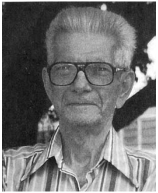 

Fifty Years of Fine and Wilf*

* Well, *almost* fifty years...

Jeffrey Shallit
School of Computer Science, University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
shallit@cs.uwaterloo.ca
http://www.cs.uwaterloo.ca/~shallit

Words

In this talk, I'll be speaking about *words*.

A word is a (possibly) empty string of symbols chosen from a finite nonempty alphabet Σ.

Σ^* is the set of all finite words.

ϵ is the empty word.

$|x|$ denotes the length of the word x, and $|x|_a$ is the number of occurrences of the symbol a in x.

x^k denotes the product $\overbrace{xxx\cdots x}^{k}$.

x^ω is the infinite word $xxx\cdots$.

If S is a set of words, then S^ω is the set of all infinite words constructed by concatenating elements of S.

Theorem

Let x, y be nonempty words. Then the following three conditions are equivalent:

(1) $xy = yx$;

(2) There exist a nonempty word z and integers $k, \ell > 0$ such that $x = z^k$ and $y = z^\ell$;

(3) There exist integers $i, j > 0$ such that $x^i = y^j$.

Note: for the implication (1) $\Rightarrow$ (2), an even weaker hypothesis suffices: we only need that xy agrees with yx on the first $|x| + |y| - \gcd(|x|, |y|)$ symbols.

Periodicity

We say an infinite 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 an infinite sequence that 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 Fine-Wilf Paper

- N. J. Fine and H. S. Wilf, "Uniqueness theorems for periodic functions"
- *Proc. Amer. Math. Soc.* **16** (1965), 109–114.
- Submitted August 7 1963, published 1965.
- The Fine-Wilf theorem: a version of the periodicity theorem for finite sequences.
- Answers the question: how long must the finite sequence $(f_n)_{0 \le n < D}$ be for period lengths h and k to imply a period of length $\gcd(h, k)$?
- $D = \mathrm{lcm}(h, k)$ works (of course!), but Fine and Wilf proved we can take $D = h + k - \gcd(h, k)$.

Theorem 1. Let $(f_n)_{n\geq 0}$ and $(g_n)_{n\geq 0}$ be two periodic sequences of period h and k, respectively. If $f_n = g_n$ for $h + k - \gcd(h, k)$ consecutive integers n, then $f_n = g_n$ for all n. The result would be false if $h + k - \gcd(h, k)$ were replaced by any smaller number.

Theorem 2. Let $f(x), g(x)$ be continuous periodic functions of periods α and β, respectively, where $\alpha/\beta = p/q$, $\gcd(p, q) = 1$. If $f(x) = g(x)$ on an interval of length $\alpha + \beta - \beta/q$, then $f = g$. The result would be false if $\alpha + \beta - \beta/q$ were replaced by any smaller number.

Theorem 3. Let $f(x), g(x)$ be continuous periodic functions of periods α and β, respectively, where α/β is irrational. If $f(x) = g(x)$ on an interval of length $\alpha + \beta$, then $f = g$. The result would be false if $\alpha + \beta$ were replaced by any smaller number.

Lyndon-Schützenberger meets Fine-Wilf

Theorem

Let w and x be nonempty words. Let $\mathbf{y} \in w\{w, x\}^\omega$ and $\mathbf{z} \in x\{w, x\}^\omega$. Then the following conditions are equivalent:

(a) $\mathbf{y}$ *and* $\mathbf{z}$ *agree on a prefix of length at least* $|w| + |x| - \gcd(|w|, |x|)$*;*

(b) $wx = xw$*;*

(c) $\mathbf{y} = \mathbf{z}$*.*

Proof.

(c) $\Rightarrow$ (a): Trivial.

(b) $\Rightarrow$ (c): By Lyndon-Schützenberger.

We'll prove (a) $\Rightarrow$ (b).

Proof.
(a) $\mathbf{y} \in w\{w,x\}^\omega$ and $\mathbf{z} \in x\{w,x\}^\omega$ agree on a prefix of length at least $|w| + |x| - \gcd(|w|,|x|) \implies$ (b) $wx = xw$:

We prove the contrapositive. Suppose $wx \neq xw$.

Then we prove that $\mathbf{y}$ and $\mathbf{z}$ differ at a position $\leq |w| + |x| - \gcd(|w|,|x|)$.

The proof is by induction on $|w| + |x|$.

Case 1: $|w| = |x|$ (which includes the base case $|w| + |x| = 2$). Then $\mathbf{y}$ and $\mathbf{z}$ must disagree at the $|w|$'th position or earlier, for otherwise $w = x$ and $wx = xw$; since
$|w| \leq |w| + |x| - \gcd(|w|,|x|) = |w|$, the result follows.

Fine-Wilf: The Proof

Case 2: WLOG $|w| < |x|$.

If w is not a prefix of x, then **y** and **z** disagree on the $|w|$'th position or earlier, and again $|w| \leq |w| + |x| - \gcd(|w|, |x|)$.

So w is a proper prefix of x.

Write $x = wt$ for some nonempty word t.

Now any common divisor of $|w|$ and $|x|$ must also divide $|x| - |w| = |t|$, and similarly any common divisor of both $|w|$ and $|t|$ must also divide $|w| + |t| = |x|$. So $\gcd(|w|, |x|) = \gcd(|w|, |t|)$.

Fine-Wilf: The Proof

Now $wt \neq tw$, for otherwise we have $wx = wwt = wtw = xw$, a contradiction.

Then $\mathbf{y} = ww \cdots \in ww\{w, t\}^\omega$ and $\mathbf{z} = x \cdots = wt \cdots \in wt\{w, t\}^\omega$. By induction (since $|wt| < |wx|$), $w^{-1}\mathbf{y}$ and $w^{-1}\mathbf{z}$ disagree at position $|w| + |t| - \gcd(|w|, |t|)$ or earlier.

Hence $\mathbf{y}$ and $\mathbf{z}$ disagree at position $2|w| + |t| - \gcd(|w|, |t|) = |w| + |x| - \gcd(|w|, |x|)$ or earlier. We're done. ■

Finite Sturmian words

The proof also implies a way to get words that optimally "almost commute", in the sense that xw and wx should agree on as long a segment as possible.

Theorem

For each $m, n \geq 1$ there exist binary words x, w of length m, n, respectively, such that xw and wx agree on a prefix of length $m + n - \gcd(m, n) - 1$ but differ at position $m + n - \gcd(m, n)$.

Indeed, our proof even provides an algorithm for computing these words:

$$S(h,k) = \begin{cases} (0^h, 0^{h-1}1), & \text{if } h = k \text{ ;} \\ (x, w), & \text{if } h > k \text{ and } S(k,h) = (w,x) \text{ ;} \\ (w, wt), & \text{if } h < k \text{ and } S(h, k-h) = (w,t) \text{ .} \end{cases}$$

These words are the finite *Sturmian words*.

Since 1965

Since 1965, research on Fine-Wilf has been in three areas:

- applications (esp. to string-searching algorithms such as Knuth-Morris-Pratt)
- generalizations (esp. to more than 2 numbers; partial words)
- variations (e.g., to abelian periods; to inequalities)

Citation history

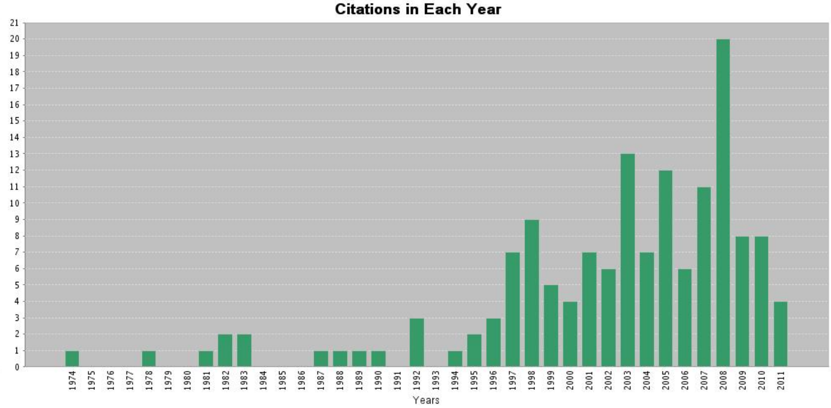

Figure: Citations of Fine-Wilf, according to Web of Science

Fine-Wilf and String Searching

The famous linear-time string searching algorithm of Knuth-Morris-Pratt finds all occurrences of a pattern p in a text t in time bounded by $O(|p| + |t|)$.

It compares the pattern to a portion of the text beginning at position i, and, when a mismatch is found, shifts the pattern to the right based on the position of the mismatch.

The worst-case in their algorithm comes from "almost-periodic" words, where long sequences of matching characters occur without a complete match.

It turns out that such words are precisely the maximal "counterexamples" in the Fine-Wilf theorem (the Sturmian pairs).

Multiple Periods

Many authors have worked on generalizations to multiple periods: Castelli, Mignosi, & Restivo (1999); Justin (2000); Constantinescu & Ilie (2003, 2005); Holub (2006), Tijdeman & Zamboni (2003, 2009), ...

For example, Castelli, Mignosi, and Restivo (1999) proved that for three periods $p_1 \leq p_2 \leq p_3$ the appropriate bound is

$$\frac{1}{2}(p_1 + p_2 + p_3 - 2\gcd(p_1, p_2, p_3) + h(p_1, p_2, p_3))$$

where h is a function related to the Euclidean algorithm on three inputs.

Partial words

Here we have words together with "don't care" symbols called "holes". Holes match each other and all other symbols.

Theorem

There exists a computable function $L(h, p, q)$ such that if a word w with h holes with periods p and q is of length $\geq L(h, p, q)$, then w also has period $\gcd(p, q)$.

Berstel and Boasson (1999) proved we can take $L(1, p, q) = p + q$.

Shur and Konovalova (2004) proved we can take $L(2, p, q) = 2p + q - \gcd(p, q)$.

Many results by Blanchet-Sadri and co-authors.

Variations on Fine & Wilf

Fine & Wilf works for equalities. How about inequalities?

For example, suppose $\mathbf{f} = (f_n)_{n \geq 0}$, $\mathbf{g} = (g_n)_{n \geq 0}$ are two periodic sequences of period h and k, respectively. Suppose $f_n \leq g_n$ for a prefix of length D. We want to conclude that $f_n \leq g_n$ everywhere.

Here the correct bound is $D = \mathrm{lcm}(h, k)$. Example: take

$$\begin{aligned} \mathbf{f} &= (1^{h-1}2)^\omega \\ \mathbf{g} &= (2^{k-1}1)^\omega \end{aligned}$$

Then $f_n \leq g_n$ for $0 \leq n < \mathrm{lcm}(h, k) - 1$, but the inequality fails at $n = \mathrm{lcm}(h, k) - 1$.

So, to get a Fine-Wilf style bound, we need some additional hypothesis.

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 $f_n = g_n$ for all $n \geq 0$.

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

Sketch of Proof, Part (a)

Define

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

By hypothesis $P \circ \mathbf{f} \geq 0$, where by $\circ$ we mean the infinite sequence obtained by taking the dot product of the coefficients of P with 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

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

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

Maximal counter-examples in (b) can be deduced as the first differences of the maximal counter-examples to Fine & Wilf (the Sturmian pairs).

For example, for $h = 5$, $k = 8$ we have $w = (-1, 1, -1, 0, 1)$ and $x = (0, 1, -1, 0, 1, -1, 1, -1)$. Then

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

Another variation

Suppose we have two periodic sequences of integers, say $(f_n)_{n\geq 0}$ of period h and $(g_n)_{n\geq 0}$ of period k. For how many consecutive terms can $f_n + g_n$ strictly decrease?

The answer, once again, is $h + k - \gcd(h, k)$.

Here is an example achieving $h + k - 1$ for $h = 5, k = 8$:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$f(n)$	0	-16	8	-8	-24	0	-16	8	-8	-24	0	-16	8
$g(n)$	0	15	-10	5	20	-5	10	-15	0	15	-10	5	20
$f+g$	0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	28

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

$$\begin{aligned} h(0) &= \texttt{r} \\ h(1) &= \texttt{em} \\ h(2) &= \texttt{b} \\ h(3) &= \texttt{er} \end{aligned}$$

Then

$$h(011233) = \texttt{rememberer}.$$

Iterated morphisms

If $\Sigma = \Delta$ we can iterate h. We write

$$\begin{array}{ccc} h^2(x) & \text{for} & h(h(x)), \\ h^3(x) & \text{for} & h(h(h(x))), \\ & \text{etc.} & \end{array}$$

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
- infinite words avoiding certain patterns

An Example from Biology

For example, consider the map φ defined by

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

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*.

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

Example: code a picture using "turtle graphics" 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 morphism g defined as follows:

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

By iterating g on $RRRR$ we get

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

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

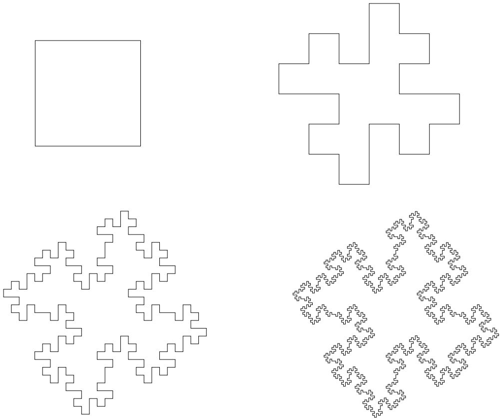

Figure: Four iterations in the construction of the von Koch curve

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 $i \geq 0$.

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

$$\varphi : \mathtt{a} \to \mathtt{ab}, \qquad \mathtt{b} \to \mathtt{cc} \qquad \mathtt{c} \to \mathtt{bb}.$$

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

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

∎

The Matrix Associated with a Morphism

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.

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

So questions about $|\varphi^n(w)|$ reduce to questions about $M(\varphi)^n$.

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 Wang characterizing 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:

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

Then we have

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

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

A Theorem on Non-Negative Matrices

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 (sketch).

- Let M be the matrix in the statement of the theorem.
- Form its associated directed graph G by putting $M_{i,j}$ edges from vertex i to vertex j.
- Decompose G into disjoint cycles and a leftover vertex set.
- Associate each sufficiently long walk in G with the first cycle it intersects.

Proof of the Theorem (continued)

- Define $P^s_{i,j,\ell}$ to be the number of directed walks of length s from vertex i to vertex j associated with cycle ℓ.
- Also define
$$T^s_\ell := \sum_{1\le i,j\le n} u_i \cdot P^s_{i,j,\ell} \cdot v_j.$$
- Then for any s large enough we have we have
$$uM^s v = \sum_\ell T^s_\ell. \tag{5}$$
- Now apply a Fine-Wilf style lemma.

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 $\sum_{1 \leq i \leq r} b_i(n+1) < \sum_{1 \leq i \leq r} b_i(n)$ for $0 \leq n < D$.

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

Fine and Wilf forever

- The Fine-Wilf paper continues to find many applications in combinatorics on words, equations in words, string matching, etc.
- No end in sight...
- Congratulations to Herb Wilf on his 80th birthday!

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, *Theoret. Comput. Sci.* **270** (2002), 659–675.
3. P. Prusinkiewicz and A. Lindenmayer, *The Algorithmic Beauty of Plants*, Springer-Verlag, 1990.
4. S. Cautis, F. Mignosi, J. Shallit, M.-w. Wang, S. Yazdani, Periodicity, morphisms, and matrices, *Theoret. Comput. Sci.* **295** (2003), 107–121.