Periodicity, Morphisms, and Matrices

Jeffrey Shallit
Department of Computer Science*
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
shallit@graceland.uwaterloo.ca
http://www.math.uwaterloo.ca/~shallit

* currently visiting University of Arizona on sabbatical

This talk is about joint work with S. Cautis, F. Mignosi, M.-w. Wang, and S. Yazdani.

Periodicity

Periodicity is an important property of words, with applications to

- string searching algorithms (e.g., Knuth-Morris-Pratt)
- formal languages (e.g., pumping lemmas)
- combinatorics on words (e.g., theorems of Thue, Lyndon-Schützenberger)

Periodicity

We say a sequence $(f_n)_{n\geq 0}$ is *periodic with period length* $h \geq 1$ if $f_n = f_{n+h}$ for all $n \geq 0$. The following is a classical "folk theorem":

Theorem. If $(f_n)_{n\geq 0}$ is a sequence which is periodic with period lengths h and k, then it is periodic with period length $\gcd(h, k)$.

Proof. By the extended Euclidean algorithm, there exist integers $r, s \geq 0$ such that $rh - sk = \gcd(h, k)$. Then we have

$$f_n = f_{n+rh} = f_{n+rh-sk} = f_{n+\gcd(h,k)}$$

for all $n \geq 0$. ∎

The 1965 Theorem of Fine & Wilf

Theorem. Let $(f_n)_{n\geq 0}$, $(g_n)_{n\geq 0}$ be two periodic sequences, of period lengths h and k respectively.

(a) If $f_n = g_n$ for $0 \leq n < h + k - \gcd(h,k)$, then $f_n = g_n$ for all $n \geq 0$.

(b) The conclusion in (a) would be false if $h + k - \gcd(h,k)$ were replaced by any smaller number.

Proof of (a). For the moment assume $\gcd(h,k) = 1$. The proof is easy when $h = k = 1$, so assume wlog $h > k$. Then we have

$$f_i = g_i = g_{i+k} = f_{i+k} = f_{(i+k) \bmod h}$$

for $0 \leq i < h - 1$.

Start with f_{k-1} and apply this relation $h-1$ times. We get

$$f_{k-1} = f_{2k-1} = \cdots = f_{(h-1)k-1} = f_{hk-1},$$

where the indices are taken (mod h). Since

$$\gcd(h, k) = 1,$$

it follows that all h indices (mod h) are represented in this equation. Hence $f_i = f_0$ for all i, and the same result holds for g_i.

Now let us remove the restriction $\gcd(h, k) = 1$. If $\gcd(h, k) = d$, group the symbols of f and g into groups of d symbols; call the result f' and g'. If f and g agree on the first $h + k - \gcd(h, k)$ symbols, then f' and g' agree on the first $\frac{h}{d} + \frac{k}{d} - 1$ symbols. Furthermore f' is periodic of period h/d and g' is periodic of period k/d. From the results above $f' = g'$ and so $f = g$. ∎

The Fine and Wilf Theorem

Proof of (b). Define strings $\sigma(h,k)$ as follows:

$$\sigma(h,k) = \begin{cases} 0, & \text{if } h = 0; \\ 0^{k-1}1, & \text{if } h \mid k; \\ \sigma(r,h)^q\, \sigma(r',r), & \text{if } h > 1 \text{ and} \\ & k = qh + r, \\ & h = q'r + r'. \end{cases}$$

Then it can be shown that if we construct periodic sequences f, g such that

- f is of period length k and has period $\sigma(h,k)$

- g is of period length h and has period $\sigma(k,h)$

then f and g agree on a prefix of a length

$$h + k - \gcd(h,k) - 1,$$

but disagree at the $h + k - \gcd(h,k)$'th term.

The Fine and Wilf Theorem

Remark. The maximal counter-examples in part (b) play a role in the Knuth-Morris-Pratt string-matching algorithm. For example, if $h = 5$ and $k = 8$ the maximal counter-examples are

$$\mathbf{f} = 1011010110101101011010110\cdots$$
$$\mathbf{g} = 101101011011010110110101\cdots$$

Variations on Fine & Wilf

Theorem. Let $\mathbf{f} = (f_n)_{n\geq 0}$, $\mathbf{g} = (g_n)_{n\geq 0}$ be two periodic sequences of real numbers, of period lengths h and k, respectively, such that

$$\sum_{0\leq i<h} f_i \geq 0 \tag{1}$$

and

$$\sum_{0\leq j<k} g_j \leq 0. \tag{2}$$

Let $d = \gcd(h, k)$.

(a) If

$$f_n \leq g_n \quad \text{for } 0 \leq n < h + k - d \tag{3}$$

then

(i) $f_n = g_n$ for all $n \geq 0$; and

(ii) $\sum_{j\leq i<j+d} f_i = \sum_{j\leq i<j+d} g_i = 0$ for all integers $j \geq 0$.

(b) The conclusion (a)(i) would be false if in the hypothesis $h + k - d$ were replaced by any smaller integer.

Sketch of Proof, Part (a)(i)

Define

$$
\begin{aligned}
P(z) &= 1 + z + \cdots + z^{h-1} = (z^h - 1)/(z - 1); \\
Q(z) &= 1 + z + \cdots + z^{k-1} = (z^k - 1)/(z - 1); \\
R(z) &= (z^k - 1)/(z^d - 1); \\
S(z) &= (z^h - 1)/(z^d - 1).
\end{aligned}
$$

By hypothesis $P \circ \mathbf{f} \geq 0$, where by $\circ$ we mean take the dot product of the coefficients of P to consecutive windows of $\mathbf{f}$. Then $R \circ (P \circ \mathbf{f}) \geq 0$. But then $RP \circ \mathbf{f} \geq 0$.

Similarly, by hypothesis $Q \circ (-\mathbf{g}) \geq 0$. Then $SQ \circ (-\mathbf{g}) \geq 0$. But $RP = SQ$, so

$$\sum_{0 \leq i < h+k-d} e_i (f_i - g_i) \geq 0. \qquad (4)$$

where $R(z)P(z) = \sum_{0 \leq i < h+k-d} e_i z^i$.

It can be shown that the e_i are strictly positive, so since $f_n \leq g_n$ for $0 \leq n < h+k-d$, we get $f_n = g_n$ for $0 \leq n < h+k-d$. By the Fine & Wilf theorem, $f_n = g_n$ for $n \geq 0$. ∎

Maximal Counter-Examples

The maximal counter-examples in (b) turn out to be just the first differences of the maximal counter-examples to Fine & Wilf.

For example, for $h = 5$, $k = 8$ we have

n	0	1	2	3	4	5	6	7	8	9	10	11	12
f_n	-1	1	-1	0	1	-1	1	-1	0	1	-1	1	-1
g_n	0	1	-1	0	1	-1	1	-1	0	1	-1	0	1

Formal Languages

Let Σ denote a finite nonempty set of symbols, called an alphabet.

Let Σ^* denote the set of all finite words over Σ.

For example, if $\Sigma = \{0, 1\}$, then

$$\Sigma^* = \{\epsilon, 0, 1, 00, 01, 10, 11, 000 \ldots\},$$

where ϵ is the empty word.

We write $|x|$ to denote the length of a word.

We write $|x|_a$ to denote the number of occurrences of the letter a in x.

Morphisms

A morphism is a map h from Σ^* to Δ^* such that
$$h(xy) = h(x)h(y)$$
for all words x, y.

It follows that h can be uniquely specified by providing its image on each letter of Σ.

For example, let
$$\begin{aligned} h(0) &= \mathtt{r} \\ h(1) &= \mathtt{em} \\ h(2) &= \mathtt{b} \\ h(3) &= \mathtt{er} \end{aligned}$$
Then
$$h(011233) = \mathtt{rememberer}.$$
If $\Sigma = \Delta$ we can iterate h. We write
$$\begin{array}{ll} h^2(x) & \text{for } h(h(x)), \\ h^3(x) & \text{for } h(h(h(x))), \\ & \text{etc.} \end{array}$$

Iterated Morphisms

Iterated morphisms appear in many different areas (often under the name L-systems), including

- models of plant growth in mathematical biology
- computer graphics

An Example from Biology

For example, consider the map φ defined by

$$\begin{aligned}\varphi(a_r) &= a_l b_r\\ \varphi(a_l) &= b_l a_r\\ \varphi(b_r) &= a_r\\ \varphi(b_l) &= a_l\end{aligned}$$

Iterating φ on a_r gives

$$\begin{aligned}\varphi^0(a_r) &= a_r\\ \varphi^1(a_r) &= a_l b_r\\ \varphi^2(a_r) &= b_l a_r a_r\\ \varphi^3(a_r) &= a_l a_l b_r a_l b_r\\ &\vdots\end{aligned}$$

Here the a's represent fat cells and the b's represent thin cells.

This models the development of the blue-green bacterium *Anabaena catenula*.

Iterated Morphisms and Computer Graphics

Szilard and Quinton [1979] observed that many interesting pictures, including approximations to fractals, could be coded using iterated morphisms.

A beautiful book by Prusinkiewicz and Lindenmayer provides many examples.

Iterated Morphisms and Computer Graphics

For example, we could code a picture using a "turtle graphics" model where R codes a move followed by a right turn, L codes a move followed by a left turn, and S codes a move straight ahead with no turn.

Consider the map g defined as follows:

$$\begin{aligned} g(R) &= RLLSRRLR \\ g(L) &= RLLSRRLL \\ g(S) &= RLLSRRLS \end{aligned}$$

By iterating g on $RRRR$ we get

$$\begin{aligned} g^0(R) &= RRRR \\ g^1(R) &= RLLSRRLRRLLSRRLRRLLS\cdots \\ g^2(R) &= RLLSRRLRRLLSRRLLRLLS\cdots \end{aligned}$$

These strings code successive approximations to a von Koch fractal curve.

The Matrix Associated with a Morphism

Given a morphism $\varphi : \Sigma^* \to \Sigma^*$ for some finite set $\Sigma = \{a_1, a_2, \ldots, a_d\}$, we define the *incidence matrix* $M = M(\varphi)$ as follows:

$$M = (m_{i,j})_{1 \le i,j \le d}$$

where $m_{i,j}$ is the number of occurrences of a_i in $\varphi(a_j)$, i.e., $m_{i,j} = |\varphi(a_j)|_{a_i}$.

Example. Consider the morphism φ defined by

$$\begin{aligned} \varphi : \mathtt{a} &\to \mathtt{ab} \\ \mathtt{b} &\to \mathtt{cc} \\ \mathtt{c} &\to \mathtt{bb}. \end{aligned}$$

Then

$$M(\varphi) = \begin{array}{c} \\ \mathtt{a} \\ \mathtt{b} \\ \mathtt{c} \end{array} \!\!\begin{array}{c} \begin{array}{ccc} \mathtt{a} & \mathtt{b} & \mathtt{c} \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 0 \end{bmatrix} \end{array}$$

The Matrix Associated with a Morphism

The matrix $M(\varphi)$ is useful because of the following proposition.

Proposition. We have

$$\begin{bmatrix} |\varphi(w)|_{a_1} \\ |\varphi(w)|_{a_2} \\ \vdots \\ |\varphi(w)|_{a_d} \end{bmatrix} = M(\varphi) \begin{bmatrix} |w|_{a_1} \\ |w|_{a_2} \\ \vdots \\ |w|_{a_d} \end{bmatrix}.$$

Proof. We have

$$|\varphi(w)|_{a_i} = \sum_{1 \le j \le d} |\varphi(a_j)|_{a_i} \, |w|_{a_j}.$$

∎

Corollary.

$$\begin{bmatrix} |\varphi^n(w)|_{a_1} \\ |\varphi^n(w)|_{a_2} \\ \vdots \\ |\varphi^n(w)|_{a_d} \end{bmatrix} = (M(\varphi))^n \begin{bmatrix} |w|_{a_1} \\ |w|_{a_2} \\ \vdots \\ |w|_{a_d} \end{bmatrix}$$

The Matrix Associated with a Morphism

Hence we find

Corollary.

$$|\varphi^n(w)| = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} M(\varphi)^n \begin{bmatrix} |w|_{a_1} \\ |w|_{a_2} \\ \vdots \\ |w|_{a_d} \end{bmatrix}.$$

The Length Sequence of an Iterated Morphism

We can now ask questions about the sequence of lengths

$$|x|,\ |h(x)|,\ |h^2(x)|,\ \ldots$$

These questions were very popular in mathematical biology (L-systems) in the 1980's.

For example, here is a classical result:

Theorem. Suppose $h : \Sigma^* \to \Sigma^*$ is a morphism, and suppose there exist a word $w \in \Sigma^*$ and a constant c such that

$$c = |w| = |h(w)| = \cdots = |h^n(w)|,$$

where $n = |\Sigma|$. Then $c = |h^i(w)|$ for all $i \geq 0$.

Proof of the Theorem

It suffices to show $|h^{n+1}(w)| = c$, because then the theorem follows by induction on n.

Let M be the incidence matrix of h. By the Cayley-Hamilton theorem,

$$M^n = c_0 M^0 + \cdots + c_{n-1} M^{n-1}$$

for some constants $c_0, c_1, \ldots, c_{n-1}$.

Define $f_i = |h^i(w)|$ and let

$$v = [|w|_{a_1}\ |w|_{a_2}\ \cdots\ |w|_{a_n}]^T.$$

Then for $0 \leq i < n$ we have

$$\begin{aligned}
f_{i+1} - f_i &= [1\ 1 \cdots 1](M^{i+1} - M^i)v \\
f_{i+1} - f_i &= [1\ 1 \cdots 1]M^i(M - I)v \\
&= [1\ 1 \cdots 1]M^i v' \\
&= 0,
\end{aligned}$$

where $v' := (M - I)v$.

Now

$$\begin{aligned} f_{n+1} - f_n &= [1\ 1 \cdots 1] M^n v' \\ &= [1\ 1 \cdots 1](c_0 + \cdots + c_{n-1} M^{n-1}) v' \\ &= \sum_{0 \le i < n} c_i [1\ 1 \cdots 1] M^i v' \\ &= 0, \end{aligned}$$

since each summand is 0. Hence $f_{n+1} = f_n$. ∎

Another Question

We might also ask, how long can the sequence of lengths

$$|x|,\ |h(x)|,\ |h^2(x)|,\ \ldots$$

strictly decrease?

This question arose naturally in a paper with Ming-wei Wang on the two-sided infinite fixed points of morphisms, i.e., those two-sided infinite words $\mathbf{w}$ such that $h(\mathbf{w}) = \mathbf{w}$.

The Length Sequence of an Iterated Morphism

If Σ has n elements, we can easily find a decreasing sequence of length n. For example, for $n = 5$, define h as follows:

$$\begin{aligned} h(\mathtt{a}) &= \mathtt{b} \\ h(\mathtt{b}) &= \mathtt{c} \\ h(\mathtt{c}) &= \mathtt{d} \\ h(\mathtt{d}) &= \mathtt{e} \\ h(\mathtt{e}) &= \epsilon \end{aligned}$$

Then we have

$$\begin{aligned} h(\mathtt{abcde}) &= \mathtt{bcde} \\ h^2(\mathtt{abcde}) &= \mathtt{cde} \\ h^3(\mathtt{abcde}) &= \mathtt{de} \\ h^4(\mathtt{abcde}) &= \mathtt{e} \\ h^5(\mathtt{abcde}) &= \epsilon \end{aligned}$$

so

$$\begin{aligned} |\mathtt{abcde}| &> |h(\mathtt{abcde})| > |h^2(\mathtt{abcde})| > |h^3(\mathtt{abcde})| \\ &> |h^4(\mathtt{abcde})| > |h^5(\mathtt{abcde})| = 0. \end{aligned}$$

The Decreasing Length Conjecture

Conjecture. If $h : \Sigma^* \to \Sigma^*$, and Σ has n elements, then

$$|w| > |h(w)| > \cdots > |h^k(w)|$$

implies that $k \leq n$.

Another way to state the Decreasing Length Conjecture is the following:

Conjecture. Let M be an $n \times n$ matrix of with non-negative integer entries. Let v be a column vector of non-negative integers, and let u be the row vector $[1\ 1\ 1\ \cdots\ 1]$. If

$$uv > uMv > uM^2v > \cdots > uM^kv$$

then $k \leq n$.

Path Algebra

There is a nice correspondence between directed graphs and non-negative matrices, as follows:

If G is a directed graph on n vertices, we can construct a non-negative matrix

$$M(G) = (m_{i,j})_{1 \leq i,j \leq n}$$

as follows: let

$$m_{i,j} = \begin{cases} 1, & \text{if there is a directed edge from} \\ & \text{vertex } i \text{ to vertex } j \text{ in } G; \\ 0, & \text{otherwise.} \end{cases}$$

Then the number of distinct walks of length n from vertex i to vertex j in G is just the i, j'th entry of M^n.

Similarly, given a non-negative $n \times n$ matrix $M = (m_{i,j})_{1 \leq i,j \leq n}$ we may form its associated graph $G(M)$ on n vertices, where we put a directed edge from vertex i to vertex j iff $m_{i,j} > 0$.

A Useful Lemma

Lemma. Let $r \geq 1$ be an integer, and suppose there exist r sequences of real numbers $\mathbf{b}_i = (b_i(n))_{n \geq 0}$, $1 \leq i \leq r$, and r positive integers $h_1, h_2, \ldots, h_r$, such that the following conditions hold:

(a) $b_i(n + h_i) \geq b_i(n)$ for $1 \leq i \leq r$ and $n \geq 0$;

(b) There exists an integer $D \geq 1$ such that $\sum_{1 \leq i \leq r} b_i(n) > \sum_{1 \leq i \leq r} b_i(n+1)$ for $0 \leq n < D$.

Then $D \leq h_1 + h_2 + \cdots + h_r - r$.

Proof of the Decreasing Length Conjecture

Theorem. Suppose M is an $n \times n$ matrix with non-negative integer entries. If there exist a row vector u and a column vector v with non-negative integer entries such that

$$uv > uMv > uM^2v > \cdots > uM^kv,$$

then $k \leq n$. Also $k = n$ only if $M^n = 0$.

Proof.

- Let M be the matrix in the statement of the theorem and G its associated graph.
- Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)^T$.
- Let V be the set of vertices in G.
- Consider some maximal set of vertices forming disjoint cycles $\{C_1, C_2, \ldots, C_r\}$ in G.
- Then V can be written as the disjoint union

  $$V = C_1 \ \cup \ C_2 \ \cup \ \cdots \ \cup \ C_r \ \cup \ W,$$

  where W is the set of vertices which do not lie in any of the disjoint cycles.

- Any directed walk in G of length $|W|$ or greater must intersect some cycle C_i, for otherwise the walk would contain a cycle disjoint from $C_1, C_2, \ldots, C_r$.
- Associate each walk of length $\geq |W|$ with the first cycle C_i it intersects.
- Define $P^s_{i,j,l}$ to be the number of directed walks of length s from vertex i to vertex j associated with cycle l.
- Also define
$$T^s_l := \sum_{1 \leq i,j \leq n} u_i v_j P^s_{ijl}.$$
- Then for any $s \geq |W|$ we have
$$uM^s w = \sum_{1 \leq l \leq r} T^s_l. \qquad (5)$$
- Then
$$T^s_l \leq T_l^{s+|C_l|},$$
since any walk of length s associated with cycle C_l can be extended to a walk of length $s + |C_l|$ by traversing the cycle C_l once.

- From the inequality $uM^s w > uM^{s+1} w$ for $0 \leq s \leq k-1$ and Eq. (5) we have

$$\sum_{1 \leq l \leq r} T_l^s > \sum_{1 \leq l \leq r} T_l^{s+1}$$

for $|W| \leq s < k$.

- Now for $1 \leq i \leq r$ and $j \geq 0$ define $b_i(j) = T_i^{|W|+j}$ and $h_i = |C_i|$.

- Then the conditions of the previous Lemma are satisfied.

- We conclude that

$$k - |W| \leq |C_1| + |C_2| + \cdots + |C_r| - r.$$

- Moreover

$$|C_1| + |C_2| + \cdots + |C_r| + |W| = |V| = n$$

and so $k \leq n - r$.

- Finally $k = n$ implies that $r = 0$, so G is acyclic and $M^n = 0$.

$\blacksquare$

For Further Reading

1. N. J. Fine and H. S. Wilf, Uniqueness theorems for periodic functions, *Proc. Amer. Math. Soc.* **16** (1965), 109–114.
2. J. Shallit and M.-w. Wang, On two-sided infinite fixed points of morphisms, in G. Ciobanu and G. Păun, eds., *Proc. FCT 1999 Conf.*, Lecture Notes in Computer Science #1684, Springer, 1999, pp. 488–499.
3. P. Prusinkiewicz and A. Lindenmayer, *The Algorithmic Beauty of Plants*, Springer-Verlag, 1990.