Reachability in 2-clock automata:
A deceptively hard problem

Paul Hunter

Université Libre de Bruxelles

MFV, December 2013
The problem

Bounded one-counter machine:

- One counter, taking integer values in $[0, M)$
- One guarded transition $q_I \rightarrow q_F$
- Three increment/decrement transitions $q_I \rightarrow q_I$

Problem
Given $a, b, c, M, t \in \mathbb{N}$ can the machine reach $q_F$?
The problem

Bounded one-counter machine:

- One counter, taking integer values in \([0, M)\)
- One guarded transition \(q_I \rightarrow q_F\)
- Three increment/decrement transitions \(q_I \rightarrow q_I\)

Problem

Given \(a, b, c, M, t \in \mathbb{N}\) can the machine reach \(q_F\)?
The problem

Bounded one-counter machine:

\[ +b +a = t? \]

- One counter, taking integer values in \([0, M)\)
- One guarded transition \(q_I \rightarrow q_F\)
- Three increment/decrement transitions \(q_I \rightarrow q_I\)

Problem
Given \(a, b, c, M, t \in \mathbb{N}\) can the machine reach \(q_F\)?
Motivation: Timed automata

Timed automata were introduced by Rajeev Alur at Stanford during his PhD thesis under David Dill.

\[
\begin{align*}
\text{Accepts timed words over } \{a\} \text{ where there are two } a\text{'s exactly one time unit apart}
\end{align*}
\]

Many problems undecidable, but what about reachability?
Motivation: Timed automata

Timed automata were introduced by Rajeev Alur at Stanford during his PhD thesis under David Dill.

Accepts timed words over \( \{a\} \) where there are two \( a \)'s exactly one time unit apart

Many problems undecidable, but what about reachability?
Reachability in Timed Automata

PSPACE-complete with $2n + 1$ clocks \[\text{[AD90]}\]

PSPACE-complete with 3 clocks \[\text{[CY92]}\]

NL-complete with 1 clock \[\text{[LMS04]}\]

Two-clock reachability is equivalent to bounded one-counter reachability \[\text{[HOW12]}\]

NP-complete for unbounded one-counter reachability \[\text{[HKOW09]}\]

PSPACE-complete with 2 clocks \[\text{[FJ13]}\]
Reachability in Timed Automata

PSPACE-complete with $2n + 1$ clocks \[\text{[AD90]}\]

PSPACE-complete with 3 clocks \[\text{[CY92]}\]

NL-complete with 1 clock \[\text{[LMS04]}\]

Two-clock reachability is equivalent to bounded one-counter reachability \[\text{[HOW12]}\]

NP-complete for unbounded one-counter reachability \[\text{[HKOW09]}\]

PSPACE-complete with 2 clocks \[\text{[FJ13]}\]
Reachability in Timed Automata

PSPACE-complete with $2n + 1$ clocks \[\text{[AD90]}\]

PSPACE-complete with 3 clocks \[\text{[CY92]}\]

NL-complete with 1 clock \[\text{[LMS04]}\]

Two-clock reachability is equivalent to bounded one-counter reachability \[\text{[HOW12]}\]

NP-complete for unbounded one-counter reachability \[\text{[HKOW09]}\]

PSPACE-complete with 2 clocks \[\text{[FJ13]}\]
Reachability in Timed Automata

PSPACE-complete with $2n + 1$ clocks \[\text{[AD90]}\]

PSPACE-complete with 3 clocks \[\text{[CY92]}\]

NL-complete with 1 clock \[\text{[LMS04]}\]

Two-clock reachability is equivalent to bounded one-counter reachability \[\text{[HOW12]}\]

NP-complete for unbounded one-counter reachability \[\text{[HKOW09]}\]

PSPACE-complete with 2 clocks \[\text{[FJ13]}\]
From timed automata to counter machines

**Idea:** Store difference of two clocks in counter value

**Problem:** How to do inequalities?

**Solution:** Impose upper-bound limit on counter value!
From timed automata to counter machines

Idea: Store difference of two clocks in counter value

Problem: How to do inequalities?

Solution: Impose upper-bound limit on counter value!
The problem

Bounded one-counter machine:

- One counter, taking integer values in $[0, M)$
- One guarded transition $q_I \rightarrow q_F$
- Three increment/decrement transitions $q_I \rightarrow q_I$

Problem
Given $a, b, c, M, t \in \mathbb{N}$ can the machine reach $q_F$?
The problem

Bounded one-counter machine:

- One counter, taking integer values in \([0, M]\)
- One guarded transition \(q_I \rightarrow q_F\)
- Three increment/decrement transitions \(q_I \rightarrow q_I\)

Problem

Given \(a, b, c, M, t \in \mathbb{N}\) can the machine reach \(q_F\)?
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:

\[ 5a - 3c \]
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:

\[ 5a - 3c \]
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:

\[ 5a - 3c \]
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:

\[ 5a - 3c \]
A geometric interpretation

Run of the machine can be thought of as a 2-dimensional walk:
Solving the 2-D case

Theorem
Let \((m, n)\) be a feasible point, and let \(P\) be the parallelogram bounded by the parallel lines, \(x = 0\) and \(x = m\). Then there is a walk from \((0, 0)\) to \((m, n)\) if and only if \(P\) contains at least \(m + n + 1\) lattice points.

Theorem (Pick’s theorem)
Let \(P\) be a convex polyhedron with vertices on lattice points. Then

\[
\text{Area}(P) = \#\text{interior points} + \frac{1}{2} \#\text{boundary points}.
\]
Solving the 2-D case

Theorem
Let \((m, n)\) be a feasible point, and let \(P\) be the parallelogram bounded by the parallel lines, \(x = 0\) and \(x = m\). Then there is a walk from \((0, 0)\) to \((m, n)\) if and only if \(P\) contains at least \(m + n + 1\) lattice points.

Theorem (Pick’s theorem)
Let \(P\) be a convex polyhedron with vertices on lattice points. Then

\[
\text{Area}(P) = \# \text{interior points} + \frac{1}{2} \# \text{boundary points}.
\]
Solving the 2-D case

There are analogues of Pick’s theorem for non-lattice vertices and in more than 2 dimensions.

Unfortunately there is no analogue of the first theorem in 3 dimensions.
A graph theoretic perspective

Consider the configuration graph $G_{a,b,c}^M$ of the counter machine:

- Vertices are integers in $[0, M)$
- $a$-edges from $n$ to $n + a$; $b$-edges from $n$ to $n + b$ and $c$-edges from $n$ to $n - c$.

Reachability in counter machine = Reachability in $G_{a,b,c}^M$.

$G_{a,b,c}^M$ has nice properties:

- $G_{a,c}^M$ is a subgraph of $G_{a,b,c}^M$
- $G_{a,b,c}^{M'}$ is a subgraph of $G_{a,b,c}^M$ if $M' \leq M$.

What does $G_{a,b,c}^M/G_{a,c}^M$ look like?
Some group theory

Given a group $G$ and a set $S \subseteq G$ the Cayley graph of $G$ with respect to $S$ is the graph with

- Vertices are elements of $G$ generated by $S$
- There is an $(s)$-edge from $x$ to $y$ if $y = x \cdot s$ for some $s \in S$.

$G_{a,b,c}^M$ is an induced subgraph of the Cayley graph of $(\mathbb{Z}, +)$ with respect to $\{a, b, -c\}$!
Given a group $G$ and a set $S \subseteq G$ the Cayley graph of $G$ with respect to $S$ is the graph with

- Vertices are elements of $G$ generated by $S$
- There is an $(s)$-edge from $x$ to $y$ if $y = x \cdot s$ for some $s \in S$.

$G_{a,b,c}^M$ is an induced subgraph of the Cayley graph of $(\mathbb{Z}, +)$ with respect to $\{a, b, -c\}$!
What does $G^M_{a,c}$ look like?

**Lemma**

- If $M \geq a + c$ then every vertex has out-degree at least 1 and in-degree at least 1.
- If $M \leq a + c$ then every vertex has out-degree at most 1 and in-degree at most 1.

**Corollary**

If $M = a + c$ then $G^M_{a,c}$ is a set of $(\gcd(a, c))$ disjoint cycles.

**Corollary**

If $M \geq a + c$ and $\gcd(a, c) | t$ then there is a path from 0 to $t$. 
What does $G_{a,c}^M$ look like?

Lemma

- If $M \geq a + c$ then every vertex has out-degree at least 1 and in-degree at least 1.
- If $M \leq a + c$ then every vertex has out-degree at most 1 and in-degree at most 1.

Corollary

If $M = a + c$ then $G_{a,c}^M$ is a set of $(\gcd(a, c))$ disjoint cycles.

Corollary

If $M \geq a + c$ and $\gcd(a, c) | t$ then there is a path from 0 to t.
What does $G_{a,c}^M$ look like?

**Lemma**

- If $M \geq a + c$ then every vertex has out-degree at least 1 and in-degree at least 1.
- If $M \leq a + c$ then every vertex has out-degree at most 1 and in-degree at most 1.

**Corollary**

If $M = a + c$ then $G_{a,c}^M$ is a set of $(\gcd(a, c))$ disjoint cycles.

**Corollary**

If $M \geq a + c$ and $\gcd(a, c) | t$ then there is a path from 0 to $t$. 
From 3-D to 2-D

Theorem

If $M \geq a + c$ then reachability in $G_{a,b,c}^M$ reduces to reachability in $G_{b, d-b}^d$ where $d = \gcd(a, c)$. 
What about if $M < a + c$?

$G_{a,b,c}^M$ is a set of disjoint paths. How to tell if $s$ and $t$ are on the same path?

**Solution**: Look at the maximum value between $s$ and $t$ on $G_{a,c}^{a+c}$.
What about if $M < a + c$?

$G_{a,b,c}^M$ is a set of disjoint paths. How to tell if $s$ and $t$ are on the same path?

**Solution:** Look at the maximum value between $s$ and $t$ on $G_{a,c}^{a+c}$. 
The vertices of $G_{a+c}^a$ are $[0, a + c)$ which are the integers modulo $a + c$. Also, $+a \equiv -c \pmod{a + c}$.

Traversing $G_{a+c}^a$ is equivalent to taking multiples of $a$ modulo $a + c$.

**Problem**

Given $a, M, t$ let $n$ be the smallest positive integer such that $t \equiv n \cdot a \pmod{M}$. What is the maximum value of $\{i \cdot a \pmod{M} : 0 \leq i \leq n\}$?
The vertices of $G_{a,c}^{a+c}$ are $[0, a + c)$ which are the integers modulo $a + c$. Also, $+a \equiv -c \pmod{a + c}$.

Traversing $G_{a,c}^{a+c}$ is equivalent to taking multiples of $a$ modulo $a + c$.

**Problem**

Given $a, M, t$ let $n$ be the smallest positive integer such that $t \equiv n \cdot a \pmod{M}$. What is the maximum value of $\{i \cdot a \pmod{M} : 0 \leq i \leq n\}$?
Every natural number can be written as a sum of Fibonacci numbers,

\[ n = \sum_{i=1}^{k} \delta_i F_i \]

where \( \delta_i \in \{0, 1\} \) and \( F_i \) is the \( i \)-th Fibonacci number. With the rewrite rule 011 \( \rightarrow \) 100 this representation is unique. This is the Fibonacci representation.
Facts about the Fibonacci representation

- The Fibonacci representation of $n$ is logarithmic in the size of $n$
- There is a 1-1 correspondence with fit-strings and polynomials in $\mathbb{Z}[X]/(X^2 - X - 1)$
- There is a 1-1 correspondence with fit-strings and elements of $\mathbb{Z}(\varphi)$
- The Fibonacci representation can be seen as the “base-$\varphi$ representation”.
Negafibonacci representation

Every integer can be written as a sum of negaFibonacci numbers,

\[ n = \sum_{i=1}^{k} \delta_i F_i \]

where \( \delta_i \in \{0, 1\} \) and \( F_i \) is the \((-i)\)-th Fibonacci number.

Application: Navigating a tiling of the hyperbolic plane [Knuth].
Negafibonacci representation

Every integer can be written as a sum of negaFibonacci numbers,

\[ n = \sum_{i=1}^{k} \delta_i F_i \]

where \( \delta_i \in \{0, 1\} \) and \( F_i \) is the \((-i)\)-th Fibonacci number.

**Application:** Navigating a tiling of the hyperbolic plane [Knuth].
Euclidean representation

Let \( r_0 = a + c, \ r_1 = a \) and consider the sequence of \( r_i \) and \( q_i \) generated by the Euclidean algorithm via

\[
r_i = q_{i+1} \cdot r_{i+1} + r_{i+2}.
\]

**Theorem**

*Every integer* \( N \in [-a, c) \) *has a unique representation of the form*

\[
N = \sum_{i=1}^{m} (-1)^{i+1} b_i \cdot r_i
\]

*where* \( 0 \leq b_1 \leq q_1 - 1; 0 \leq b_k \leq q_k, \text{ for } k \geq 2 \text{ and } b_k = 0 \text{ if } b_{k+1} = q_{k+1}. \) *Moreover, the difference between lexicographic neighbours in this encoding is either* \( a \) *or* \( -c. \)
Euclidean representation example

Consider $a = 17, \ c = 5$:

$$
\begin{align*}
22 & = 1.17 + 5 \quad (q_1 = 1) \\
17 & = 3.5 + 2 \quad (q_2 = 3) \\
5 & = 2.2 + 1 \quad (q_3 = 2) \\
2 & = 2.1 + 0 \quad (q_4 = 2)
\end{align*}
$$

Permissible $b_4 b_3 b_2 \ (b_1 = 0)$:

$$
\begin{array}{cccccccc}
000(0) & 010(2) & 020(4) & 103(-16) & 113(-14) & 202(-12) \\
001(-5) & 011(-3) & 100(-1) & 110(1) & 120(3) & 203(-17) \\
002(-10) & 012(-8) & 101(-6) & 111(-4) & 200(-2) \\
003(-15) & 013(-13) & 102(-11) & 112(-9) & 201(-7)
\end{array}
$$
Algorithm for 2-D reachability

Finding the maximum value between $s$ and $t$ on $G_{a,c}^{a+c}$ then becomes:

- Compute the representation of $s$ and $t$
- Solve the resulting linear constraint problem to find the maximum value between $s$ and $t$
The Ostrowski representation can be seen as a generalization of (nega)Fibonacci representation. Given $\alpha \in \mathbb{R}_{\geq 0}$ let 

$[a_0, a_1, \ldots]$ be the continued fraction representation of $\alpha$. That is:

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

Let $\frac{p_n}{q_n}$ represent the $n$-th approximation of $\alpha$ and let $\theta_n = q_n \alpha - p_n$. 
Theorem

If \( \alpha \) is irrational then

- Every natural number \( N \) can be written uniquely in the form
  \[
  N = \sum_{i=1}^{m} b_i q_{i-1}
  \]
  where \( 0 \leq b_1 \leq a_1 - 1; 0 \leq b_k \leq a_k \), for \( k \geq 2 \) and \( b_k = 0 \) if \( b_{k+1} = a_{k+1} \).

- Every real number \( x \in [-\alpha, 1 - \alpha) \) can be written uniquely in the form
  \[
  x = \sum_{i=1}^{\infty} b_i \theta_{i-1}
  \]
  where \( 0 \leq b_1 \leq a_1 - 1; 0 \leq b_k \leq a_k \), for \( k \geq 2 \), \( b_k = 0 \) if \( b_{k+1} = a_{k+1} \) and \( b_k \neq a_k \) for infinitely many odd indices.
What’s going on?

Intuitively $\sum_{i=1}^{\infty} b_i \theta_{i-1}$ is the fractional part (shifted to $[-\alpha, 1 - \alpha]$) of $N\alpha$ where

$$N = \sum_{i=1}^{\infty} b_i q_{i-1}.$$ 

Integer multiples of $\frac{a}{a+c}$ modulo 1 are equivalent to integer multiples of $a$ modulo $a+c$ when $\alpha$ is rational.

When $\alpha$ is rational,

- The continued fraction for $\alpha$ is finite so the Ostrowski representation is finite, and
- $\theta_n = (-1)^{n+1} \frac{r_n}{r_0}$ where $r_i$ is derived from the Euclidean algorithm.

Corollary

The Euclidean representation is equivalent to the Ostrowski representation.
What’s going on?

Intuitively  \( \sum_{i=1}^{\infty} b_i \theta_{i-1} \) is the fractional part (shifted to \([−α, 1 − α)\)) of \( Nα \) where

\[
N = \sum_{i=1}^{\infty} b_i q_{i-1}.
\]

Integer multiples of \( \frac{a}{a+c} \) modulo 1 are equivalent to integer multiples of \( a \) modulo \( a + c \)

When \( α \) is rational,

- The continued fraction for \( α \) is finite so the Ostrowski representation is finite, and
- \( \theta_n = (-1)^{n+1} \frac{r_n}{r_0} \) where \( r_i \) is derived from the Euclidean algorithm.

Corollary

The Euclidean representation is equivalent to the Ostrowski representation
Returning to geometry
Returning to geometry

\[(1, 0), (3, 1), (7, 2), (17, 5)\]
Returning to geometry

(1, 0) (3, 1) (7, 2) (17, 5)