Literature: Esparza: Automata theory, an algorithmic approach
↳ Lecture notes, online (link on webpage), 2010.

Example (Formula in Presburger arithmetic and its solution space):

Consider $\varphi = \exists x : (2x = y \wedge 2y = z)$

Defines

$$Sol(\varphi) = \left\{ {}^{y}_{z}\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}2\\4\end{pmatrix}, \begin{pmatrix}4\\8\end{pmatrix}, \begin{pmatrix}6\\12\end{pmatrix}, \dots \right\} = \left\{ \begin{pmatrix}2n\\4n\end{pmatrix} \mid n \in \mathbb{N} \right\}$$

Example (lsbf):

$$lsbf\left(\begin{pmatrix}3\\10\\0\end{pmatrix}\right) = \begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix}\begin{pmatrix}0\\0\\0\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}\begin{pmatrix}0\\0\\0\end{pmatrix}^*$$

Concerning the form of atomic expressions:

↳ Why can we assume

$$\varphi = \bar{a}\,\bar{x} \leq b \;?$$

↳ Because we allow $\mathbb{Z}$ as coefficients,
every atomic formula can be brought into this form:

$$x \geq y + 4 \;\rightsquigarrow\; -x + y \leq -4$$

Construct DFA A_φ for $L(\varphi)$:

Key idea:

- States of A_φ are integers $q \in \mathbb{Z}$.
- Transitions and final states chosen so that

(Δ) state q accepts encodings of $\bar{c} \in \mathbb{N}^n$ with $\bar{a}\,\bar{c} \leq q$.

Transition relation:

Consider $q \in \mathbb{Z}$ and $\overline{bit} \in \{0,1\}^n$.
What should be the target state q' with $q \xrightarrow{\overline{bit}} q'$?
Note that

$w' \in (\{0,1\}^n)^*$ is accepted from q'
iff $\overline{bit}.w'$ is accepted from q.

Word w' encodes $\overline{c'} \in \mathbb{N}^n$.

Word $\overline{bit}\, w'$ encodes $2\overline{c'} + \overline{bit}$ (lsbf, shift to right)

Hence

$\overline{c'}$ is accepted from q'

iff $2\overline{c'} + \overline{bit}$ accepted from q.

Hence, to satisfy (Δ), we need

$$\overline{a}\,\overline{c'} \leq q' \quad \text{iff} \quad \overline{a}(2\overline{c'} + \overline{bit}) \leq q$$

Now we can compute q':

$$\overline{a}\,(2\overline{c'} + \overline{bit}) \leq q$$

$$\Leftrightarrow \quad 2\,\overline{a}\,\overline{c'} + \overline{a}\,\overline{bit} \leq q$$

$$\Leftrightarrow \quad \overline{a}\,\overline{c'} \leq \frac{1}{2}(q - \overline{a}\,\overline{bit})$$

$$(\overline{a}\,\overline{c'} \text{ integer}) \Leftrightarrow \quad \overline{a}\,\overline{c'} \leq \left\lfloor \frac{1}{2}(q - \overline{a}\,\overline{bit}) \right\rfloor$$

Define

$$q \xrightarrow{\overline{bit}} q' := \left\lfloor \frac{1}{2}(q - \overline{a}\,\overline{bit}) \right\rfloor$$

<u>Final states:</u>

(in general) A state is final
iff it accepts ϵ
(here) iff it accepts $\overline{0}$.

To satisfy (Δ), need

$$\overline{a}\,\overline{0} \leq q$$

$$\Leftrightarrow \quad 0 \leq q.$$

<u>Initial state:</u>

$b \in \mathbb{Z}$, since we want to accept all $\overline{c} \in \mathbb{N}^n$
with $\overline{a}\,\overline{c} \leq b$

<u>Algorithm:</u>

A_e is defined as a fixed point of a chain of automata

$$A_e^0 \subseteq A_e^1 \subseteq \ldots \subseteq \underbrace{A_e^k = A_e^{k+1}}_{=: A_e}$$

Input: Atomic formula $\varphi = \bar{a}\,\bar{x} \leq b$

Output: DFA $A_\varphi = (\{0,1\}^n, Q, q_0, \rightarrow, Q_F)$

with $L(A_\varphi) = L(\varphi)$

begin: $Q := \emptyset;$

$\rightarrow := \emptyset;$

$Q_F := \emptyset;$

$q_0 := b;$

$W := \{b\};$ // Worklist

while $W \neq \emptyset$ do

pick and delete q from W;

$Q := Q \cup \{q\}$

if $q \geq 0$ then

$Q_F := Q_F \cup \{q\};$

end if

for all $\overline{bit} \in \{0,1\}^n$ do

$j := \left\lfloor \frac{1}{2}(q - \bar{a}\,\overline{bit}) \right\rfloor;$

if $j \notin Q$ then

$W := W \cup \{j\};$

end if

$\rightarrow := \rightarrow \cup \{q \xrightarrow{\overline{bit}} j\}$

end for all

end while

end

Example:

Consider $\varphi = 2x - y \leq 2$

Initial state: $q_0 = 2$.

Compute a few transitions:

$$2 \xrightarrow{\binom{0}{0}} \left\lfloor \tfrac{1}{2}\left(2-(2\ \ -1)\binom{0}{0}\right)\right\rfloor = 1$$

$$2 \xrightarrow{\binom{0}{1}} \left\lfloor \tfrac{1}{2}\left(2-(2\ \ -1)\binom{0}{1}\right)\right\rfloor = 1$$

$$2 \xrightarrow{\binom{1}{0}} \left\lfloor \tfrac{1}{2}\left(2-(2-1)\binom{1}{0}\right)\right\rfloor = 0$$

$$2 \xrightarrow{\binom{1}{1}} \left\lfloor \tfrac{1}{2}\left(2-(2-1)\binom{1}{1}\right)\right\rfloor = 0$$

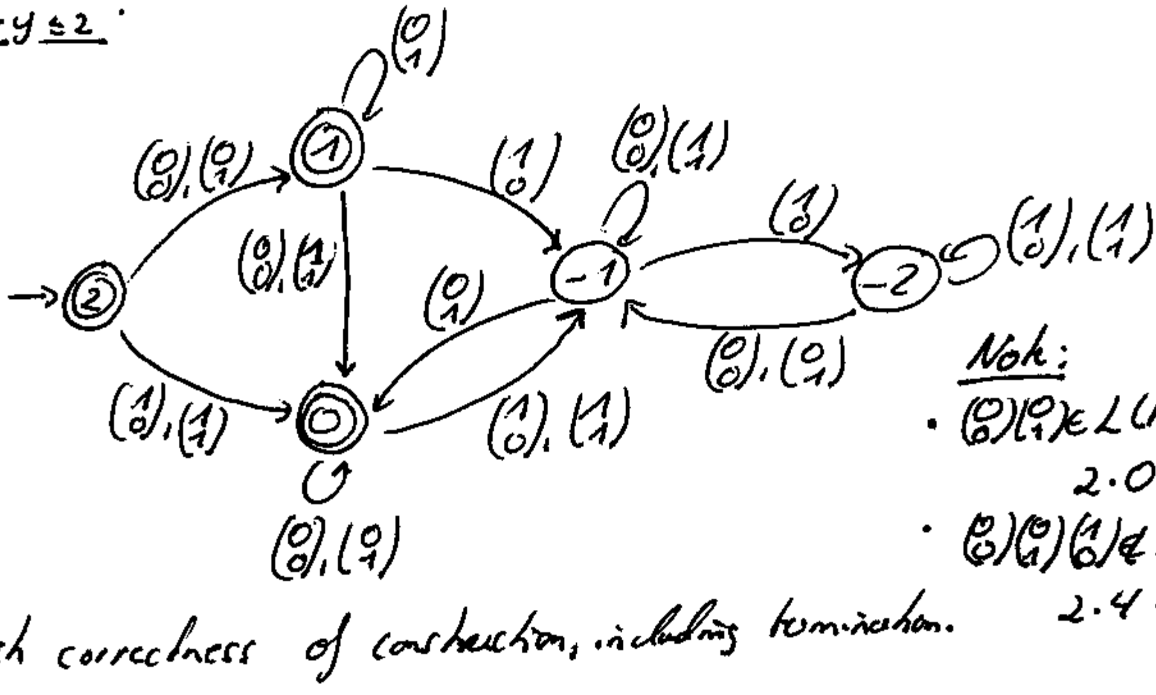
$$1 \xrightarrow{\binom{0}{0}} \left\lfloor \tfrac{1}{2}\left(1-(2-1)\binom{0}{0}\right)\right\rfloor = 0$$

$$1 \xrightarrow{\binom{0}{1}} \left\lfloor \tfrac{1}{2}\left(1-(2\ -1)\binom{0}{1}\right)\right\rfloor = 1$$

$$1 \xrightarrow{\binom{1}{0}} \left\lfloor \tfrac{1}{2}\left(1-(2\ -1)\binom{1}{0}\right)\right\rfloor = -1$$

$$\vdots$$

$\underline{A_{2x-y\le 2}}$:



Note:

- $\binom{0}{0}\binom{0}{1} \in L(A_c)$ and $2\cdot 0 - 2 \le 2$
- $\binom{0}{0}\binom{0}{1}\binom{1}{0} \notin L(A_c)$ since $2\cdot 4 - 2 \not\le 2$.

Establish correctness of construction, including termination.

Correctness:

For every $q \in \mathbb{Z}$ and every $w \in (\{0,1\}^n)^*$ we have

q accepts w iff w encodes $\bar{c}$ with $\bar{a}\,\bar{c} \le q$.

By induction on $|w|$.

Termination:

Lemma:

Let $\tau = \bar{a}\,\bar{x} \leq b$. Let $s = \sum_{i=1}^{n} |a_i|$.

All states $j \in \mathbb{Z}$ added to the worklist satisfy

$$-|b| - s \leq j \leq |b| + s$$

Proof:

By induction on the number of loop iterations in the algorithm.

$\underset{k=0}{\text{IH}}$: The only state in the worklist is $q_0 = b$. ✓

IS: Assume all states added to the worklist so far satisfy the inequalities.

Assume the loop iteration now adds $j \in \mathbb{Z}$.

Then there was a state $q \in \mathbb{Z}$ in the worklist and $\overline{bit} \in \{0,1\}^n$ so that

$$j = \left\lfloor \tfrac{1}{2}(q - \bar{a}\,\overline{bit}) \right\rfloor$$

Since by induction hypothesis q satisfies

$$-|b| - s \leq q \leq |b| + s$$

we have

$$\left\lfloor \frac{-|b| - s - \bar{a}\,\overline{bit}}{2} \right\rfloor \leq j \leq \left\lfloor \frac{|b| + s - \bar{a}\,\overline{bit}}{2} \right\rfloor.$$

Note that

$$-|b| - s \leq \left\lfloor \frac{-|b| - 2s}{2} \right\rfloor \leq \left\lfloor \frac{-|b| - s - \bar{a}\,\overline{bit}}{2} \right\rfloor$$

and

$$\left\lfloor \frac{|b| + s - \bar{a}\,\overline{bit}}{2} \right\rfloor \leq \frac{|b| + 2s}{2} \leq |b| + s$$

Hence,

$$-|b| - s \leq j \leq |b| + s. \qquad \square$$