warshall Algorithm for shortest closure

We can compute $A^\bullet$ using the following iterations generating $A^0, \dots, A^n$.

$$
\begin{aligned}
A^0 &= A \\
A^k_{ij} &= \min(A^{k-1}_{ij}, A^{k-1}_{ikj})
\end{aligned}
$$

Theorem 18.3

$A^\bullet = A^n$

Exercise 18.4

a. *Prove Theorem 18.3.* *Hint: Inductively show each loop-free path is considered*

b. *Extend the above algorithm to support strict inequalities*

c. *Does the above algorithm also work for $\mathbb{Z}$?*

Example: DBM

Example 18.4

Consider DBM:

$$A^0 = \begin{bmatrix} 0 & -1 & -1 \\ 4 & 0 & 1 \\ 3 & \infty & 0 \end{bmatrix}$$

First iteration: $A^1 = min(A^0, \begin{bmatrix} A^0_{111} & A^0_{112} & A^0_{113} \\ A^0_{211} & A^0_{212} & A^0_{213} \\ A^0_{311} & A^0_{312} & A^0_{313} \end{bmatrix}) = min(A^0, \begin{bmatrix} 0 & -1 & -1 \\ 4 & 3 & 3 \\ 3 & 2 & 2 \end{bmatrix}) = \begin{bmatrix} 0 & -1 & -1 \\ 4 & 0 & 1 \\ 3 & 2 & 0 \end{bmatrix}$

Second iteration: $A^2 = min(A^1, \begin{bmatrix} A^1_{121} & A^1_{122} & A^1_{123} \\ A^1_{221} & A^1_{222} & A^1_{223} \\ A^1_{321} & A^1_{322} & A^1_{323} \end{bmatrix}) = min(A^1, \begin{bmatrix} 3 & -1 & 0 \\ 4 & 0 & 1 \\ 6 & 2 & 2 \end{bmatrix}) = \begin{bmatrix} 0 & -1 & -1 \\ 4 & 0 & 1 \\ 3 & 2 & 0 \end{bmatrix}$

Third iteration: $A^3 = min(A^2, \begin{bmatrix} A^1_{131} & A^1_{132} & A^1_{133} \\ A^1_{231} & A^1_{232} & A^1_{233} \\ A^1_{331} & A^1_{332} & A^1_{333} \end{bmatrix}) = min(A^2, \begin{bmatrix} 2 & 1 & -1 \\ 4 & 3 & 1 \\ 3 & 2 & 0 \end{bmatrix}) = \begin{bmatrix} 0 & -1 & -1 \\ 4 & 0 & 1 \\ 3 & 2 & 0 \end{bmatrix}$

Incremental difference logic for SMT solvers

DBMs are not good for SMT solvers, where we need pop and unsat core.

SMT solvers implements difference logic constraints using difference graph.
Maintains a current assignment.

- push($x_1 - x_2 \leq b$):
  1. Adds corresponding edge from the graph
  2. If current assignment is feasible with new atom, exit
  3. If not, adjust assignments until it saturates z3:src/smt/diff_logic.h:make_feasible

- Pop($x_1 - x_2 \leq b$):
  - Remove the corresponding edge without worry

- Unsat core
  - If assignment fails to adjust, we can find the set of edges that required the adjustment
  - the edges form negative cycle are reported as unsat core

Topic 18.2

Difference logic : canonical representation

Canonical representation

Sometimes a class for formulas have canonical representation.

Definition 18.3

A set of objects R canonically represents a class of formulas Σ if for each $F, F' \in \Sigma$ if $F \equiv F'$ and $o \in R$ represents F then o represents F'.

Tightness

Definition 18.4

A is tight if for all i and j

- *if $A_{ij} < \infty$, $\exists v \models F[A].\ v_i - v_j = A_{ij}$*
- *if $A_{ij} = \infty$, $\forall m < \infty.\ \exists v \models F[A].\ v_i - v_j > m$*

Theorem 18.4

If F is sat, $A^\bullet$ is tight.

Proof.

Suppose there is a better bound $b < A^\bullet_{ij}$ exists such that $F[A^\bullet] \Rightarrow x_i - x_j \leq b$.

Like the last proof, there is a path $i_0..i_m$ such that $A_{i_0..i_m} \leq b$, $i_0 = i$ and $i_m = j$.(why?)

If $i_0..i_m$ has a loop then the sum along the loop must be positive.
Therefore, there must be a shorter path from i to j with smaller sum.(why?)
Therefore, a loopfree path from i to j exists with sum less than b. Therefore, $A^\bullet$ is tight $\square$

Implication checking and canonical form

Theorem 18.5

The set of shortest path closed DBMs canonically represents difference logic formulas.

Exercise 18.5

Give an efficient method of checking equisatisfiablity and implication using DBMs.

Topic 18.3

Octagonal constraints

Octagonal constraints

Definition 18.5

Octagonal constraints are boolean combinations of inequalities of the form $\pm x \pm y \leq b$ or $\pm x \leq b$ where x and y are $\mathbb{Z}/\mathbb{Q}$ variables and b is an $\mathbb{Z}/\mathbb{Q}$ constant.

We can always translate octagonal constraints into equisatisfiable difference constraints.

Octagon to difference logic encoding (contd.)

Consider conjunction of octagonal atoms F over variables $V = \{x_1, \dots, x_n\}$.

We construct a difference logic formula F' over variables $V' = \{x'_1, \dots, x'_{2n}\}$.

In the encoding, x'_{2i-1} represents x_i and x'_{2i} represents $-x_i$.

Octagon to difference logic encoding

F' is constructed as follows

$$
\begin{array}{rrcll}
F \ni & x_i \leq b & \rightsquigarrow & x'_{2i-1} - x'_{2i} \leq 2b & \in F' \\
F \ni & -x_i \leq b & \rightsquigarrow & x'_{2i} - x'_{2i-1} \leq 2b & \in F' \\
F \ni & x_i - x_j \leq b & \rightsquigarrow & x'_{2i-1} - x'_{2j-1} \leq b,\ x'_{2j} - x'_{2i} \leq b & \in F' \\
F \ni & x_i + x_j \leq b & \rightsquigarrow & x'_{2i-1} - x'_{2j} \leq b, \quad x'_{2j-1} - x'_{2i} \leq b & \in F' \\
F \ni & -x_i - x_j \leq b & \rightsquigarrow & x'_{2i} - x'_{2j-1} \leq b, \quad x'_{2j} - x'_{2i-1} \leq b & \in F'
\end{array}
$$

Theorem 18.6

If F is over $\mathbb{Q}$ then

- *If $(v_1, \dots, v_n) \models F$ then $(v_1, -v_1, \dots, v_n, -v_n) \models F'$*
- *If $(v_1, v_2, \dots, v_{2n-1}, v_{2n}) \models F'$ then $(\frac{(v_1 - v_2)}{2}, \dots, \frac{(v_{2n-1} - v_{2n})}{2}) \models F$*

Exercise 18.6

a. Prove the above. *b. Give an example over $\mathbb{Z}$ when Theorem 18.6 fails*

Example: octagonal DBM

Definition 18.6

The DBM corresponding to F' are called octagonal DBMs(ODBMs).

Exercise 18.7

Consider: $x_1 + x_2 \leq 4 \wedge x_2 - x_1 \leq 5 \wedge x_1 - x_2 \leq 3 \wedge -x_1 - x_2 \leq 1 \wedge x_2 \leq 2 \wedge -x_2 \leq 7$

Corresponding ODBM

$$\begin{bmatrix} 0 & \infty & 3 & 4 \\ \infty & 0 & 1 & 5 \\ 5 & 4 & 0 & 4 \\ 1 & 3 & 14 & 0 \end{bmatrix}$$

$x_1 + x_2 \leq 4 \rightsquigarrow x_1 - x_4 \leq 4, x_3 - x_2 \leq 4$

$x_2 - x_1 \leq 5 \rightsquigarrow x_3 - x_1 \leq 5, x_2 - x_4 \leq 5$

$x_1 - x_2 \leq 3 \rightsquigarrow x_1 - x_3 \leq 3, x_4 - x_2 \leq 3$

$-x_1 - x_2 \leq 1 \rightsquigarrow x_1 - x_4 \leq 1, x_3 - x_2 \leq 1$

$x_2 \leq 2 \rightsquigarrow x_3 - x_4 \leq 4$

$-x_2 \leq 7 \rightsquigarrow x_3 - x_4 \leq 14$

Relating indices and coherence

Let $\overline{2k} \triangleq 2k-1$ and $\overline{2k-1} \triangleq 2k$

Example 18.5

$\bar{1}\bar{1} = 22 \quad \bar{2}\bar{1} = 12 \qquad \bar{2}\bar{2} = 11$

Exercise 18.8

- $\bar{3}\bar{1} =$
- $\bar{4}\bar{2} =$
- $\bar{3}\bar{2} =$
- $\bar{1}\bar{1} =$

Relating indices and coherence II

Consider the following DBM due to 2 variable octagonal constraints.

$$\begin{bmatrix} 0 & \infty & 3 & 4 \\ \infty & 0 & 1 & 5 \\ 5 & 4 & 0 & 4 \\ 1 & 3 & 14 & 0 \end{bmatrix}$$

Cells with matching colors are pairs $(ij, \overline{ji})$.

Definition 18.7

A DBM A is coherent if $\forall i, j.\ A_{ij} = A_{\overline{ji}}$.

Unsatisfiability

For $\mathbb{Q}$, any method of checking unsat of difference constraints will work on ODBMs.

Let A be ODBM of F. $A^\bullet$ will let us know in $2n$ steps if F is sat.

For $\mathbb{Z}$, we may need to interpret ODBMs differently.
We will cover this shortly.

Topic 18.4

Octagonal constraints : canonical form

Implication checking and canonical form

Floyd-Warshall Algorithm does not obtain canonical form for ODBMs.

$x'_k = -x'_{\bar{k}}$ is not needed for satisfiablity check. Consequently, $A^\bullet$ is not canonical over $\mathbb{Q}$.

We need to tighten the bounds that may be proven due to the above equalities.

Exercise 18.9

Give an example such that $A^\bullet$ is not tight for octagonal constraints.

Canonical closure for octagonal constraints

Let us define closure property for ODBMs.

Definition 18.8

For a ODBM A, let $F[A]$ define the corresponding formula over original variables.

Definition 18.9

For both $\mathbb{Z}$ and $\mathbb{Q}$, an ODBM A is tight if for all i and j

- *if $A_{ij} < \infty$ then $\exists v \models F[A].\ v'_i - v'_j = A_{ij}$ and*
- *if $A_{ij} = \infty$ then $\forall m < \infty.\ \exists v \models F[A].\ v'_i - v'_j > m$,*

where $v'_{2k-1} \triangleq v_k$ and $v'_{2k} \triangleq -v_k$

Theorem 18.7

If A is tight then A is a canonical representation of $F[A]$

$\mathbb{Q}$ tightness condition

Theorem 18.8

Let us suppose $F[A]$ is sat.
If $\forall i, j, k,\ A_{ij} \leq A_{ikj}$ and $A_{ij} \leq (A_{i\bar{i}} + A_{\bar{j}j})/2$ then A is tight

Proof.

Consider cell ij in A s.t. $i \neq j$.(otherwise trivial)
Suppose A_{ij} is finite.
Let $A' = A[ji \mapsto -A_{ij}, \overline{ij} \mapsto -A_{ij}]$

claim: $v \models F[A]$ and $v'_i - v'_j = A_{ij}$ iff $v \models F[A']$
Forward direction easily holds.(why?)
Since A has no negative cycles, $A_{ij} + A_{ji} \geq 0$. So, $A_{ji} \geq -A_{ij}$. So, $A_{ji} \geq A'_{ji}$. Therefore, A is pointwise greater than A'. Therefore, $F[A'] \Rightarrow F[A]$.
Since $A'_{ij} = -A'_{ji}$, if $v \models F[A']$ then $v'_i - v'_j = A_{ij}$. Backward direction holds. ...

$\mathbb{Q}$ tightness condition(contd.)

Proof(contd.)

Now we are only left to show the following.

claim: $F[A']$ is sat, which is there are no negative cycles in A'

A' can have negative cycles only if ji or $\overline{ij}$ occur in the cycle.(why?)

Wlog, we assume only ji occurs in a negative cycle $i = i_0..i_m = j$

Therefore, $A'_{ji} + \sum_{l \in 1..m} A'_{i_{(l-1)}i_l} < 0$. Therefore, $-A_{ij} + \sum_{l \in 1..m} A_{i_{(l-1)}i_l} < 0$.

Therefore, $\sum_{l \in 1..m} A_{i_{(l-1)}i_l} < A_{ij}$. Contradiction.

One more case to consider

Assume both ji and $\overline{ij}$ occur in a negative cycle $i = i_0..i_m i'_0..i_{m'} = j$, where $i_m = \bar{i}$ and $\bar{j} = i'_0$.

Therefore, $A'_{ji} + A'_{\bar{i}\bar{j}} + \sum_{l \in 1..m} A'_{i_{l-1}i_l} + \sum_{l \in 1..m'} A'_{i'_{l-1}i'_l} < 0$.

Therefore, $-2A_{ij} + \sum_{l \in 1..m} A'_{i_{l-1}i_l} + \sum_{l \in 1..m'} A'_{i'_{l-1}i'_l} < 0$.

Therefore, $-2A_{ij} + A_{i\bar{i}} + A_{j\bar{j}} < 0$. Contradiction. □

Exercise 18.10

a. Prove the $A_{ij} = \infty$ case. *b. Does converse of the theorem hold?*

Computing canonical closure for octagonal constraints

Due to the previous theorem and desire of efficient computation, let us redefine $A^\bullet$ for ODBMs.

Definition 18.10

We compute $A^\bullet$ using the following iterations generating $A^0, \dots, A^{2n} = A^\bullet$. Let $o = 2k - 1$ for some $k \in 1..n$.

$$
\begin{aligned}
A^0 &= A \\
(A^{o+1})_{ij} &= \min\left(A^o_{ij}, \frac{A^o_{i\bar{i}} + A^o_{\bar{j}j}}{2}\right) && \text{(odd rule)} \\
(A^o)_{ij} &= \min\left(A^{o-1}_{ij}, A^{o-1}_{ioj}, A^{o-1}_{i\bar{o}j}, A^{o-1}_{io\bar{o}j}, A^{o-1}_{i\bar{o}oj}\right) && \text{(even rule)}
\end{aligned}
$$

In the even rule, three new paths are considered to exploit the structure of ODBMs.

We will prove that $A^\bullet$ is tight in post lecture slides.

Even rule intuition

In octagon formulas, x_k may insert itself between $x_{\lceil i/2 \rceil}$ and $x_{\lceil j/2 \rceil}$ in the following four ways.

1. $\pm x_{\lceil i/2 \rceil} - x_k \leq A_{io}$ and $x_k \pm x_{\lceil j/2 \rceil} \leq A_{oj}$ Update using $A_{io} + A_{oj}$
2. $\pm x_{\lceil i/2 \rceil} + x_k \leq A_{i\bar{o}}$ and $-x_k \pm x_{\lceil j/2 \rceil} \leq A_{\bar{o}j}$ Update using $A_{i\bar{o}} + A_{\bar{o}j}$
3. $\pm x_{\lceil i/2 \rceil} + x_k \leq A_{i\bar{o}}$, $x_k \pm x_{\lceil j/2 \rceil} \leq A_{oj}$, and $-x_k \leq A_{\bar{o}o}/2$ Update using $A_{i\bar{o}} + A_{\bar{o}o} + A_{oj}$
4. $\pm x_{\lceil i/2 \rceil} - x_k \leq A_{io}$, $-x_k \pm x_{\lceil j/2 \rceil} \leq A_{\bar{o}j}$, and $x_k \leq A_{o\bar{o}}/2$ Update using $A_{io} + A_{o\bar{o}} + A_{\bar{o}j}$

The above cases are considered in the four paths in the definition 18.10.

Example: canonical closure of ODBM

Example 18.6

Consider:

$$\begin{bmatrix} 0 & \infty & 3 & 4 \\ \infty & 0 & 1 & 5 \\ 5 & 4 & 0 & 4 \\ 1 & 3 & 14 & 0 \end{bmatrix}$$

First we apply the even rule $o = 1$:

$A^1_{ij} = A^1_{\bar{j}\bar{i}} = \min(A^0_{ij}, A^0_{i1j}, A^0_{i2j}, A^0_{i12j}, A^0_{i21j})$

$A^1_{12} = A^1_{21} = \min(A^0_{12}, A^0_{112}, A^0_{122}, A^0_{1122}, A^0_{1212}) = min(\infty, \infty, \infty, \infty, \infty) = \infty$

$A^1_{24} = A^1_{13} = min(A^0_{24}, A^0_{214}, A^0_{224}, A^0_{2124}, A^0_{2214}) = min(5, \infty, 5, \infty, \infty) = 5$

$A^1_{34} = A^1_{34} = \min(A^0_{34}, A^0_{314}, A^0_{324}, A^0_{3124}, A^0_{3214}) = min(4, 9, 9, \infty, \infty) = 4$

$A^1_{43} = A^1_{43} = \min(A^0_{43}, A^0_{413}, A^0_{423}, A^0_{4123}, A^0_{4213}) = min(14, 4, 4, \infty, \infty) = 4$

Exercise 18.11

Find the tight ODBM for the following octagonal constraints:

$2 \leq x + y \leq 7 \wedge x \leq 9 \wedge y - x \leq 1 \wedge -y \leq 1$

Octagonal constraints over $\mathbb{Z}$

For $\mathbb{Z}$, we need a stronger property to ensure tightness.

Theorem 18.9

Let A be ODBM interpreted over $\mathbb{Z}$.
if $\forall i, j, k,\ A_{ij} \leq A_{ikj},\ A_{ij} \leq (A_{i\bar{i}} + A_{j\bar{j}})/2$, and $A_{i\bar{i}}$ is even then A is tight.

Exercise 18.12

Prove the above theorem.

Computing canonical closure for octgonal DBMs over $\mathbb{Z}$

In this case, let us present an incremental version of the closure iterations.

Lets suppose A is tight and we add another octagonal atom in A that updates $A_{i_0 j_0}$ and $A_{\bar{j}_0 \bar{i}_0}$.

(Observe: always updated together)

Let A^0 be the updated DBM.

$$(A^1)_{ij} = \min(A^0_{ij}, A^0_{ii_0j_0j}, A^0_{i\bar{j}_0\bar{i}_0j}) \qquad \text{if } i \neq \bar{j}$$

$$(A^1)_{i\bar{i}} = \min(A^0_{i\bar{i}}, A^0_{i\bar{j}_0\bar{i}_0i_0j_0\bar{i}}, A^0_{ii_0j_0\bar{j}_0\bar{i}_0\bar{i}}, 2\lfloor \frac{A^0_{ii_0j_0\bar{i}}}{2} \rfloor)$$

$$(A^2)_{ij} = \min(A^1_{ij}, \frac{A^1_{i\bar{i}} + A^1_{\bar{j}j}}{2})$$

Theorem 18.10

A^2 is tight

Topic 18.5

Problem

Difference logic for integers

Exercise 18.13

Consider a difference logic formula with integer bounds. Show that it has an integer solution if it has a rational solution.

End of Lecture 18

Topic 18.6

Post lecture proofs

Tightness of $A^\bullet$

Theorem 18.11
$A^\bullet$ (defined in 18.10) is tight.

Proof.
For each i, j, and k, we need to show $A^\bullet_{ij} \leq (A^\bullet_{i\bar{i}} + A^\bullet_{j\bar{j}})/2$ and $A^\bullet_{ij} \leq A^\bullet_{ikj}$.

claim: For $k > 0$, $A^{2k}_{ij} \leq (A^{2k}_{i\bar{i}} + A^{2k}_{j\bar{j}})/2$

Note $A^{2k}_{i\bar{i}} = A^{2k-1}_{i\bar{i}}$.(why?)

By def,

$$(A^{2k})_{ij} \leq \frac{A^{2k-1}_{i\bar{i}} + A^{2k-1}_{j\bar{j}}}{2}.$$

Therefore,

$$(A^{2k})_{ij} \leq \frac{A^{2k}_{i\bar{i}} + A^{2k}_{j\bar{j}}}{2}.$$

...

Tightness of $A^\bullet$(contd.)

Proof(contd.)

We are yet to prove $\forall i, j.\ A^\bullet_{ij} \leq A^\bullet_{ikj}$.

Let $Fact(k, o) \triangleq \forall i, j.\ A^o_{ij} \leq A^o_{ikj} \land A^o_{ij} \leq A^o_{i\bar{k}j}$

So we need to prove $\forall k \in 1..n.\ Fact(2k, 2n)$.

the following three will prove the above by induction:(why?)

1. In odd rules (o is odd), $Fact(k, o) \Rightarrow Fact(k, o + 1)$ (preserve)
2. In even rules (o is even), $Fact(k, o) \Rightarrow Fact(k, o + 1)$ (preserve)
3. After even rules (o is even), $Fact(o, o)$ (establish)

...

Tightness of $A^\bullet$: odd rules preserve the facts

Proof(contd.)

claim: odd rule, if $\forall i,j.\ A^o_{ij} \leq A^o_{ikj} \wedge A^o_{ij} \leq A^o_{i\bar{k}j}$ then $\forall i,j.\ A^{o+1}_{ij} \leq A^{o+1}_{ikj}$.

We have four cases(why?) and denoted them by pairs.

(1,1) $A^{o+1}_{ik} = A^o_{ik}$, $A^{o+1}_{kj} = A^o_{kj}$: $\underbrace{A^{o+1}_{ij} \leq A^o_{ij}}_{\text{odd rule}} \underbrace{\leq A^o_{ikj}}_{\text{lhs}} \underbrace{= A^{o+1}_{ikj}}_{\text{case cond.}}$

(2,1) $A^{o+1}_{ik} = (A^o_{i\bar{i}} + A^o_{k\bar{k}})/2$, $A^{o+1}_{kj} = A^o_{kj}$:

$$\underbrace{A^o_{ij} \leq \frac{A^o_{i\bar{i}} + A^o_{\bar{j}j}}{2}}_{\text{odd rule}} \underbrace{\leq \frac{A^o_{i\bar{i}} + A^o_{\bar{j}kj}}{2}}_{\text{lhs}} \underbrace{\leq \frac{A^o_{i\bar{i}} + A^o_{\bar{j}\bar{k}kj}}{2}}_{\text{lhs}} \underbrace{\leq \frac{A^o_{i\bar{i}} + A^o_{\bar{k}k} + A^o_{\bar{j}\bar{k}} + A^o_{kj}}{2}}_{\text{rewrite}} \underbrace{\leq \frac{A^o_{i\bar{i}} + A^o_{k\bar{k}}}{2} + A^o_{kj}}_{\text{coherence}} \underbrace{= A^{o+1}_{ikj}}_{\text{case cond.}}$$

(2,1) $A^{2k}_{ik} = A^o_{ik}$, $A^{o+1}_{kj} = (A^o_{k\bar{k}} + A^o_{j\bar{j}})/2$ (Symmetric to the last case)

(2,2) $A^{o+1}_{ik} = (A^o_{i\bar{i}} + A^o_{k\bar{k}})/2$ and $A^{o+1}_{kj} = (A^o_{k\bar{k}} + A^o_{j\bar{j}})/2$: (left for exercise) ...

Exercise 18.14

Prove the last case.

Tightness of $A^{\bullet}$: even rules preserve the facts

Proof(contd.)

claim: even rule, if $\forall i,j.\ A^{o-1}_{ij} \leq A^{o-1}_{ikj} \wedge A^{o-1}_{ij} \leq A^{o-1}_{\bar{i}\bar{k}\bar{j}}$ then $\forall i,j.\ A^{o}_{ij} \leq A^{o}_{ikj}$.

Here, we have 25 cases(why?) and denoted them by pairs:

(1,1) $A^{o}_{ik} = A^{o-1}_{ik}, A^{o}_{kj} = A^{o-1}_{kj}$: $\underbrace{A^{o}_{ij} \leq A^{o-1}_{ij}}_{\text{even rule}} \underbrace{\leq A^{o-1}_{ikj}}_{\text{lhs}} \underbrace{= A^{o}_{ikj}}_{\text{case cond.}}$

(2,1) $A^{o}_{ik} = A^{o-1}_{iok}, A^{o}_{kj} = A^{o-1}_{kj}$: $\underbrace{A^{o}_{ij} \leq A^{o-1}_{ioj}}_{\text{even rule}} \underbrace{\leq A^{o-1}_{iokj}}_{\text{lhs}} \underbrace{= A^{o}_{ikj}}_{\text{case cond.}}$.

(4,5) $A^{o}_{ik} = A^{o-1}_{io\bar{o}k}, A^{o}_{kj} = A^{o-1}_{k\bar{o}oj}$: $\underbrace{A^{o}_{ij} \leq A^{o-1}_{ioj}}_{\text{even rule}} \underbrace{\leq A^{o-1}_{ioj} + A^{o-1}_{o\bar{o}o} + A^{o-1}_{\bar{o}k\bar{o}}}_{\text{no negative loops}} \underbrace{\leq A^{o-1}_{io\bar{o}k} + A^{o-1}_{k\bar{o}oj}}_{\text{rewrite}} \underbrace{= A^{o}_{ikj}}_{\text{case cond.}}$

...

Exercise 18.15

Prove cases (1,4), (2,3) and (3,3).

Hint: key proof technique: introduce cycles, introduce k

Tightness of $A^{\bullet}$: even rule establishes the fact

Proof(contd.)

claim: even rule, $\forall i, j.\ A^o_{ij} \leq A^o_{ioj} \wedge A^o_{ij} \leq A^o_{i\bar{o}j}$

We only prove $A^o_{ij} \leq A^o_{ioj}$, the other inequality is symmetric.

Again, we have 25 cases.(why?)

Since there are no negative cycles and $A^o_{oo} = 0$,

$A_{io} = A_{ioo} \leq A_{io\bar{o}o}$ and $i\bar{o}o \leq i\bar{o}oo$.

Therefore, only four cases left to consider.(why?)

(1,1) $A^o_{io} = A^{o-1}_{io}, A^o_{oj} = A^{o-1}_{oj}$: $\underbrace{A^o_{ij} \leq A^{o-1}_{ioj}}_{\text{even rule}} \underbrace{= A^o_{ioj}}_{\text{case cond.}}$

(2,2) $A^o_{io} = A^{o-1}_{i\bar{o}o}, A^o_{oj} = A^{o-1}_{o\bar{o}j}$:

$$\underbrace{A^o_{ij} \leq A^{o-1}_{i\bar{o}j}}_{\text{even rule}} \underbrace{\leq A^{o-1}_{i\bar{o}j} + A^{o-1}_{o\bar{o}o}}_{\text{no negative cycles}} \underbrace{\leq A^{o-1}_{i\bar{o}o} + A^{o-1}_{o\bar{o}j}}_{\text{rewrite}} \underbrace{= A^o_{ioj}}_{\text{case cond.}}$$

$\square$

Exercise 18.16

Prove case (1,2).