Closed Forms for Numerical Loops

Zachary Kincaid\(^1\)  Jason Breck\(^2\)  John Cyphert\(^2\)  Thomas Reps\(^{2,3}\)

\(^1\)Princeton University  \(^2\)University of Wisconsin-Madison  \(^3\)GrammaTech, Inc

January 16, 2019
Loop summarization

The problem: given a loop, compute a formula that represents its behavior.

```
while (i < n):
    i := i + 2
    j := j + 1
```
Loop summarization

The problem: given a loop, compute a formula that represents its behavior.

\[ \text{while}(i < n): \]
\[ i := i + 2 \]
\[ j := j + 1 \]

Before exec

\[ \exists k \in \mathbb{N}. \left( \begin{array}{l}
  i' = i + 2k \\
  j' = j + k \\
  n' = n \\
  i' \geq n \land (k \geq 1 \Rightarrow i' \leq n + 1)
\end{array} \right) \]

After exec

\[ \text{Loop counter} \]
Loop summarization

The problem: given a loop, compute a formula that represents its behavior.

while \( i < n \):
  \( i := i + 2 \)
  \( j := j + 1 \)

\[ \exists k \in \mathbb{N}. \left( \begin{array}{c}
  i' = i + 2k \\
  j' = j + k \\
  n' = n \\
  i' \geq n \land (k \geq 1 \Rightarrow i' \leq n + 1) \\
  \neg (2j' = i')
\end{array} \right) \]

Summary can be used to answer questions about program behavior

- Is \( \{ i = j = 0 \land n > 0 \} \text{loop}\{2j = i\} \) valid?
Today: Linear loops

while ( * ):
    x := A x

non-deterministic

A ∈ Q^{n×n}
Today: Linear loops

```python
while ( * ):
    x := Ax
```

A ∈ Q^{n×n}

- In the paper: affine & solvable polynomial loops
  [Rodríguez-Carbonell & Kapur, ISAAC 2004].
Why linear loops?

- Natural problem
Why linear loops?

- Natural problem
- Practical applications
  - Any loop can be *approximated* by a linear loop [KBCR POPL’18]
  - Summary for the approximation gives invariants for the loop
Approximating general loops [KBCR POPL’18]

binary-search(A,target):
    lo = 1, hi = size(A), ticks = 0
    while (lo <= hi):
        ticks++;
        mid = lo + (hi-lo)/2
        if A[mid] == target:
            return mid
        else if A[mid] < target:
            lo = mid+1
        else:
            hi = mid-1

Not a linear transformation
Approximating general loops [KBCR POPL’18]

binary-search(A,target):
    lo = 1, hi = size(A), ticks = 0
    while (lo <= hi):
        ticks++;
        mid = lo + (hi-lo)/2
        if A[mid] == target:
            return mid
        else if A[mid] < target:
            lo = mid+1
        else:
            hi = mid-1

while (*):
    \[
    \begin{bmatrix}
    x \\
    y \\
    z
    \end{bmatrix}
    :=
    \begin{bmatrix}
    1 & 0 & 1 \\
    0 & 1 & 0 \\
    0 & 0 & 1
    \end{bmatrix}
    \begin{bmatrix}
    x \\
    y \\
    z
    \end{bmatrix}
    \]
Approximating general loops [KBCR POPL’18]

```
while
(ticks, lo, hi, mid, target, A)[ticks] 
\sim \begin{bmatrix}
  x \\
  y \\
  z
\end{bmatrix} \iff \begin{array}{l}
  x = ticks \land hi - lo \leq y \land z = 1
\end{array}
```

```python
binary_search(A, target):
    lo = 1, hi = size(A), ticks = 0
    while (lo <= hi):
        ticks++;
        mid = lo + (hi-lo)/2
        if A[mid] == target:
            return mid
        elif A[mid] < target:
            lo = mid+1
        else:
            hi = mid-1
```
Approximating general loops [KBCR POPL’18]

**binary-search(A,target)**

lo = 1, hi = size(A)

**while** (lo <= hi):

    ticks++;

    mid = lo + (hi-lo)

    if A[mid] == target:
        **return** mid

    else if A[mid] < target:
        lo = mid+1

    else:
        hi = mid-1
binary-search(A,target):
    lo = 1, hi = size(A), ticks = 0
    while (lo <= hi):
        ticks++;
        mid = lo + (hi-lo)/2
        if A[mid] == target:
            return mid
        else if A[mid] < target:
            lo = mid+1
        else:
            hi = mid-1

\[ \exists k \in \mathbb{N}. \left( \begin{array}{l}
    x' = x + kz \\
    y' = (1/2)^k y \\
    z' = z
\end{array} \right) \]
Approximating general loops [KBCR POPL’18]

binary-search(A,target):

lo = 1, hi = size(A), ticks = 0

while (lo <= hi):
    ticks++;
    mid = lo + (hi-lo)/2
    if A[mid] == target:
        return mid
    else if A[mid] < target:
        lo = mid+1
    else:
        hi = mid-1

∃k ∈ N. (ticks′ = ticks + k
∧ hi′ − lo′ ≤ (1/2)^k(hi − lo))
Hasn’t this problem already been solved?

Given a square matrix $A \in \mathbb{Q}^{n \times n}$, can compute $A^k$ symbolically.

Entries of $A^k$ are exponential polynomials:

$$a_1 \lambda_1^k k^{d_1} + \cdots + a_n \lambda_n^k k^{d_n}$$

Algebraic numbers

Camille Jordan
Hasn’t this problem already been solved?

Given a square matrix $A \in \mathbb{Q}^{n \times n}$, can compute $A^k$ symbolically.

Entries of $A^k$ are exponential polynomials:

$$a_1 \lambda_1^k k^{d_1} + \cdots + a_n \lambda_n^k k^{d_n}$$

Algebraic numbers

```
while(*):

x := Ax
```

$$\exists k \in \mathbb{N}. x' = A^k x$$

Camille Jordan
No.

Skolem's problem (variant):

Given an exponential-polynomial $f$ over the algebraic numbers, does there exist some $n \in \mathbb{N}$ such that $f(k) = 0$?

Decidability of Skolem's problem is unknown!
Skolem's problem (variant):

\[ \text{Given an exponential-polynomial } f \text{ over the algebraic numbers, does there exists some } n \in \mathbb{N} \text{ such that } f(k) = 0? \]

Decidability of Skolem's problem is unknown!

Essential problem: algebraic numbers.
Starting point of this work: *avoid algebraic numbers*

1. *Periodic rational* matrices have closed forms over $\mathbb{Q}$.
   - Computable in polytime
Outline

Starting point of this work: *avoid algebraic numbers*

1. *Periodic rational* matrices have closed forms over $\mathbb{Q}$.
   - Computable in polytime

2. All matrices have best periodic-rational approximations.
Starting point of this work: 

**avoid algebraic numbers**

1. *Periodic rational* matrices have closed forms over $\mathbb{Q}$.
   - Computable in polytime

2. All matrices have best periodic-rational approximations.

3. Exponential-polynomial arithmetic over $\mathbb{Q}$ is decidable.
Closed forms for linear loops
Known:

- Eigenvalues of $A$ are rational $\Rightarrow A^k$ can be expressed in exponential-polynomial arithmetic over $\mathbb{Q}$. 
Known:

- Eigenvalues of $A$ are rational $\Rightarrow A^k$ can be expressed in exponential-polynomial arithmetic over $\mathbb{Q}$.
- [Boigelot PhD thesis ’99]: $A$ generates a finite monoid $\Rightarrow A^k$ can be expressed in Presburger arithmetic.
Known:

- Eigenvalues of $A$ are rational $\Rightarrow A^k$ can be expressed in exponential-polynomial arithmetic over $\mathbb{Q}$.
- [Boigelot PhD thesis ’99]: $A$ generates a finite monoid $\Rightarrow A^k$ can be expressed in Presburger arithmetic.

**Common generalization:** A matrix $A$ is **periodic rational** if there is some power $p$ such that $A^p$ has rational eigenvalues.
Known:

- Eigenvalues of $A$ are rational $\Rightarrow A^k$ can be expressed in exponential-polynomial arithmetic over $\mathbb{Q}$.
- [Boigelot PhD thesis ’99]: $A$ generates a finite monoid $\Rightarrow A^k$ can be expressed in Presburger arithmetic.

**Common generalization:** A matrix $A$ is periodic rational if there is some power $p$ such that $A^p$ has rational eigenvalues.

- $A$ periodic rational $\Rightarrow$ can express closed form as

$$
\left( \exists k \in \mathbb{N}. x' = A^k x \right) \equiv \left( \exists k \in \mathbb{N}. \bigvee_{i=0}^{p-1} k \equiv i \mod p \land x' = (A^p)^{\lfloor k/p \rfloor} A^i x \right)
$$
• **Problem:** Rational period of a matrix might be exponential in its size
  • Expressing closed form takes exponential space!
• **Problem:** Rational period of a matrix might be exponential in its size
  • Expressing closed form takes exponential space!
• **Solution:** periodic rational spectral decomposition
Let $A \in \mathbb{Q}^{n \times n}$ be a square rational matrix. A periodic rational spectral decomposition of $A$ is a set of triples

$$\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle\} \subset \mathbb{N} \times \mathbb{Q} \times \mathbb{Q}^n$$

such that

- for each $i$, $v_i$ is a generalized eigenvector of $A^{p_i}$, with eigenvalue $\lambda_i$. 

---

**Periodic rational spectral decomposition (PRSD)**
Periodic rational spectral decomposition (PRSD)

Let \( A \in \mathbb{Q}^{n \times n} \) be a square rational matrix. A periodic rational spectral decomposition of \( A \) is a set of triples

\[
\{ \langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle \} \subset \mathbb{N} \times \mathbb{Q} \times \mathbb{Q}^n
\]

such that

- for each \( i \), \( v_i \) is a generalized eigenvector of \( A^{p_i} \), with eigenvalue \( \lambda_i \).
- \( \{ v_1, \ldots, v_m \} \) is linearly independent
Periodic rational spectral decomposition (PRSD)

Let $A \in \mathbb{Q}^{n \times n}$ be a square rational matrix. A periodic rational spectral decomposition of $A$ is a set of triples

$$\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle\} \subset \mathbb{N} \times \mathbb{Q} \times \mathbb{Q}^n$$

such that

- for each $i$, $v_i$ is a generalized eigenvector of $A^{p_i}$, with eigenvalue $\lambda_i$.
- $\{v_1, \ldots, v_m\}$ is linearly independent
- Informally: $\{v_1, \ldots, v_m\}$ is maximal
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle\}$.

- $(x' = A^k x)$ takes exponential space, \textit{but}
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, \mathbf{v}_1 \rangle, \ldots, \langle p_m, \lambda_m, \mathbf{v}_m \rangle\}$.

- $(\mathbf{x}' = A^k \mathbf{x})$ takes exponential space, but

- for any $i$, $(\mathbf{v}_i^T \mathbf{x}' = \mathbf{v}_i^T A^k \mathbf{x})$ can be computed in polytime

  - Intuition: break up period.
    Each $\mathbf{v}_i$ is an easy-to-compute projection
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle \}$. 

- $\left(x' = A^k x\right)$ takes exponential space, but

- for any $i$, $\left(v_i^T x' = v_i^T A^k x\right)$ can be computed in polytime

  - Intuition: break up period.
    Each $v_i$ is an easy-to-compute projection

\[ A \text{ is periodic rational} \iff \text{State-space can be recovered from projections} \]

\[
\left(x' = A^k x\right) \equiv \left( \bigwedge_{i=1}^m v_i^T x' = v_i^T A^k x \right)
\]
Approximating linear loops
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle\}$.

- Set $V = [v_1 \ v_2 \ \ldots \ v_m]^T$. 
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle\}$.

- Set $V = \begin{bmatrix} v_1 & v_2 & \ldots & v_m \end{bmatrix}^T$.
- There exists a unique $B \in \mathbb{Q}^{m \times m}$ with $VA = BV$.
  - $B$ is periodic rational.
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle \}$.

- Set $V = [v_1 \ v_2 \ \ldots \ v_m]^T$.
- There exists a unique $B \in \mathbb{Q}^{m \times m}$ with $VA = BV$.
  - $B$ is periodic rational
  - $B$ simulates $A$, and $V$ is a simulation:

$$
\begin{array}{ccc}
  & V & \\
\vdots & \vdots & \vdots \\
A & & B \\
a' & & b'
\end{array}
$$
Let $A$ be a matrix with PRSD $\{\langle p_1, \lambda_1, v_1 \rangle, \ldots, \langle p_m, \lambda_m, v_m \rangle \}$.

- Set $V = [v_1 \ v_2 \ \ldots \ v_m]^T$.
- There exists a unique $B \in \mathbb{Q}^{m \times m}$ with $VA = BV$.
  - $B$ is periodic rational
  - $B$ simulates $A$, and $V$ is a simulation:

\[
\begin{array}{ccc}
  a & \cdots & b \\
  \downarrow & \leftarrow & \downarrow \\
  A & \leftarrow & B \\
  \downarrow & & \downarrow \\
  a' & \cdots & b' \\
  \downarrow & \leftarrow & \downarrow \\
  V & \leftarrow & V \\
\end{array}
\]

$B$ is the best periodic-rational approximation of $A$.
Invariant generation pipeline

General loop $\rightarrow$ Linear loop

[POPL'18]
Invariant generation pipeline

General loop $\rightarrow$ Linear loop $\rightarrow$ Periodic rational linear loop

[KBCR POPL'18] This work
Invariant generation pipeline

General loop \textsuperscript{[KBCR POPL’18]} \rightarrow \text{Linear loop} \quad \text{This work} \quad \rightarrow \text{Periodic rational linear loop} \rightarrow \text{Closed form}
Invariant generation pipeline

General loop -> Linear loop -> Periodic rational linear loop

[KBCR POPL'18]

This work

Invariants

Closed form
Reasoning about non-linear arithmetic
Exponential-polynomial arithmetic is decidable

Two steps:

1. Eliminate all symbols except the loop counter (i.e., program variables)
   - Key idea: terms are linear over the ring of exponential-polynomials.
   - $\left(2^k k^3 - 3^k k^2 + 140 \cdot 3^k\right)x + \left(4^k k\right)y + \left(2^k\right)z$
   - Eliminate symbols using linear q.e. [Loos & Weispfenning ’93]
Exponential-polynomial arithmetic is decidable

Two steps:

1. Eliminate all symbols except the loop counter (i.e., program variables)
   - Key idea: terms are linear over the ring of exponential-polynomials.
   - \((2^k k^3 - 3^k k^2 + 140 \cdot 3^k)x + (4^k k)y + (2^k)z\)
   - Eliminate symbols using linear q.e. [Loos & Weispfenning ’93]

2. Find a bound for the loop counter
   - Key idea: exponential-polynomials are eventually dominated by the term with largest base (and largest degree)
   - E.g., \(2^k k^3 - 3^k k^2 + 140 \cdot 3^k\) is eventually negative
Consequences

Suppose $A$ is periodic rational. The following problems are decidable:

- Is $\{P\}\{\textbf{while}(\ast) : x := Ax\}\{Q\}$ valid?

Linear rational arithmetic
Suppose $A$ is periodic rational. The following problems are decidable:

- Is $\{ P \} \{ \text{while}(\ast) : x := A x \} \{ Q \}$ valid?

- Does $(x := v; \text{while}(C) \text{ do } x := A x)$ terminate?
Experiments
Suite of 101 microbenchmarks from C4B, HOLA, and literature:
Contributions:

1. Periodic rational linear loops have closed forms over \( \mathbb{Q} \).
   - Polytime computation of the summary
Contributions:

1. Periodic rational linear loops have closed forms over $\mathbb{Q}$.
   - Polytime computation of the summary

2. Every matrix has a best periodic-rational approximation.
Contributions:

1. Periodic rational linear loops have closed forms over $\mathbb{Q}$.
   - Polytime computation of the summary

2. Every matrix has a best periodic-rational approximation.

3. Exponential-polynomial arithmetic over $\mathbb{Q}$ is decidable.