Discussion on Octagon

March 20, 2021

1 Draft

Synthesizing an Octagon Predicate p

Definition 1 (Octagon)**.** *Given a set of variables X where all variables in the set belongs to a numerical set $\mathbb{I}$, which can be $\mathbb{Z}, \mathbb{R}$ or $\mathbb{Q}$. We call* octagonal constraint *any constraint of the form $\pm x_i \pm x_j \geq c$ where $c \in \mathbb{I}$ and $x_i, x_j \in X$. An* octagon *is the set of points that satisfies the conjunction of all octagonal constraints.*

Assume the program we consider is affine linear. From the definition of incorrectness logic and the iteration rule, our target is to synthesize a predicate $p(\mathbf{x}, n)$ for a loop program where the update of the loop body can be expressed as $\mathbf{x}' = M\mathbf{x}$, s.t.

$$\models \forall \mathbf{x}.n.(p(\mathbf{x}, n+1) \implies \exists \mathbf{y}.\mathbf{x} = M\mathbf{y} \wedge p(\mathbf{y}, n))$$

After the elimination of the existential quantifier we get:

$$\models \forall \mathbf{x}.n.(p(\mathbf{x}, n+1) \implies p(k_0(\mathbf{x} - \mathbf{c}) + k_1\mathbf{v}_i, n))$$

Example 1. *We first consider the simplest example where $X = \{x, n\}$, i.e. $\mathbf{x}$ only contains one variable. We assume the update of the program is $x' = ax + b$. The octagon is equivalently given by the form:*

$$\begin{aligned} x + y &\geq \mathcal{A}_{x,y} \\ x - y &\geq \mathcal{B}_{x,y} \\ -x + y &\geq \mathcal{C}_{x,y} \\ -x - y &\geq \mathcal{D}_{x,y} \end{aligned}$$

where $x, y \in X$.

For this example, then the constraint system S_1 of $p(\mathbf{x}, n+1)$ can be given as:

$$
\begin{array}{ll}
2x & \geq \mathcal{A}_{x,x} \\
 & 0 \geq \mathcal{B}_{x,x} \\
 & 0 \geq \mathcal{C}_{x,x} \\
-2x & \geq \mathcal{D}_{x,x} \\
x+n & +1 \geq \mathcal{A}_{x,n} \\
x-n & +1 \geq \mathcal{B}_{x,n} \\
-x+n & +1 \geq \mathcal{C}_{x,n} \\
-x-n & +1 \geq \mathcal{D}_{x,n} \\
2n & +2 \geq \mathcal{A}_{n,n} \\
 & 0 \geq \mathcal{B}_{n,n} \\
 & 0 \geq \mathcal{C}_{n,n} \\
-2n & -2 \geq \mathcal{D}_{n,n}
\end{array}
$$

Similarly, from the fact that $\mathbf{y} = [y] = [\frac{1}{a}x - \frac{b}{a}]$, *we can also derive a system* S_2 *for* $p(\mathbf{y}, n)$*:*

$$
\begin{array}{ll}
\frac{2}{a}x & -\frac{2b}{a} \geq \mathcal{A}_{x,x} \\
 & 0 \geq \mathcal{B}_{x,x} \\
 & 0 \geq \mathcal{C}_{x,x} \\
-\frac{2}{a}x & \frac{2b}{a} \geq \mathcal{D}_{x,x} \\
\frac{1}{a}x+n & -\frac{b}{a} \geq \mathcal{A}_{x,n} \\
\frac{1}{a}x-n & -\frac{b}{a} \geq \mathcal{B}_{x,n} \\
-\frac{1}{a}x+n & +\frac{b}{a} \geq \mathcal{C}_{x,n} \\
-\frac{1}{a}x-n & +\frac{b}{a} \geq \mathcal{D}_{x,n} \\
2n & \geq \mathcal{A}_{n,n} \\
 & 0 \geq \mathcal{B}_{n,n} \\
 & 0 \geq \mathcal{C}_{n,n} \\
-2n & \geq \mathcal{D}_{n,n}
\end{array}
$$

Target of the synthesis is to synthesize the unknown parameter $\{\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}\}$ *s.t.* $\models \forall x.n.(S_1 \implies S_2)$.

According to the method in previous SAS'06: