Polynomial Solutions of Recurrence Relations

O. Shkaravska  M. van Eekelen  A. Tamalet

Digital Security, ICIS
Radboud Universiteit Nijmegen

Tallinn, 9 June 2009

Sponsored by the Netherlands Organisation for Scientific Research (NWO), project Amortized Heap Space Usage Analysis (AHA), grantnr. 612.063.511.
Motivation: recurrences in program analysis and math.

Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

Outline

1. Motivation: recurrences in program analysis and math.

2. Our Contribution: multi-step quadratic recurrences for 1-variable polynomials
Motivation: recurrences in program analysis and math.

Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

Size/Resource Recurrences

tails : $L_n(\alpha) \rightarrow L_{f(n)}(\alpha)$

tails $l = \begin{array}{l}
\text{match } l \text{ with} \\
\text{Nil } \Rightarrow \text{Nil} \\
\text{Cons}(hd, tl) \Rightarrow l ++ \text{tails}(tl)
\end{array}$

\[ \vdash f(0) = 0 \]
\[ n \geq 1 \quad \vdash f(n) = n + f(n - 1) \]
Linear Recurrences for 1-variable Functions

\[ \vdash f(0) = 0 \]
\[ n \geq 1 \quad \vdash f(n) = n + f(n - 1) \]

Homogenisation by symbolic differentiation:
\[ f'(n) := f(n) - f(n - 1), \]
\[ f'(n) = 1 + f'(n - 1), \quad f'(1) = 1 - 0 = 1 \]
\[ f''(n) := f'(n) - f'(n - 1) \]
\[ f''(n) = f''(n - 1), \quad f''(2) = f'(2) - f'(1) = 1, \]
\[ f''(n) = 1 \]
\[ f'''(n) = 0. \text{ If the solution is a polynomial, then the degree is 2:} \]
\[ f(n) = an^2 + bn + c \]
\[ f(0) = 0, \quad f(1) = 1, \quad f(2) = 3 \implies c = 0, \quad a = b = \frac{1}{2} \]
Non-linear recurrences: math. challenge

No general theory, as for linear recurrences. We consider polynomial solutions for such recurrences.

\[
\begin{align*}
    p(n_1, 0) &= 4n_1^2 \\
    p(0, n_2) &= 4n_2^2 \\
    p(n_1, n_2) &= (p(n_1 - 1, n_2) + n_1 - (p(n_1, n_2 - 1) + n_2))^2 + 17n_1n_2
\end{align*}
\]

We want to know such \( D \), that either \( \text{degree}(p) := z \leq D \) or \( D \) is not a polynomial at all.

If such \( D \) is known then we can use MUC or, as above (better!), fit a polynomial by solving SLE and check then if it suits the recurrence.

In the example we take \( D = 2 \) and obtain

\[
p(n_1, n_2) = 4n_1^2 + 4n_2^2 + 9n_1n_2
\]
Motivation: recurrences in program analysis and math.
Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

### Multi-step Quadratic Recurrence

**t-step Quadratic Recurrence**

\[ p(n) = \alpha_{11} p^2(n - r_1) + \alpha_{12} p(n - r_1) p(n - r_2) + \alpha_{22} p^2(n - r_2) + \alpha_{13} p(n - r_1) p(n - r_3) + \alpha_{33} p^2(n - r_3) + \ldots + \]

\[ \alpha_{t-1,t} p(n - r_{t-1}) p(n - r_t) + \alpha_{tt} p^2(n - r_t) + \]

\[ L\left(p(n - r_1), \ldots, p(n - r_t)\right) \]

**Our Aim**

Find \( D \) such that \( \text{deg}(p) \leq D \)
Motivation: recurrences in program analysis and math.
Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

Technicalities: gather coefficients at \( n^t \) in the r.h.s.

\[
p(n) = a_z n^z + \ldots + a_1 n + a_0
\]
\[
p(n - r) = a_z (n - r)^z + \ldots + a_1 (n - r) + a_0
\]
\[
p(n - r_k)p(n - r_l) = \sum_{0 \leq i, j \leq z} a_i a_j (n - r_k)^i (n - r_l)^j
\]
\[
p(n) = \sum_{1 \leq k \leq l \leq t} \alpha_{kl} \sum_{0 \leq i, j \leq z} a_i a_j
\]
\[
(K_{k, l}^{i, j, -0} n^{i+j} + K_{k, l}^{i, j, -1} n^{i+j-1} + \ldots + K_{k, l}^{i, j, -(i+j)})
\]
where
\[
K_{k, l}^{i, j, -0} = 1
\]
\[
\ldots
\]
\[
K_{k, l}^{i, j, -m} = \sum_{\gamma=0}^{m} C_i^\gamma C_j^{m-\gamma} (-r_k)^\gamma (-r_l)^{m-\gamma}
\]
## Cancellation equations for multi-step recurrence

<table>
<thead>
<tr>
<th>$t$</th>
<th>The coefficient at $n^t$</th>
<th>Cancellation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2z$</td>
<td>$v_0 = a_za_z\sum_{1 \leq k \leq l \leq t} K_{k, l}^{z, z, -0} \alpha_{kl}$</td>
<td>$2z &gt; z \Rightarrow v_0 = 0$</td>
</tr>
<tr>
<td>$2z - 1$</td>
<td>$v_1 = a_za_z\sum_{1 \leq k \leq l \leq t} K_{k, l}^{z, z, -1} \alpha_{kl} + a_{z-1}a_z\sum_{1 \leq k \leq l \leq t} K_{k, l}^{z-1, z, -0} \alpha_{kl} + a_za_{z-1}\sum_{1 \leq k \leq l \leq t} K_{k, l}^{z, z-1, -0} \alpha_{kl}$</td>
<td>$2z - 1 &gt; z \Rightarrow v_1 = 0$</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2z - m$</td>
<td>$v_m = \sum_{0 \leq i + j \leq m} a_{z-i}a_{z-j}\sum_{1 \leq k \leq l \leq t} K_{k, l}^{z-i, z-j, -(m-(i+j))} \alpha_{kl}$</td>
<td>$2z - m &gt; z \Rightarrow v_m = 0$</td>
</tr>
</tbody>
</table>
Motivation: recurrences in program analysis and math.
Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

Cancellation conditions form a homogeneous linear system w.r.t $\alpha_{kl}$

A homogeneous linear system: $A\bar{x} = 0$

- Folklore: if the amount of equations is equal to the amount of variables then the only solution is zero: $\bar{x} = \bar{0}$,
- in fact: if $\text{rank}(A) =$ “the amount of variables”, then $\bar{x} = \bar{0}$.

We note:

- the first $m + 1$ cancellation conditions form a homogeneous system w.r.t. $\alpha_{kl}$: $\nu_0 = 0$, $\nu_1 = 0$, ... $\nu_m$;
- $z > m$ implies $2z - m > z$ then all the $m + 1$ cancellation conditions must hold simultaneously, i.e. they form this system of $m + 1$ equations;
- our coefficients $\alpha_{kl}$ form exactly its solution;
Cancellation conditions form a homogeneous linear system w.r.t $\alpha_{kl}$

We note (continue):

- Let $z > \#\{\alpha_{kl}\} - 1$ ("the amount of coefficients" $\alpha_{kl} - 1$). Then we have a homogeneous system where the amount of equations, $\#\{\alpha_{kl}\}$ is equal to the amount of variables. Folklore: "it implies" that the system has only zero solution, i.e. all the coefficients $\alpha_{kl}$ are zero and the recurrence is linear.

- The real problem: we have to show that the RANK of the matrix of the system $v_m = 0$, where $0 \leq m \leq \#\{\alpha_{kl}\} - 1$, is equal to $\#\{\alpha_{kl}\}$;
  It is difficult: its determinant after $m \geq 4$ is really weird, with the unknown coefficients $a_i$ (at the moment I do not know if you can get rid of them).
Cancellation conditions form a homogeneous linear system w.r.t $\alpha_{kl}$

What we do know:

- for $1 \leq m \leq 3$ the coefficients for $m$ are expressible via the coefficients for $m - 1$,
- using this, we show that for $m \leq 3$ the unknown coefficients $a_i$ may be omitted,
- the determinant for the two-step recurrence over $p(n - r_1)$ and $p(n - r_2)$ with $m = 2$ is non-zero, that is the homogeneous system over $\alpha_{11}, \alpha_{12}, \alpha_{22}$ has a solution and it is zero, i.e. the recurrence is linear.
Motivation: recurrences in program analysis and math.
Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

Cancellation conditions form a homogeneous linear system w.r.t $\alpha_{kl}$

**Theorem 1**

If a quadratic two-step recurrence has a polynomial solution then its degree $z \leq 2$

If $z > 2$ then $2z - 2 > z$ and the cancellation conditions for $m = 0, 1, 2$ must hold. Moreover, the determinant of the matrix of the corresponding linear system is non-zero. Therefore, all the coefficients $\alpha_{11}, \alpha_{12}, \alpha_{22}$ are zero and the recurrence is linear.

Shkaravska, van Eekelen, Tamalet

Polynomial Solutions
Idea: coefficients at $n^{2z-m}$ are polynomials on $z$

$\#\{\alpha_{kl}\} \geq 4$: reduce to a system with simpler determinants.

We want to obtain the presentation

$$v_m(z) = A_{mm}z^m + \ldots + A_{m0} = 0,$$

from which follows:

$$\begin{cases} 
\text{either } A_{mm} \neq 0 \Rightarrow z \leq \left| \frac{A_{0m}}{A_{mm}} \right| \\
\text{or } A_{mm} = 0 \Rightarrow \text{we have a simpler equation instead of} \ v_m = 0
\end{cases}$$
Motivation: recurrences in program analysis and math.

Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

Computing $A_{mi}$ for $v(z) = A_{mm}z^m + \ldots + A_{m0}$

Lemma 1

The coefficient at the highest degree of $z$ in $v_m(z)$ is

$$A_{mm} = \frac{(-r_k - r_l)^m}{m!} a_z a_z$$
To our aim: find $D$, such that $z \leq D$

Theorem 1

$$z < \#(\alpha_{kl}) \text{ or }$$
$$z \leq \frac{|A_{d_00}|}{|A_{d_0d_0}|}, \text{ where } d_0 = \min_{1 \leq d \leq \#(\alpha_{kl})} \{A_{dd} \neq 0\}.$$  

Suppose that $z \geq \#(\alpha_{kl})$. Then all $v_m = 0$, where $0 \leq m \leq \#(\alpha_{kl})$, hold.

Suppose that $d$ with the property $A_{dd} \neq 0$ does not exist, that is for all $1 \leq m \leq \#(\alpha_{kl})$ we have $A_{mm} = 0$.  

Shkaravska, van Eekelen, Tamalet

Polynomial Solutions
To our aim: find $D$, such that $z \leq D$

From what follows that $\sum_{1 \leq k \leq l \leq t} (r_k + r_l)^m \alpha_{kl} = 0$ for $0 \leq m \leq \#(\alpha_{kl})$.

The determinant of this system is Vandermonde determinant.

If all the sums $r_k + r_l$ are different, then the determinant is non-zero. Therefore, the system has only the zero solution, which means that the recurrence is linear.

But this is often not the case: e.g. $\alpha_{13} p(n - 1)p(n - 3)$ and $\alpha_{22} p(n - 2)p(n - 2)$. 
Motivation: recurrences in program analysis and math.
Our Contribution: multi-step quadratic recurrences for 1-variable polynomials

To our aim: find $D$, such that $z \leq D$

Def.: $\{R_1, \ldots, R_s\} = \{R \mid \exists r_k r_l. R = r_k + r_l\}$

$$\sum_{i=1}^{s} R_i^m \beta_i = 0 \text{ for } 0 \leq m \leq \#(\alpha_{kl}).$$

$$\beta_i = \sum_{r_k + r_l = R_i} \alpha_{kl} = 0$$

($\#\{\alpha_{kl}\} + 1) - 1 + s$ equations over $s + \#\{\alpha_{kl}\}$ variables.
Future Work

- continue with multi-step quadratic recurrences, $t \geq 3$.
- extend to degree $d \geq 2$ recurrences
- extend to recurrences over multivariate polynomial solutions