Counting equivalence classes of words in F_2

Bobbe Cooper and Eric Rowland

LaCIM
Université du Québec à Montréal

February 20, 2012

Outline

1. Whitehead's theorem
2. Minimal words
3. Root words
4. Enumerating equivalence classes

Notation

- $L_2 = \{a, b, \overline{a}, \overline{b}\}$, where $\overline{a} = a^{-1}$ and $\overline{b} = b^{-1}$.
- $F_2 = \langle a, b \rangle = \{w_1 \cdots w_\ell \in L_2^* : w_i \neq w_{i+1}^{-1} \text{ for } 1 \leq i \leq \ell - 1\}$.
- $C_2 = \{w_1 \cdots w_\ell \in F_2 : w_\ell \neq w_1^{-1}\}$.

We are interested in equivalence classes of words in F_2 under Aut F_2.

Definition

A word $w \in F_2$ is *minimal* if $|w| \leq |\phi(w)|$ for all $\phi \in \operatorname{Aut} F_2$.

A *Type I automorphism* is an automorphism ϕ that permutes L_2.

Whitehead's theorem

We write $w \sim v$ if $\phi(w) = v$ for some automorphism ϕ.

Theorem (Whitehead, 1936)

If $w, v \in F_n$ such that $w \sim v$ and v is minimal, then there exists a sequence $\phi_1, \phi_2, \ldots, \phi_m$ of Type I and Type II automorphisms such that

- $\phi_m \cdots \phi_2 \phi_1(w) = v$ *and*
- *for* $0 \leq k \leq m - 1$, $|\phi_{k+1}\phi_k \cdots \phi_2\phi_1(w)| \leq |\phi_k \cdots \phi_2\phi_1(w)|$, *with strict inequality unless* $\phi_k \cdots \phi_2\phi_1(w)$ *is minimal.*

The set of Whitehead automorphisms is finite.

Corollary

There is an algorithm for determining whether $w \in F_2$ is minimal.
There is an algorithm for determining whether $w, v \in F_2$ are equivalent.

Running times

- Myasnikov and Shpilrain (2003) showed that the number of minimal words equivalent to minimal $w \in F_2$ is bounded by a polynomial in $|w|$.
- Lee (2006) showed that the same is true for minimal $w \in F_n$ under a local condition on w and determined the polynomial degree.

These results imply upper bounds on the time required to determine whether $w, v \in F_n$ are equivalent.

- Khan (2004) showed that the running time in F_2 is at most quadratic in $\max(|w|, |v|)$.

All these results make use of counting subwords of w.

Computing equivalence classes

Corollary

There is an algorithm for computing all equivalence classes of F_2 containing a word of length $\leq n$.

It is easy to recognize equivalence under a Type I automorphism.

It is also easy to recognize equivalence under conjugation.
For example, $aba\overline{b}$, $ba\overline{b}a$, $a\overline{b}ab$, and $\overline{b}aba$.

So we choose a representative from each "cyclic permutation" class.

Equivalence classes

0.1	ϵ	$\star$
1.1	a	
2.1	aa	
3.1	aaa	
4.1	$aaaa$	
4.2	$ab\overline{a}\overline{b}$	$\star$
4.3	$aabb$ $aba\overline{b}$	$\star$ $\star$
5.1	$aaaaa$	
5.2	$aaba\overline{b}$	
5.3	$aab\overline{a}\overline{b}$	
5.4	$aaabb$ $aab\overline{a}b$	

6.1	$aaaaaa$
6.2	$aaaba\overline{b}$
6.3	$aaabbb$
6.4	$aaab\overline{a}\overline{b}$
6.5	$aabaa\overline{b}$
6.6	$aaba\overline{bb}$
6.7	$aabba\overline{b}$
6.8	$aabb\overline{a}\overline{b}$
6.9	$aab\overline{aa}\overline{b}$
6.10	$aaaabb$ $aaab\overline{a}b$ $aab\overline{aa}b$
7.1	$aaaaaaa$
7.2	$aaaaba\overline{b}$
7.3	$aaaabbb$

7.4	$aaaab\overline{a}\overline{b}$
7.5	$aaabaa\overline{b}$
7.6	$aaaba\overline{bb}$
7.7	$aaabba\overline{b}$
7.8	$aaabb\overline{a}b$
7.9	$aaabb\overline{a}\overline{b}$
7.10	$aaab\overline{a}bb$
7.11	$aaab\overline{aa}\overline{b}$
7.12	$aaab\overline{a}\overline{bb}$
7.13	$aabaa\overline{bb}$
7.14	$aabba\overline{bb}$
7.15	$aabb\overline{aa}\overline{b}$
7.16	$aaaaabb$ $aaaab\overline{a}b$ $aaab\overline{aa}b$

Outline

Type II automorphisms

Definition

Fix $x \in L_2$ and $A \subset L_2 \backslash \{x, \overline{x}\}$.
Define $\phi : L_2 \to F_2$ by

$$\phi(y) = \overline{x}^{\chi(\overline{y} \in A)} \, y \, x^{\chi(y \in A)},$$

where $\chi(\text{true}) = 1$ and $\chi(\text{false}) = 0$.
We write $\phi = (A, x)$ and call ϕ a *Type II automorphism*.

The automorphism $(\{y\}, x)$ maps $x \mapsto x$, $\overline{x} \mapsto \overline{x}$, $y \mapsto yx$, and $\overline{y} \mapsto \overline{xy}$.

Example

Let $\phi = (\{b\}, a)$; then $\phi(a\overline{b}) = a\overline{a}\overline{b} = \overline{b}$, so $a\overline{b}$ is not minimal.

An automorphism $(\{y\}, x)$ is called a *one-letter automorphism*.

Type II automorphisms

Definition

Fix $x \in L_2$ and $A \subset L_2 \backslash \{x, \overline{x}\}$.
Define $\phi : L_2 \to F_2$ by

$$\phi(y) = \overline{x}^{\chi(\overline{y} \in A)} \, y \, x^{\chi(y \in A)},$$

where $\chi(\text{true}) = 1$ and $\chi(\text{false}) = 0$.
We write $\phi = (A, x)$ and call ϕ a *Type II automorphism*.

The automorphism $(\{y\}, x)$ maps $x \mapsto x$, $\overline{x} \mapsto \overline{x}$, $y \mapsto yx$, and $\overline{y} \mapsto \overline{x}\,\overline{y}$.

The automorphism $(\{y, \overline{y}\}, x)$ conjugates both x and y by x.
Therefore, on C_2 it suffices to consider one-letter automorphisms.

Length-2 subwords track the effects of one-letter automorphisms.

Subword counts

Definition

Let $(v)_w$ denote the number of (possibly overlapping) occurrences of v and v^{-1} in the cyclic word w.

Example

Let $w = aa\bar{b}\bar{b}\bar{a}ba\bar{b}a$. The length-2 subword counts are $(aa)_w = 2$, $(bb)_w = 1$, $(ab)_w = 1$, $(ba)_w = 1$, $(a\bar{b})_w = 2$, and $(\bar{b}a)_w = 2$.

Lemma

If $w \in C_2$ and $x, y \in L_2$, then $(xy)_w = (yx)_w$.

Characterization of minimal words

Theorem

$w \in C_2$ is minimal if and only if $|(ab)_w - (a\bar{b})_w| \leq \min((aa)_w, (bb)_w)$.

Corollary

If w, v are minimal words with the same first letter, then wv is minimal.

The converse is not true in general:
If $w = a$ and $v = abb$, then wv is minimal but v is not.

Outline

Equivalence classes

0.1	ϵ	$\star$
1.1	a	
2.1	aa	
3.1	aaa	
4.1	$aaaa$	
4.2	$ab\bar{a}\bar{b}$	$\star$
4.3	$aabb$	$\star$
	$aba\bar{b}$	$\star$
5.1	$aaaaa$	
5.2	$aaba\bar{b}$	
5.3	$aab\bar{a}\bar{b}$	
5.4	$aaabb$	
	$aab\bar{a}b$	

6.1	$aaaaaa$
6.2	$aaaba\bar{b}$
6.3	$aaabbb$
6.4	$aaab\bar{a}\bar{b}$
6.5	$aabaa\bar{b}$
6.6	$aaba\bar{b}\bar{b}$
6.7	$aabba\bar{b}$
6.8	$aabb\bar{a}\bar{b}$
6.9	$aab\bar{a}\bar{a}\bar{b}$
6.10	$aaaabb$
	$aaab\bar{a}b$
	$aab\bar{a}\bar{a}b$
7.1	$aaaaaaa$
7.2	$aaaaba\bar{b}$
7.3	$aaaabbb$

7.4	$aaaab\bar{a}\bar{b}$
7.5	$aaabaa\bar{b}$
7.6	$aaaba\bar{b}\bar{b}$
7.7	$aaabba\bar{b}$
7.8	$aaabb\bar{a}b$
7.9	$aaabb\bar{a}\bar{b}$
7.10	$aaab\bar{a}bb$
7.11	$aaab\bar{a}\bar{a}\bar{b}$
7.12	$aaab\bar{a}\bar{b}\bar{b}$
7.13	$aabaa\bar{b}\bar{b}$
7.14	$aabba\bar{b}\bar{b}$
7.15	$aabb\bar{a}\bar{a}\bar{b}$
7.16	$aaaaabb$
	$aaaab\bar{a}b$
	$aaab\bar{a}\bar{a}b$

Growing words from other words

Definition

A *child* of $w \neq \epsilon$ is a word obtained by duplicating a letter in w.
Define each letter $x \in L_2$ to be a child of ϵ.

Example

The children of *aabb* are *aaabb* and *aabbb*.

A child of a minimal word is necessarily minimal.

Root words

Definition

A *root word* is a minimal word that is not a child of any minimal word.

Root words are new minimal words with respect to duplicating a letter.

Example

The minimal word $aabb$ is a root word, since neither of its parents abb and aab is minimal.

Example

The minimal words $aba\bar{b}$ and $ab\bar{a}\bar{b}$ are root words. They are not children of any minimal word; in particular they have no subword xx.

Characterization of root words

Recall:

Theorem

$w \in C_2$ is minimal if and only if $|(ab)_w - (a\bar{b})_w| \leq \min((aa)_w, (bb)_w)$.

Root words are "maximally minimal".

Theorem

$w \in C_2$ is a root word if and only if $|(ab)_w - (a\bar{b})_w| = (aa)_w = (bb)_w$.

Proof.

A minimal word w is a root word if and only if replacing any xx by x in w causes the word to lose minimality.
Shortening a subword xx decrements $(aa)_w$ or $(bb)_w$, so w is a root word precisely when both inequalities hold for equality. $\square$

Corollaries

Corollary

Let $n \geq 1$. Then $w \in C_2$ is a root word if and only if w^n is a root word.

Corollary

If w is a root word, then $(a)_w = (b)_w = |w|/2$.

Proof.

The only length-2 subwords with unequal generator weights are aa, $\overline{aa}$, bb, and $\overline{bb}$, but $(aa)_w = (bb)_w$. $\square$

Equivalence classes

0.1	ϵ	$\star$
1.1	a	
2.1	aa	
3.1	aaa	
4.1	$aaaa$	
4.2	$ab\overline{a}\overline{b}$	$\star$
4.3	$aabb$	$\star$
	$aba\overline{b}$	$\star$
5.1	$aaaaa$	
5.2	$aaba\overline{b}$	
5.3	$aab\overline{a}\overline{b}$	
5.4	$aaabb$	
	$aab\overline{a}b$	

6.1	$aaaaaa$
6.2	$aaaba\overline{b}$
6.3	$aaabbb$
6.4	$aaab\overline{a}\overline{b}$
6.5	$aabaa\overline{b}$
6.6	$aaba\overline{bb}$
6.7	$aabba\overline{b}$
6.8	$aabb\overline{a}\overline{b}$
6.9	$aab\overline{aa}\overline{b}$
6.10	$aaaabb$
	$aaab\overline{a}b$
	$aab\overline{aa}b$
7.1	$aaaaaaa$
7.2	$aaaaba\overline{b}$
7.3	$aaaabbb$

7.4	$aaaab\overline{a}\overline{b}$
7.5	$aaabaa\overline{b}$
7.6	$aaaba\overline{bb}$
7.7	$aaabba\overline{b}$
7.8	$aaabb\overline{a}b$
7.9	$aaabb\overline{a}\overline{b}$
7.10	$aaab\overline{a}bb$
7.11	$aaab\overline{aa}\overline{b}$
7.12	$aaab\overline{a}\overline{bb}$
7.13	$aabaa\overline{bb}$
7.14	$aabba\overline{bb}$
7.15	$aabb\overline{aa}\overline{b}$
7.16	$aaaaabb$
	$aaaab\overline{a}b$
	$aaab\overline{aa}b$

Equivalence classes

8.1	$aaaaaaaa$
8.2	$aaaaaab\bar{b}$
8.3	$aaaaabbb$
8.4	$aaaaab\bar{a}\bar{b}$
8.5	$aaaabaa\bar{b}$
8.6	$aaaaba\bar{b}\bar{b}$
8.7	$aaaabba\bar{b}$
8.8	$aaaabbbb$
8.9	$aaaabb\bar{a}b$
8.10	$aaaabb\bar{a}\bar{b}$
8.11	$aaaab\bar{a}bb$
8.12	$aaaab\bar{a}\bar{a}\bar{b}$
8.13	$aaaab\bar{a}\bar{b}\bar{b}$
8.14	$aaabaaa\bar{b}$

8.15	$aaabaa\bar{b}\bar{b}$
$\vdots$	$\vdots$
8.37	$aaababbb \star$
	$aababa\bar{b}\bar{b} \star$
	$aabba\bar{b}a\bar{b} \star$
8.38	$aaabbabb \star$
	$aaba\bar{b}\bar{b}ab \star$
	$ababa\bar{b}a\bar{b} \star$
8.39	$aababb\bar{a}\bar{b} \star$
	$aabab\bar{a}\bar{b}\bar{b} \star$
	$aabb\bar{a}\bar{b}a\bar{b} \star$
8.40	$aababba\bar{b} \star$
	$aababb\bar{a}b \star$
	$aaba\bar{b}\bar{a}\bar{b}\bar{b} \star$

8.41	$aaaaaabb$
	$aaaaab\bar{a}b$
	$aaaab\bar{a}\bar{a}b$
	$aaab\bar{a}\bar{a}\bar{a}b$
8.42	$aaba\bar{b}abb \star$
	$aabba\bar{b}ab \star$
	$aabba\bar{b}\bar{a}\bar{b} \star$
	$aabb\bar{a}\bar{b}\bar{a}b \star$
	$abab\bar{a}ba\bar{b} \star$
8.43	$aaba\bar{b}\bar{a}bb \star$
	$aaba\bar{b}\bar{b}\bar{a}b \star$
	$aab\bar{a}bb\bar{a}\bar{b} \star$
	$aabb\bar{a}\bar{b}ab \star$
	$abab\bar{a}b\bar{a}\bar{b} \star$

Length of a root word

Theorem

If w is a root word, then $|w|$ is divisible by 4.

Proof.

We have

$$\begin{aligned} |w| &= (aa)_w + (bb)_w + (ab)_w + (ba)_w + (a\bar{b})_w + (\bar{b}a)_w \\ &= 2(aa)_w + 2(ab)_w + 2(a\bar{b})_w \\ &= 2|(ab)_w - (a\bar{b})_w| + 2(ab)_w + 2(a\bar{b})_w. \end{aligned}$$

If $(ab)_w \geq (a\bar{b})_w$ then $|w| = 4(ab)_w$;
if $(ab)_w < (a\bar{b})_w$ then $|w| = 4(a\bar{b})_w$. □

Run-lengths in a root word

Let $\lambda(w)$ be the length of the longest subword of w of the form x^ℓ.
For example, $\lambda(aa\overline{b}\overline{b}\overline{a}ba\overline{b}a) = 3$.

Theorem

If w is a root word, then $\lambda(w) \leq \frac{|w|}{4} + 1$.

Furthermore, the root word $a^{n+1}(ba)^{n-1}b^{n+1}$ achieves this bound.

Root classes

The property of being a root word is respected by equivalence classes.

Theorem

If w is a root word, $w \sim v$, and $|w| = |v|$, then v is a root word.

We refer to an equivalence class containing a root word as a *root class*.

Outline

1. Whitehead's theorem
2. Minimal words
3. Root words
4. Enumerating equivalence classes

Number of equivalence classes of each size

$\lvert w \rvert$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
0	1											
1	1											
2	1											
3	1											
4	2	1										
5	3	1										
6	9	0	1									
7	15	0	1									
8	31	5	4	1	2							
9	52	28	15	6								
10	257	41	24	12	6							
11	792	46	35	20	13	5						
12	2076	78	293	31	48	13	5					
13	4711	1970	403	78	27	18	12	5				
14	17387	3796	1062	238	74	24	18	12	5			
15	55675	6445	2285	635	207	70	25	17	12	5		
16	159686	10303	15129	1448	859	203	67	25	17	12	5	
17	417137	110815	12926	3047	1045	448	199	68	24	17	12	$\ddots$
18	1357294	250913	35119	6728	2256	890	444	196	68	24	17	$\ddots$
19	4204439	513498	89426	16208	5001	1864	859	440	197	67	24	$\ddots$
20	12316599	969362	678470	40127	15681	4232	1709	855	437	197	67	$\ddots$

Growing classes from other classes

length 12:

$aaaaaaba\bar{b}abb$
$aaaaaabb\bar{a}\bar{b}\bar{a}b$
$aaaaaba\bar{b}ab\bar{a}b$
$aaaaab\bar{a}b\bar{a}\bar{b}\bar{a}b$
$aaaaba\bar{b}ab\overline{aa}b$
$aaaab\overline{aa}b\bar{a}\bar{b}\bar{a}b$
$aaaba\bar{b}ab\overline{aaa}b$

length 13:

$aaaaaaaba\bar{b}abb$
$aaaaaaabb\bar{a}\bar{b}\bar{a}b$
$aaaaaaba\bar{b}ab\bar{a}b$
$aaaaaab\bar{a}b\bar{a}\bar{b}\bar{a}b$
$aaaaaba\bar{b}ab\overline{aa}b$
$aaaaab\overline{aa}b\bar{a}\bar{b}\bar{a}b$
$aaaaba\bar{b}ab\overline{aaa}b$
$aaaab\overline{aaa}b\bar{a}\bar{b}\bar{a}b$

length 14:

$aaaaaaaaba\bar{b}abb$
$aaaaaaaabb\bar{a}\bar{b}\bar{a}b$
$aaaaaaaba\bar{b}ab\bar{a}b$
$aaaaaaab\bar{a}b\bar{a}\bar{b}\bar{a}b$
$aaaaaaba\bar{b}ab\overline{aa}b$
$aaaaaab\overline{aa}b\bar{a}\bar{b}\bar{a}b$
$aaaaaba\bar{b}ab\overline{aaa}b$
$aaaaab\overline{aaa}b\bar{a}\bar{b}\bar{a}b$
$aaaaba\bar{b}ab\overline{aaaa}b$

Main goal

Enumerate equivalence classes containing a minimal word of length *n*.

Number of root classes of each size

$\|w\|$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
0	1											
4	1	1										
8	2	5	4	0	2							
12	5	19	249	0	31							
16	12	89	10914	0	380							
20	36	455	473406	0	4547							

Theorem

The size of a root word class is 1, 2, 3, *or* 5.

To the extent that equivalence classes grow regularly in size, this perhaps explains the stabilization.

Conjecture by size

The *weight* $\min((a)_w, (b)_w)$ is invariant on equivalence classes.

The number of size-k classes of words of length 20 and weight 4:

$$990, 131, 118, 107, 92, 79, 66, 55, 41, 36, 29, 24, 17, 12, 5, 0, 0, 0, \dots$$

Difference sequence:

$$859, 13, 11, 15, 13, 13, 11, 14, 5, 7, 5, 7, 5, 7, 5, 0, 0, \dots$$

Conjectures by length

The number of size-1 classes of words of length n and weight 2:

$$0, 0, 0, 0, 1, 2, 4, 4, 6, 6, 8, 8, 10, 10, 12, 12, 14, 14, 16, 16, 18, \dots$$

is an eventual linear quasi-polynomial modulo 2.

The number of size-1 classes of words of length n and weight 4:

$$0, 0, 0, 0, 0, 0, 0, 0, 11, 29, 49, 70, \\ 110, 151, 217, 288, 390, 497, 641, 794, 990, \dots$$

appears to be an eventual cubic quasi-polynomial modulo 4.