Fife's Theorem Revisited

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

Overlaps

An *overlap* is a word of the form *axaxa*, where *a* is a single letter and *x* is a possibly empty word.

Thus, an overlap is just slightly more than a square.

An example in English is `alfalfa`.

An example in French is `entente`.

An example in German is `endende`.

An example in Italian is `intinti`.

Thue and overlap-free words

Axel Thue proved that the Thue-Morse word

$$\mathbf{t} = (t_n)_{n \geq 0} = 0110100110010110 \cdots$$

is overlap-free: it contains no overlaps.

Here t_n is the parity of the number of 1's in the base-2 expansion of n.

The Thue-Morse word can also be viewed in another way: as the fixed point of the Thue-Morse morphism μ sending $0 \to 01$, $1 \to 10$.

Other overlap-free words

However, $\mathbf{t}$ is not the only binary overlap-free infinite word.

For example, consider the sequence where we count the parity of the number of 0's in the base-2 expansion of n:

$$\mathbf{h} = 0010011010010110011010011001011010010110011010 \cdots ;$$

it is also overlap-free.

Can we somehow characterize all overlap-free binary words?

A fragility result

Brown, Rampersad, JOS, and Vasiga (2006) showed:

Theorem. If we flip the bits in any finite nonempty set of positions of $\mathbf{t}$, the result has an overlap.

Is there a version of this theorem for other overlap-free infinite words?

Not as stated - since, for example, both $0\mathbf{t}$ and $1\mathbf{t}$ are both overlap-free.

A fragility conjecture

Conjecture. For every overlap-free word **x** there exists a constant C (depending on **x**) such that if we flip the bits in any nonempty set of positions $> C$, then the result has an overlap.

The work of Earl Fife

A description of all overlap-free words was given by Earl Fife in 1980.

He defined

$$X = \{\mu(0), \mu(1), \mu^2(0), \mu^2(1), \ldots\}$$

and a *canonical decomposition* for words ending in 01 or 10 as follows:

$$w = z\, y\, \overline{y}$$

where y is the longest word in X such that $y\,\overline{y}$ is a suffix of w. Here $\overline{y}$ is the complementary word to y, obtained by sending $0 \to 1$ and $1 \to 0$.

Example: the canonical decomposition of 001001101001 is

$$0010 \quad 0110 \quad 1001.$$

The work of Earl Fife

Fife defined three maps based on the canonical decomposition $w = z\,y\,\overline{y}$:

$$\alpha(w) = w\,y\,y\,\overline{y}$$
$$\beta(w) = w\,y\,\overline{y}\,\overline{y}\,y$$
$$\gamma(w) = w\,\overline{y}\,y$$

Fife proved that every infinite overlap-free word has a unique description of the form $\mathbf{x}(01)$, $\mathbf{x}(001)$, $\mathbf{x}(10)$, or $\mathbf{x}(110)$, where $\mathbf{x}$ is an infinite word over the alphabet α, β, γ satisfying certain properties.

These properties amount to specifying a finite automaton accepting the set of valid words.

Deficiencies of Fife's theory

- finite words need to be examined at the end, not the beginning, to determine their canonical decomposition
- one needs to look at arbitrarily large factors of a word to determine its canonical decomposition
- the transformations α, β, γ are unmotivated and appear out of nowhere
- verifying the automaton is complicated
- not clear how to extend this to other kinds of repetitions

An alternative: the decomposition of Restivo-Salemi

Restivo and Salemi (1985) discovered an alternative decomposition for finite binary overlap-free words.

Theorem.
Every finite binary overlap-free word w can be written uniquely in the form $x\mu(y)z$, where y is overlap-free, and $x, z \in \{\epsilon, 0, 00, 1, 11\}$.

Furthermore, if $|w| \geq 7$, then this decomposition is unique.

An alternative: the decomposition of Restivo-Salemi

The Restivo-Salemi decomposition was extended to infinite binary overlap-free words by Allouche, Currie, and JOS (1998).

Theorem.
Every infinite binary overlap-free word $\mathbf{w}$ can be written uniquely in the form

$$\mathbf{w} = x\,\mu(\mathbf{y})$$

where $x \in \{\epsilon, 0, 1, 00, 11\}$ and $\mathbf{y}$ is overlap-free.

Furthermore, the correct decomposition can be deduced by examining the first 5 symbols of $\mathbf{w}$.

Iterating the Restivo-Salemi decomposition

The Restivo-Salemi decomposition can be iterated:

$$\begin{aligned}\mathbf{w} &= x_1\ \mu(\mathbf{y}_1) \\ &= x_1\ \mu(x_2)\ \mu^2(\mathbf{y}_2) \\ &= x_1\ \mu(x_2)\ \mu^2(x_3)\ \mu^3(\mathbf{y}_3) = \cdots\end{aligned}$$

If the sequence of x_i contains infinitely many nonempty words, then this gives the decomposition

$$\mathbf{w} = x_1\ \mu(x_2)\ \mu^2(x_3)\ \cdots .$$

Otherwise, we get

$$\mathbf{w} = x_1\ \mu(x_2)\ \mu^2(x_3)\ \cdots\ \mu^i(x_{i+1})\ \mu^\omega(a)$$

for $a \in \{0, 1\}$.

Further, this decomposition is unique.

Iterating the Restivo-Salemi decomposition

So we can specify an infinite binary overlap-free word by providing

(i) the infinite sequence of x_i, or

(ii) the finite sequence of x_i (which is followed by 0^ω) and a.

We encode the permissible x_i as follows:

$$
\begin{aligned}
p_0 &= \epsilon \\
p_1 &= 0 \\
p_2 &= 00 \\
p_3 &= 1 \\
p_4 &= 11
\end{aligned}
$$

An example of the iterated decomposition

Let's start with

$\mathbf{h} = 0010011010010110011010011001011010010110011010 01\cdots$,

the word counting the number of 0's (mod 2) in the binary expansion of n. Then

$$\begin{aligned}
\mathbf{h} &= 00\,\mu(10110010110100110010110011010010110 1001\cdots) \\
&= 00\,\mu(1)\,\mu(\mu(0100110100101100110100110010 11010\cdots)) \\
&= 00\,\mu(1)\,\mu(\mu(0))\,\mu(\mu(\mu(101100101101001100101100 1\cdots))) \\
&= 00\,\mu(1)\,\mu^2(0)\,\mu^3(1)\,\mu^4(0)\cdots \\
&= p_2\,\mu(p_3)\,\mu^2(p_1)\,\mu^3(p_3)\,\mu^4(p_1)\cdots .
\end{aligned}$$

So $\mathbf{h}$ is encoded by the sequence of indices $2313131\cdots = 2(31)^\omega$.

Valid decomposition sequences

However, not every sequence of x_i gives an infinite overlap-free word.

For example, if $x_1 = 00$, then $x_2 \neq 0$, for otherwise $\mathbf{w}$ begins $00\mu(0) = 0001$, which has an overlap.

Can we somehow characterize the "legal" sequences of x_i that give the overlap-free infinite words?

Yes, using a finite automaton.

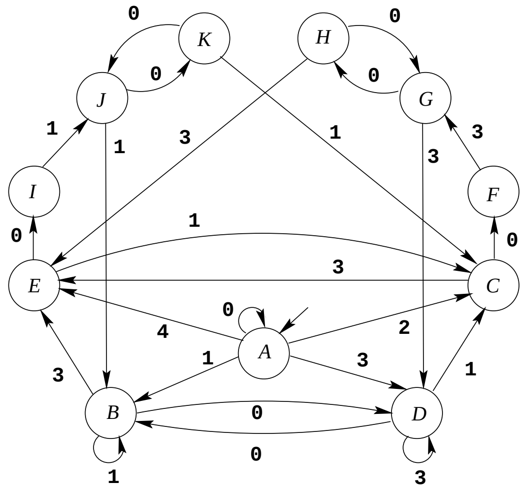
The automaton

Let $\mathcal{O}$ denote the set of all infinite overlap-free words.
States of the automaton represent subsets of $\mathcal{O}$, as follows:

$$
\begin{aligned}
A &= \mathcal{O} \\
B &= \{\mathbf{x} \in \Sigma^\omega \;:\; 1\mathbf{x} \in \mathcal{O}\} \\
C &= \{\mathbf{x} \in \Sigma^\omega \;:\; 1\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 101\} \\
D &= \{\mathbf{x} \in \Sigma^\omega \;:\; 0\mathbf{x} \in \mathcal{O}\} \\
E &= \{\mathbf{x} \in \Sigma^\omega \;:\; 0\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 010\} \\
F &= \{\mathbf{x} \in \Sigma^\omega \;:\; 0\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 11\} \\
G &= \{\mathbf{x} \in \Sigma^\omega \;:\; 0\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 1\} \\
H &= \{\mathbf{x} \in \Sigma^\omega \;:\; 1\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 1\} \\
I &= \{\mathbf{x} \in \Sigma^\omega \;:\; 1\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 00\} \\
J &= \{\mathbf{x} \in \Sigma^\omega \;:\; 1\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 0\} \\
K &= \{\mathbf{x} \in \Sigma^\omega \;:\; 0\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 0\}
\end{aligned}
$$

We connect states as follows: an arrow from state S to state T is labeled i means

$$\mathbf{w} \in T \iff p_i\, \mu(\mathbf{w}) \in S.$$



The main result

Theorem.
Every infinite binary overlap-free word $\mathbf{x}$ is encoded by an infinite path, starting in state A, through the automaton.

Every infinite path through the automaton not ending in 0^ω codes a unique infinite binary overlap-free word $\mathbf{x}$. If a path $\mathbf{i}$ ends in 0^ω and this suffix corresponds to a cycle on state A or a cycle between states B and D, then $\mathbf{x}$ is coded by either $\mathbf{i}; 0$ or $\mathbf{i}; 1$. If a path $\mathbf{i}$ ends in 0^ω and this suffix corresponds to a cycle between states J and K, then $\mathbf{x}$ is coded by $\mathbf{i}; 0$. If a path $\mathbf{i}$ ends in 0^ω and this suffix corresponds to a cycle between states G and H, then $\mathbf{x}$ is coded by $\mathbf{i}; 1$.

Proof of the main theorem

The assertions encoded by the automaton follow easily from the following

Lemma.
Let $a \in \Sigma$. Then

(a) $\mathbf{x} \in \mathcal{O} \iff \mu(\mathbf{x}) \in \mathcal{O}$;

(b) $a\,\mu(\mathbf{x}) \in \mathcal{O} \iff \overline{a}\,\mathbf{x} \in \mathcal{O}$;

(c) $a\,a\,\mu(\mathbf{x}) \in \mathcal{O} \iff \overline{a}\,\mathbf{x} \in \mathcal{O}$ and $\mathbf{x}$ begins $\overline{a}\,a\,\overline{a}$.

Proof of Lemma not very hard: see Allouche, JOS, Currie, *Elect. J. Combinatorics* **5** (1998), #R27.

Verifying the assertions

Let's verify the transition $\delta(I, 1) = J$.

From the correspondence given before we need to check that

$$p_1\mu(\mathbf{x}) \in I \quad \iff \quad \mathbf{x} \in J.$$

But $p_1 = 0$, so we need to verify

$$0\mu(\mathbf{x}) \in I \quad \iff \quad \mathbf{x} \in J.$$

Verifying the assertions

Let's verify

$$0\mu(\mathbf{x}) \in I \quad \Longleftrightarrow \quad \mathbf{x} \in J.$$

Recall that

$$\begin{aligned} I &= \{\mathbf{w} \in \Sigma^\omega : 1\mathbf{w} \in \mathcal{O} \text{ and } \mathbf{w} \text{ begins with } 00\} \\ J &= \{\mathbf{w} \in \Sigma^\omega : 1\mathbf{w} \in \mathcal{O} \text{ and } \mathbf{w} \text{ begins with } 0\} \end{aligned}$$

We have

$$\begin{aligned} 0\mu(\mathbf{x}) \in I &\Longleftrightarrow 10\mu(\mathbf{x}) \in \mathcal{O} \text{ and } 0\mu(\mathbf{x}) \text{ begins with } 00 \\ &\Longleftrightarrow \mu(1\mathbf{x}) \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 0 \\ &\Longleftrightarrow 1\mathbf{x} \in \mathcal{O} \text{ and } \mathbf{x} \text{ begins with } 0. \end{aligned}$$

Verifying the assertions

We also need to verify that transitions not show lead to empty sets.

For example, let's check $\delta(F, 4) = \emptyset$.

Recall that

$$F = \{\mathbf{w} \in \Sigma^\omega \;:\; 0\mathbf{w} \in \mathcal{O} \text{ and } \mathbf{w} \text{ begins with } 11\}.$$

So by the correspondence, we need to check that

$$\mathbf{x} \in \emptyset \iff 11\mu(\mathbf{x}) \in F.$$

Verifying the assertions

Let's check

$$\mathbf{x} \in \emptyset \iff 11\mu(\mathbf{x}) \in F.$$

We have

$$11\mu(\mathbf{x}) \in F \iff 011\mu(\mathbf{x}) \in \mathcal{O}.$$

But if $\mathbf{x}$ begins with 00, then $011\mu(\mathbf{x}) = 0110101\cdots$, which has an overlap.

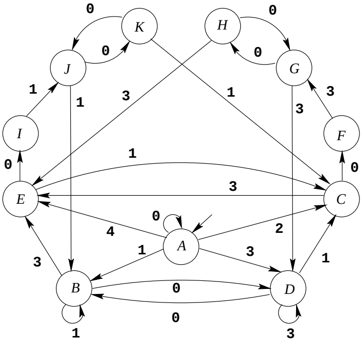
If $\mathbf{x}$ begins with 01, then $011\mu(\mathbf{x}) = 0110110\cdots$, which has an overlap.

If $\mathbf{x}$ begins with 1, then $011\mu(\mathbf{x}) = 01110\cdots$, which has an overlap.

This verifies the assertion.

Theorem. The lexicographically least infinite binary overlap-free word is $001001\overline{\mathbf{t}}$.

Proof. Let $\mathbf{x}$ be the lexicographically least infinite word, and let $\mathbf{y}$ be its code.
Then $\mathbf{y}[1]$ must be 2, since any other choice codes a word that starts with 01 or something lexicographically greater.
Once $\mathbf{y}[1] = 2$ is chosen, if the next symbol is 3, then the only choices are 2301 and 2310 and 2303. But 2301 codes $00\mu(1)\mu^3(0) = 001001101001$, and 2310 codes $00\mu(1)\mu^2(0)\mu^3(a) \geq 001001100110\cdots$ and 2313 codes $00\mu(1)\mu^2(0)\mu^3(1) = 001001101001\cdots$; all of these are lexicographically greater than $00\mu(\mu(1)) = 001001$, which is coded by 203. So the next two symbols must be $\mathbf{y}[2..3] = 03$.



Now we are in state G.

We argue that the lexicographically least word that follows causes us to alternate between states G and H on 0, producing $100\cdots$.

For otherwise our only choices are 30, 31, or (if we are in G) 33 as the next two symbols, and all of these code a word lexicographically greater than 100.

Hence $\mathbf{y} = 203\,0^{\omega}; 1$ is the code for the lexicographically least sequence, and this codes $001001\bar{\mathbf{t}}$.

More consequences of the main theorem

Theorem. All of the sets $A, B, C, \ldots, K$ are uncountable.

Proof. It suffices to provide two paths, whose labels form a code, from each state to itself (except A).

For example, for the state K, the paths 13010 and 1301000 lead from K to itself.

More consequences of the main theorem

An infinite word $(a_n)_{n\geq 0}$ is k-automatic if there is an automaton with output that, on input n in base k, reaches a state whose associated output is a_n.

Theorem. An infinite binary overlap-free word is 2-automatic if and only if (a) it is encoded by the automaton previously shown and (b) the sequence of symbols coding it is ultimately periodic.

Proof of 2-automatic result

It suffices to look at the 2-decimation of

$$x_1 \ \mu(x_2) \ \mu^2(x_3) \ \cdots .$$

If x_1 empty this is

$$x_2 \ \mu(x_3) \ \mu^2(x_4) \ \cdots$$

and

$$\overline{x_2} \ \mu(\overline{x_3}) \ \mu^2(\overline{x_4}) \ \cdots .$$

If $|x_1| = 1$ this is

$$x_1 \ \overline{x_2} \ \mu(\overline{x_3}) \ \mu^2(\overline{x_4}) \cdots$$

and

$$x_2 \ \mu(x_3) \ \mu^2(x_4) \ \cdots .$$

Proof of 2-automatic result

If $|x_1| = 2$ this is

$$a\ x_2\ \mu(x_3)\ \mu^2(x_4)\ \cdots$$

and

$$a\ \overline{x_2}\ \mu(\overline{x_3})\ \mu^2(\overline{x_4})\ \cdots .$$

Now $x_1\ \mu(x_2)\ \mu^2(x_3)\cdots$ is 2-automatic iff the set of all 2-decimations is finite.

But if it is finite then for some $i < j$ we have

$$x_i\ \mu(x_{i+1})\ \mu^2(x_{i+2})\ \cdots = x_j\ \mu(x_{j+1})\ \mu^2(x_{j+2})\ \cdots$$

so the x_i are ultimately periodic with period $j - i$.

On the other hand, if the x_i are ultimately periodic then the set of all decimations is finite, since we can specify any decimation by (1) an initial term of length at most 4 (2) whether subsequent terms are complemented and (3) which of a finite set of x_i begins the second term.

Back to the fragility conjecture

Conjecture. For every overlap-free word **x** there exists a constant C (depending on **x**) such that if we flip the bits in any nonempty set of positions $> C$, then the result has an overlap.

Consider the set of infinite words given by

$$1\{113011, 313011\}^{\omega}.$$

From our automaton, all these code infinite overlap-free words.

But then $1(113011)^{\omega}$ has infinitely many distinct positions where finitely many symbols can be flipped to get a new overlap-free word.

Conjecture disproved!

Further results

In a paper with N. Rampersad and A. Shur to be presented at WORDS 2011, we show that the analogous result holds for the exponent $7/3$ (in place of $2 + \epsilon$, which corresponds to overlaps).

Similar results have already been obtained for all exponents $2 < e \leq 7/3$ and finite words by Blondel, Cassaigne, and Jüngers.

For Further Reading

- J. Berstel. A rewriting of Fife's theorem about overlap-free words. In J. Karhumäki, H. Maurer, and G. Rozenberg, editors, *Results and Trends in Theoretical Computer Science*, Vol. 812 of *Lecture Notes in Computer Science*, pp. 19–29. Springer-Verlag, 1994.
- V. D. Blondel, J. Cassaigne, and R. M. Jungers. On the number of α-power-free binary words for $2 < \alpha \leq 7/3$. *Theoret. Comput. Sci.* **410** (2009), 2823–2833.
- E. D. Fife. Binary sequences which contain no *BBb*. *Trans. Amer. Math. Soc.* **261** (1980), 115–136.
- A. Restivo and S. Salemi. Overlap free words on two symbols. In M. Nivat and D. Perrin, editors, *Automata on Infinite Words*, Vol. 192 of *Lecture Notes in Computer Science*, pp. 198–206. Springer-Verlag, 1985.