Morphisms, Matrices, and Periodicity

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

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

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

Then

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

Iterated Morphisms

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

$$h^2(x) \text{ for } h(h(x)),$$
$$h^3(x) \text{ for } h(h(h(x))),$$
$$\text{etc.}$$

We can then ask about the sequence of lengths

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

In particular, how long can it 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 $h(\mathbf{w}) = \mathbf{w}$.

Iterated Morphisms

If Σ has n elements, we can easily find a decreasing sequence of length n. 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 $k \leq n$.

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

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

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.

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

Thus 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

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

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

Path Algebra

There is a notion in the literature on non-negative matrices called *irreducibility*.

Definition. An $n \times n$ non-negative matrix

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

is said to be *irreducible* if for all i, j with $1 \leq i, j \leq n$ there exists a power of M, say M^e, such that the entry in row i and column j is > 0.

From our observation above we see that a non-negative matrix is irreducible iff its associated graph $G(M)$ is strongly connected.

A Result That is Both Stronger and Weaker

One way we can have $uM^iv \leq uM^jv$ is if $M^i \leq M^j$.

Theorem. Let M be an $n \times n$ matrix with non-negative integer entries. Then there exist integers r, s with $0 \leq r < s \leq 2^n$ such that $M^r \leq M^s$.

Proof. First, we need some facts about irreducible matrices.

Decomposition Theorem. If M is *reducible*, then there exists a permutation matrix P such that

$$P^TMP = \begin{bmatrix} M_{11} & 0 & \cdots & 0 \\ M_{21} & M_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{t1} & M_{t2} & \cdots & M_{tt} \end{bmatrix}$$

where the diagonal blocks $M_{11}, M_{22}, \cdots, M_{tt}$ are square matrices that are either irreducible or equal to $[0]$, the 1×1 zero matrix.

The Diagonal Lemma

For an irreducible matrix M, let $\delta(M)$ be the least integer $e \geq 1$ such that $\operatorname{diag}(M^e) > 0$.

For an integer $n \geq 1$, define $\delta(n) = \sup \delta(M)$, where the supremum is over all irreducible $n \times n$ matrices M.

Diagonal Lemma. Let the function f be defined as follows:

$$f(n) = \begin{cases} 1, & \text{if } n = 1; \\ n(n-1), & \text{if } n > 1. \end{cases}$$

Then $\delta(n) \leq f(n)$.

Proof. The result is clearly true for $n = 1$, so assume $n \geq 2$.

Consider the associated graph $G(M)$.

The Diagonal Lemma

Construct a Hamiltonian walk (i.e., a closed walk through the graph, possibly repeating vertices and edges, that visits every vertex at least once) as follows: start at any vertex v_1, and choose a path from v_1 to v_2. Such a path exists because $G(M)$ is strongly connected, and is clearly of length $\leq n-1$ (where length is the number of edges traversed). Choose a path from v_2 to v_3, etc. Continue until the last vertex v_n is reached, and now choose a path back to v_1. Clearly the total length of this walk is $e \leq n(n-1)$. Then for each vertex v_i, there exists a walk of length exactly e from v_i back to itself. Thus by path algebra we have $\mathrm{diag}(M^e) > 0$. ∎

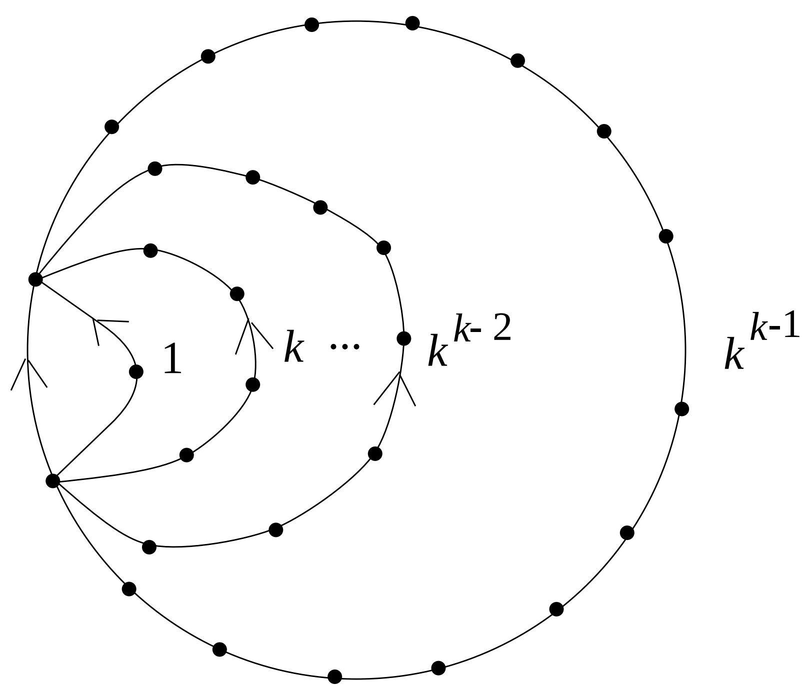
The Diagonal Function $\delta(n)$

Remark. The upper bound $\delta(n) \leq n(n-1)$ in the Diagonal Lemma is not sharp. It has recently been improved by Bo to

$$\delta(n) \leq \frac{n^2 - 2n + 4}{2}.$$

Lower Bounds:

It's possible to construct an infinite family of examples for which $\delta(n) \sim n(\log n)(\log \log n)^{-1}$. This is based on an idea of Jim Geelen.



The Diagonal Function $\delta(n)$

Let $N = k^{k-1}$. Create a graph G with a directed cycle on N vertices, and between two vertices of this cycle put bypasses with 1, k, k^2, $\ldots$, k^{k-2} vertices.

The total number of vertices is

$$n := k^{k-1} + \sum_{0 \leq i \leq k-2} k^i < 2N,$$

but

$$\delta(G) = k^k + \sum_{0 \leq i \leq k-2} k^i$$

$$> N(\log N)/(\log \log N).$$

It would be of great interest to determine more precise upper and lower bounds for $\delta(n)$.

A Result That is Both Stronger and Weaker

Theorem. Let M be an $n \times n$ matrix with non-negative integer entries. Then there exist integers r, s with $0 \leq r < s \leq 2^n$ such that $M^r \leq M^s$.

Proof. By induction on n.

For $n = 1$, if $M = [x]$ with $x \geq 1$, then clearly $M^0 = I \leq M$, while if $M = [0]$ then $M = M^2 = [0]$.

Now assume $n \geq 2$ and the result has been proved for all $n' < n$.

There are two cases to consider: (1) M is irreducible and (2) M is reducible.

Case 1: M is irreducible. By the Diagonal Lemma, there exists an integer e, $1 \leq e \leq n(n-1)$, such that $\mathrm{diag}(M^e) > 0$. Thus $I = M^0 \leq M^e$. Since $n \geq 2$, we have $e \leq n(n-1) \leq 2^n$.

Case 2: M is reducible. By the Decomposition Theorem we may assume that, up to permuting the entries of M that

$$M = \begin{bmatrix} M_{11} & 0 & \cdots & 0 \\ M_{21} & M_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{t1} & M_{t2} & \cdots & M_{tt} \end{bmatrix} \tag{1}$$

where $M_{11}, M_{22}, \ldots, M_{tt}$ are square matrices that are either $[0]$ or irreducible. There are now two cases to consider, based on the form of M_{tt}.

Case 2a: $M_{tt} = [0]$. Then the last column of M is 0. Letting $B = M'$, we can write

$$M = \left[\begin{array}{c|c} B & 0 \\ \hline x & 0 \end{array}\right]$$

where x is a vector of dimension $n-1$. An easy induction gives

$$M^i = \left[\begin{array}{c|c} B^i & 0 \\ \hline xB^{i-1} & 0 \end{array}\right] \tag{2}$$

for all integers $i \geq 1$.

Since B is of dimension $(n-1) \times (n-1)$, by induction there exist integers r, s with $0 \leq r < s \leq 2^{n-1}$ such that

$$B^r \leq B^s.$$

Hence, using (2), we find

$$M^{r+1} = \left[\begin{array}{c|c} B^{r+1} & 0 \\ \hline xB^r & 0 \end{array}\right] \leq \left[\begin{array}{c|c} B^{s+1} & 0 \\ \hline xB^s & 0 \end{array}\right] = M^{s+1},$$

and $1 \leq r+1 < s+1 \leq 2^{n-1} + 1 \leq 2^n$.

Case 2b: M_{tt} is irreducible. Let $k = \dim M_{tt}$. Then $1 \leq k < n$. By the Diagonal Lemma, there exists an integer e, with $1 \leq e \leq f(k)$, such that $M_{tt}^e \geq I$. But it is easy to see that $f(k) \leq 2^k$ for all $k \geq 1$, so $1 \leq e \leq 2^k$.

Let

$$B = \begin{bmatrix} M_{11} & 0 & \cdots & 0 \\ M_{21} & M_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{t-1,1} & M_{t-1,2} & \cdots & M_{t-1,t-1} \end{bmatrix}$$

so that

$$M = \left[\begin{array}{c|c} B & 0 \\ \hline C & M_{tt} \end{array}\right].$$

By induction applied to B^e we know there exist r, s with $0 \leq r < s \leq 2^{n-k}$ such that

$$(B^e)^r \leq (B^e)^s.$$

From above we have

$$M^e = \left[\begin{array}{c|c} B^e & 0 \\ \hline \hat{C} & M_{tt}^e \end{array}\right]$$

for some $\hat{C}$. It is not hard to see that

$$(M^e)^r \leq (M^e)^s,$$

and $0 \leq er < es \leq 2^k 2^{n-k} = 2^n$. The proof is complete. ∎

Remark. BO has recently improved the upper bound from 2^n to $3^{n/2}$.

The Function $\alpha(n)$

For a non-negative $n \times n$ integer matrix M, define $\alpha(M)$ to be the least positive integer j such that there exists an integer i with $0 \le i < j$ such that $M^i \le M^j$. Define $\alpha(n) = \sup \alpha(M)$, where the supremum is over all non-negative integer matrices M. Then the previous Theorem can be rephrased as the inequality $\alpha(n) \le 2^n$.

Theorem. For all $n \ge 906$, we have $\alpha(n) \ge e^{\sqrt{n \log n}}$.

Proof. Define $C_n = (c_{i,j})_{1 \le i,j \le n}$ to be the $n \times n$ permutation matrix given by $c_{i,i+1} = 1$ for $1 \le i < n$, $c_{n,1} = 1$, and all other entries 0. Then the inequality $C_n^i \le C_n^j$ does not hold for $0 \le i < j < n$, for the entry in row 1 and column $i+1$ of C_n^i is 1, while the corresponding entry in C_n^j is 0. On the other hand, $C_n^n = I$, the identity. Hence $\alpha(C_n) = n$.

Suppose we are given a partition of the integer n, i.e., an expression of the form $n = n_1 + n_2 + \cdots + n_k$, where each of the n_i is a positive integer. Form the $n \times n$ matrix $M = M(n_1, n_2, \cdots, n_k)$ where the matrices C_{n_i} are arranged along the diagonal, i.e.,

$$M = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_k}.$$

As above, $\alpha(M) = \mathrm{lcm}(n_1, n_2, \ldots, n_k)$. Thus, to provide a lower bound on $\alpha(n)$, it suffices to estimate $g(n) := \max\ \mathrm{lcm}(n_1, n_2, \ldots, n_k)$, where the maximum is over all partitions of n.

Luckily this function $g(n)$ has been studied extensively, starting with LANDAU [1903], who showed that $\log g(n) \sim \sqrt{n \log n}$. It is known (MASSIAS, NICOLAS, and ROBIN [1989]) that

$$g(n) \geq e^{\sqrt{n \log n}}$$

for $n \geq 906$. This completes the proof of the lower bound. ∎

A Special Case of the Decreasing Length Conjecture

If we cannot yet prove the Decreasing Length Conjecture as stated, how about a special case?

Consider the case where each letter is purely periodic, that is, there exists $r \geq 1$ such that the sequence defined by

$$f_i = |h^i(a)|$$

satisfies $f_{i+r} = f_i$ for all $i \geq 0$.

Note that for any periodic sequence $(f_i)_{i\geq 0}$ of positive integers, say of period r, we can create a morphism on $r+1$ letters

$$\{a_0, a_1, \ldots , a_{r-1}, e\}$$

whose length sequence coincides with $(f_i)_{i\geq 0}$, as follows:

$$\begin{aligned} h(a_0) &= a_1 e^{f_1 - 1} \\ h(a_1) &= a_2 e^{f_2 - 1} \\ &\vdots \\ h(a_{r-1}) &= a_0 e^{f_0 - 1} \end{aligned}$$

where $h(e) = \epsilon$. Then

$$f_i = |h^i(a_0 e^{f_0 - 1})|$$

for all $i \geq 0$.

We are then interested in studying for how many terms the sum of two or more periodic sequences can strictly decrease.

By taking first differences, we are interested in studying for how many terms the sum of two or more periodic sequences whose periods sum to 0 can be strictly negative (or strictly positive).

This leads to considering analogues of the FINE and WILF theorem.

The Fine and Wilf Theorem

In 1965, Fine and Wilf proved

Theorem. Let $(f_n)_{n\geq 0}$, $(g_n)_{n\geq 0}$ be two periodic sequences, of periods 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 (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:

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

For example:

$$\begin{aligned} \sigma(6,10) &= 0001000001 \\ \sigma(10,6) &= 000100 \end{aligned}$$

The Fine and Wilf Theorem

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.

In the case of our example, where $h = 10$, $k = 6$:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f_i	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0
g_i	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0

Recently Mignosi and JOS proved the following analogue:

An Analogue of the Fine and Wilf Theorem

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

$$\sum_{0\leq i<h} f_i = \sum_{0\leq j<k} g_j = 0.$$

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

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

Proof Sketch (by M.-w. Wang)

Any periodic sequence $(b_n)_{n\geq 0}$ of period p can be written in the form

$$b_n = \sum_{\substack{\omega \\ \omega^p=1}} c_\omega \, \omega^n.$$

Thus there are constants c_i and d_j such that

$$f_n = \sum_{0\leq i<h} c_i \omega_h^{in};$$
$$g_n = \sum_{0\leq j<k} d_j \omega_k^{jn};$$

where ω_p is a p'th root of unity.

Let

$$\begin{aligned} r &= [r_1, r_2, \ldots, r_m] \\ &= [1, \omega_h, \omega_h^2, \ldots, \omega_h^{h-1}, 1, \omega_k, \omega_k^2, \ldots, \omega_k^{k-1}], \end{aligned}$$

where $m = h + k$.

Proof Sketch

Let $B = h+k-\gcd(h,k)$, and define a $B \times m$ matrix $T = (t_{i,j})$ by

$$t_{i,j} = r_j^i$$

for $0 \le i < B$, $1 \le j \le m$. Define a column vector

$$v = [c_0, c_1, \ldots, c_{h-1}, d_0, d_1, \ldots, d_{k-1}]^T.$$

Then the hypothesis of the theorem states that $Tv \le 0$, and the desired conclusion is $Tv = 0$.

Some of the elements of r will appear more than once in r, and hence some of the columns of T are identical. Let T' be the matrix obtained from T by deleting the extra identical columns. Then T' is a $B \times B$ matrix.

Proof Sketch

Let T'' be the $B\times(B-1)$ matrix obtained from T' by deleting the single column of 1's. Define

$$y(X) = \frac{(X^h - 1)(X^k - 1)}{(X^{\gcd(h,k)} - 1)(X - 1)}$$
$$= \sum_{0\le i<B} a_i X^i.$$

It can be shown that the coefficients a_i of y are all strictly positive. Furthermore, if we let

$$z = [a_0\ a_1\ a_2\ \cdots\ a_{B-1}],$$

then it is easy to see that $zT'' = 0$.

Suppose there exists a column vector v such that $Tv \le 0$ but $Tv \ne 0$. Then it is easy to see that there exists v'' such that $T''v'' \le 0$ but $T''v'' \ne 0$. But since z is strictly positive we would have $zT''v'' \le 0$ and $zT''v'' \ne 0$. But $zT'' = 0$, a contradiction. ∎

Back to the Decreasing Length Conjecture

Using this technique generalized to k sequences, we can prove the Decreasing Length Conjecture in the case where all letters are purely periodic.

For Further Reading

1. Z. Bo, Improvements on inequalities for non-negative matrices, *Australasian J. Combinat.* **21** (2000), 251–255.

2. N. J. Fine and H. S. Wilf, Uniqueness theorems for periodic functions, *Proc. Amer. Math. Soc.* **16** (1965), 109–114.

3. 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.

4. J. Shallit and M.-w. Wang, An inequality for non-negative matrices, *Linear Alg. Appl.* **290** (1999), 135–144.