# Potential Versus Actual Signature Space

Mariela Carvacho, Jen Paulhus*, and Aaron Wootton

GRINNELL COLLEGE

http://www.math.grinnell.edu/∼paulhusj

# 13th Algorithmic Number Theory Symposium

University of Wisconsin, Madison, USA,

July 16-20, 2018

http://www.math.grinnell.edu/∼paulhusj/ants2018

Submissions still welcome for a poster session (anyone may submit, this year we are including strong undergraduate submissions). See the website for more information.

$X$ a compact Riemann surface.

Automorphism group $G$ of $X$ leads to covering map $X \to X/G$, branched at $r$ places.

$X$ a compact Riemann surface.

Automorphism group $G$ of $X$ leads to covering map $X \to X/G$, branched at $r$ places.

If $X$ has genus $g$, and $X/G$ has genus $h$, and those branch points have monodromy of order $m_1, \ldots, m_r$, respectively, then

$$[h; m_1, \ldots, m_r]$$

is the **signature** of the action of $G$ on $X$.

$X$ a compact Riemann surface.

Automorphism group $G$ of $X$ leads to covering map $X \to X/G$, branched at $r$ places.

If $X$ has genus $g$, and $X/G$ has genus $h$, and those branch points have monodromy of order $m_1, \ldots, m_r$, respectively, then

**orbit genus** $\downarrow$ $\qquad\qquad$ $\downarrow$ $r$ **is tail length**

$$[h;\ \underbrace{m_1, \ldots, m_r}_{\textbf{tail}}]$$

is the **signature** of the action of $G$ on $X$.

A finite group $G$ acts on a compact Riemann surface $X$ of genus $g \geq 2$ with signature $[h; m_1, \ldots, m_r]$ if and only if:

I. the Riemann-Hurwitz formula is satisfied:

$$g = 1 + |G|(h-1) + \frac{|G|}{2} \sum_{j=1}^{r} \left(1 - \frac{1}{m_j}\right),$$

II. there exists a *generating vector* $(a_1, b_1, \ldots a_h, b_h, c_1, \ldots, c_r)$ of elements of $G$ which satisfies the following properties:

1. $G = \langle a_1, b_1, a_2, b_2, \ldots, a_h, b_h, c_1, \ldots, c_r \rangle$.
2. The order of $c_j$ is $m_j$ for $1 \leq j \leq r$.
3. $\prod_{i=1}^{h} [a_i, b_i] \prod_{j=1}^{r} c_j = e_G$, the identity in $G$.

A finite group $G$ acts on a compact Riemann surface $X$ of genus $g \geq 2$ with signature $[h; m_1, \ldots, m_r]$ if and only if:

I. the Riemann-Hurwitz formula is satisfied:

$$g = 1 + |G|(h-1) + \frac{|G|}{2} \sum_{j=1}^{r} \left(1 - \frac{1}{m_j}\right),$$

II. there exists a *generating vector* $(a_1, b_1, \ldots a_h, b_h, c_1, \ldots, c_r)$ of elements of $G$ which satisfies the following properties:

1. $G = \langle a_1, b_1, a_2, b_2, \ldots, a_h, b_h, c_1, \ldots, c_r \rangle$.
2. The order of $c_j$ is $m_j$ for $1 \leq j \leq r$.
3. $\prod_{i=1}^{h} [a_i, b_i] \prod_{j=1}^{r} c_j = e_G$, the identity in $G$.

**potential signatures** satisfy I.

A finite group $G$ acts on a compact Riemann surface $X$ of genus $g \geq 2$ with signature $[h; m_1, \ldots, m_r]$ if and only if:

I. the Riemann-Hurwitz formula is satisfied:

$$g = 1 + |G|(h-1) + \frac{|G|}{2} \sum_{j=1}^{r} \left(1 - \frac{1}{m_j}\right),$$

II. there exists a *generating vector* $(a_1, b_1, \ldots a_h, b_h, c_1, \ldots, c_r)$ of elements of $G$ which satisfies the following properties:

1. $G = \langle a_1, b_1, a_2, b_2, \ldots, a_h, b_h, c_1, \ldots, c_r \rangle$.
2. The order of $c_j$ is $m_j$ for $1 \leq j \leq r$.
3. $\prod_{i=1}^{h} [a_i, b_i] \prod_{j=1}^{r} c_j = e_G$, the identity in $G$.

**potential signatures** satisfy I.
**actual signatures** satisfy I. and II.

These are not always the same.

**Example**

$[0; 3, 3, 9]$ satisfies Riemann-Hurwitz for a curve of genus 2 and a group of order 9. But this signature cannot be an actual signature for abelian groups. (There's an issue with the lcm of the $m_i$. See Breuer Theorem 9.1.)

These are not always the same.

**Example**

$[0; 3, 3, 9]$ satisfies Riemann-Hurwitz for a curve of genus 2 and a group of order 9. But this signature cannot be an actual signature for abelian groups. (There's an issue with the lcm of the $m_i$. See Breuer Theorem 9.1.) All groups of order 9 are abelian.

These are not always the same.

**Example**

$[0; 3, 3, 9]$ satisfies Riemann-Hurwitz for a curve of genus 2 and a group of order 9. But this signature cannot be an actual signature for abelian groups. (There's an issue with the lcm of the $m_i$. See Breuer Theorem 9.1.) All groups of order 9 are abelian.

Sometimes they are badly not the same for a fixed group

**Example**

Take $q = p^n$ for $p$ an odd prime. Then $[0; \underbrace{2, 2, \ldots, 2}_{r>4}]$ is a potential signature for $\mathrm{SL}(2, q)$, but only one element of order 2.

These are not always the same.

**Example**

$[0; 3, 3, 9]$ satisfies Riemann-Hurwitz for a curve of genus 2 and a group of order 9. But this signature cannot be an actual signature for abelian groups. (There's an issue with the lcm of the $m_i$. See Breuer Theorem 9.1.) All groups of order 9 are abelian.

Sometimes they are badly not the same for a fixed group

**Example**

Take $q = p^n$ for $p$ an odd prime. Then $[0; \underbrace{2, 2, \ldots, 2}_{r>4}]$ is a potential signature for $\mathrm{SL}(2, q)$, but only one element of order 2. $r$ copies of this element of order 2 will never generate $\mathrm{SL}(2, q)$.

We wondered which **groups** only have a finite number of potential signatures which *fail* to be actual signatures.

We say such groups satisfy the **Finiteness Signature Condition** (FSC).

We wondered which **groups** only have a finite number of potential signatures which *fail* to be actual signatures.

We say such groups satisfy the **Finiteness Signature Condition** (FSC).

The **order set** is:

$$\mathcal{O}(G) = \{o(g) \mid g \in G\} - \{1\}$$

$[1; n]$ will be a potential signature for every $n \in \mathcal{O}(G)$ for every group $G$.

$[1; n]$ will be a potential signature for every $n \in \mathcal{O}(G)$ for every group $G$.

To create a generating vector, we need $[a, b] \in [G, G]$ and $c \in G$ with $o(c) = n$ so that $[a, b] \cdot c = e_G$. Hence $[a, b]$ must have order $n$ to create generating vector $(a, b, c)$.

$[1; n]$ will be a potential signature for every $n \in \mathcal{O}(G)$ for every group $G$.

To create a generating vector, we need $[a, b] \in [G, G]$ and $c \in G$ with $o(c) = n$ so that $[a, b] \cdot c = e_G$. Hence $[a, b]$ must have order $n$ to create generating vector $(a, b, c)$.

More generally, $[h; n]$ is a potential signature for every positive orbit genus $h$ and $n \in \mathcal{O}(G)$, and so there must be $a_i, b_i, c \in G$ with $o(c) = n$ so that $\prod_{i=1}^{h} [a_i, b_i] \cdot c = e_G$.

$[1; n]$ will be a potential signature for every $n \in \mathcal{O}(G)$ for every group $G$.

To create a generating vector, we need $[a, b] \in [G, G]$ and $c \in G$ with $o(c) = n$ so that $[a, b] \cdot c = e_G$. Hence $[a, b]$ must have order $n$ to create generating vector $(a, b, c)$.

More generally, $[h; n]$ is a potential signature for every positive orbit genus $h$ and $n \in \mathcal{O}(G)$, and so there must be $a_i, b_i, c \in G$ with $o(c) = n$ so that $\prod_{i=1}^{h} [a_i, b_i] \cdot c = e_G$.

The commutator subgroup must contain an element of every order in $\mathcal{O}(G)$.

For every element $n$ of the order set, $[0; \underbrace{n, \ldots, n}_{r}]$ will be a potential signature for sufficiently large $r$.

For every element $n$ of the order set, $[0; \underbrace{n, \ldots, n}_{r}]$ will be a potential signature for sufficiently large $r$.

For each $n$ in $\mathcal{O}(G)$, the set of elements in $G$ of that order must generate the group.

Suppose $(c_1, \ldots, c_r)$ is a generating vector with $o(c_j) = n \in \mathcal{O}(G)$ and $n$ odd. Then so are:

$$(c_1, \ldots, c_r, c_r, c_r^{-1})$$

$$(c_1, \ldots, c_r, c_r^2, c_r^{-1}, c_r^{-1}) \ldots$$

Suppose $(c_1, \ldots, c_r)$ is a generating vector with $o(c_j) = n \in \mathcal{O}(G)$ and $n$ odd. Then so are:

$$(c_1, \ldots, c_r, c_r, c_r^{-1})$$

$$(c_1, \ldots, c_r, c_r^2, c_r^{-1}, c_r^{-1}) \ldots$$

If $(c_1, \ldots, c_r)$ is a generating vector with $o(c_j) = n$ and $n$ even and $r$ odd. Then so are:

$$(c_1, \ldots, c_r, c_r, c_r^{-1}) \ldots$$

$$(c_1, \ldots, c_r, c_1, \ldots, c_r)$$

$$(c_1, \ldots, c_r, c_1, \ldots, c_r, c_r, c_r^{-1}) \ldots$$

**Theorem (Carvacho, Paulhus, Wootton)**

*A group $G$ has the FSC if and only if the following conditions hold:*

1. *The commutator subgroup $[G, G]$ contains an element of order every $n_i \in \mathcal{O}(G)$.*
2. *For each $n_i \in \mathcal{O}(G)$, there exists an odd integer $N_i$ such that $[0; \underbrace{n_i, \ldots, n_i}_{N_i}]$ is an actual signature.*

**Theorem (Carvacho, Paulhus, Wootton)**

*A group $G$ has the FSC if and only if the following conditions hold:*

1. *The commutator subgroup $[G, G]$ contains an element of order every $n_i \in \mathcal{O}(G)$.*
2. *For each $n_i \in \mathcal{O}(G)$, there exists an odd integer $N_i$ such that $[0; \underbrace{n_i, \ldots, n_i}_{N_i}]$ is an actual signature.*

The proof is to show, given these conditions, the orbit genus of failures (potential signatures which are not actual signatures) is bounded and that the tail length of failures is bounded (by constructing appropriate generating vectors).

For condition (2), here's an example to highlight the key idea.

For condition (2), here's an example to highlight the key idea.

## Example

$G$ a group, $\mathcal{O}(G) = \{n_1, n_2, n_3\}$. Let $\{g_1, g_2, g_3\}$ be a set of generators of $G$ of order $n_3$.

Suppose $c_1$ and $c_2$ in $G$ with $o(c_i) = n_i$.

For condition (2), here's an example to highlight the key idea.

## Example

$G$ a group, $\mathcal{O}(G) = \{n_1, n_2, n_3\}$. Let $\{g_1, g_2, g_3\}$ be a set of generators of $G$ of order $n_3$.

Suppose $c_1 = g_1 g_2^{-2} g_3$ and $c_2 = g_3^{-1} g_1 g_2$ in $G$ with $o(c_i) = n_i$.

For condition (2), here's an example to highlight the key idea.

## Example

$G$ a group, $\mathcal{O}(G) = \{n_1, n_2, n_3\}$. Let $\{g_1, g_2, g_3\}$ be a set of generators of $G$ of order $n_3$.

Suppose $c_1 = g_1 g_2^{-2} g_3$ and $c_2 = g_3^{-1} g_1 g_2$ in $G$ with $o(c_i) = n_i$.

Then

$$(c_1, c_2, \underbrace{g_2^{-1}, g_1^{-1}, g_3}_{c_2{}^{-1}}, \underbrace{g_3^{-1}, g_2, g_2, g_1^{-1}}_{c_1{}^{-1}})$$

is a generating vector for signature

$$[0; n_1, n_2, \underbrace{n_3, \ldots, n_3}_{7}].$$

**Theorem (Carvacho, Paulhus, Wootton)**

*If a group G satisfies the FSC, then it is either a non-abelian p-group, or a perfect group (commutator subgroup is the whole group).*

**Theorem (Carvacho, Paulhus, Wootton)**

*If a group $G$ satisfies the FSC, then it is either a non-abelian p-group, or a perfect group (commutator subgroup is the whole group).*

Since the commutator subgroup must contain elements of every order in $\mathcal{O}(G)$, any group satisfying FSC must be non-abelian.

**Theorem (Carvacho, Paulhus, Wootton)**

*If a group $G$ satisfies the FSC, then it is either a non-abelian $p$-group, or a perfect group (commutator subgroup is the whole group).*

Since the commutator subgroup must contain elements of every order in $\mathcal{O}(G)$, any group satisfying FSC must be non-abelian.

What if we have a group $G$ which is not a $p$-group but satisfies FSC?

$p$ and $q$ two distinct primes in $\mathcal{O}(G)$.

Since FSC, $G$ is generated by elements of order $p$, which means $G/[G,G]$ is generated by elements of order $p$.

$p$ and $q$ two distinct primes in $\mathcal{O}(G)$.

Since FSC, $G$ is generated by elements of order $p$, which means $G/[G,G]$ is generated by elements of order $p$.

But $G/[G,G]$ is also abelian so $G/[G,G]$ is elementary abelian of order $p^k$, some $k$.

$p$ and $q$ two distinct primes in $\mathcal{O}(G)$.

Since FSC, $G$ is generated by elements of order $p$, which means $G/[G,G]$ is generated by elements of order $p$.

But $G/[G,G]$ is also abelian so $G/[G,G]$ is elementary abelian of order $p^k$, some $k$.

Same argument for the prime $q$ implies $G/[G,G]$ is elementary abelian of order $q^\ell$, some $\ell$. So $G/[G,G]$ must be trivial, hence $G$ is perfect. ■

Not all perfect groups satisfy FSC!

See $\mathrm{SL}(2, q)$ above when $q$ is odd.

Not all non-abelian $p$-groups satisfy FSC!

**Example**

Group $(27, 4)$ is $\langle a, b \mid a^9 = b^3 = e, bab^{-1} = a^4 \rangle$. Its commutator subgroup only has elements of order 3. The 8 elements of order 3 only generate a subgroup of order 9.

Not all non-abelian $p$-groups satisfy FSC!

**Example**

Group $(27, 4)$ is $\langle a, b \mid a^9 = b^3 = e, bab^{-1} = a^4 \rangle$. Its commutator subgroup only has elements of order 3. The 8 elements of order 3 only generate a subgroup of order 9.

**Example**

Group $(243, 26)$ has 170 elements of order 3 and 72 of order 9. The commutator subgroup contains elements of both non-trivial orders. But the elements of order 9 generate a subgroup of order 81.

But some $p$-groups do satisfy FSC!

**Corollary**

*For p odd, any non-abelian p-group of exponent p satisfies FSC.*

But some $p$-groups do satisfy FSC!

**Corollary**

*For p odd, any non-abelian p-group of exponent p satisfies FSC.*

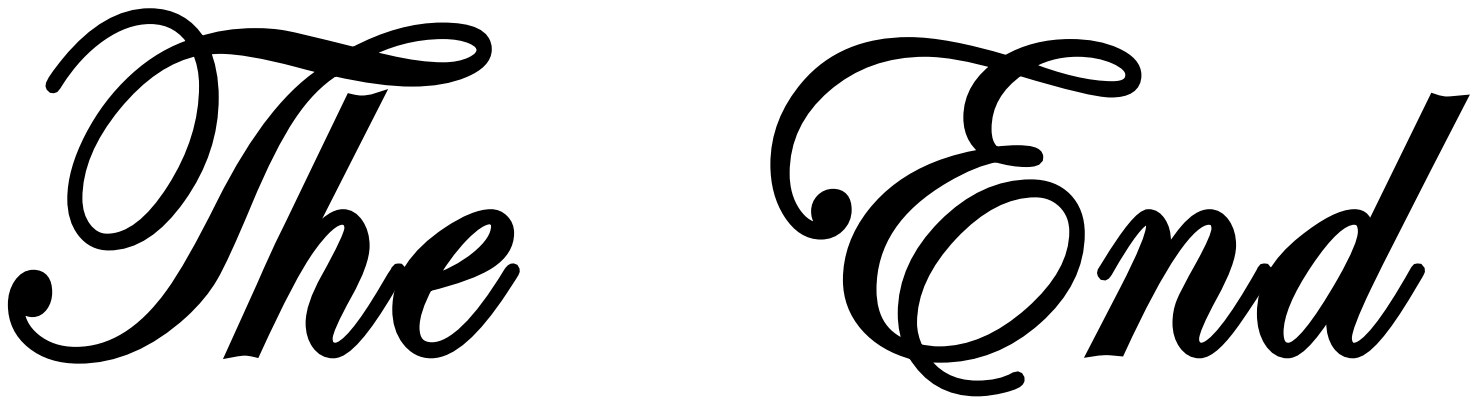
**Example**

Group $(243, 28)$ has a commutator subgroup with elements of both order 9 and 3. And the group can be generated by the elements of order 9, as well as generated by the elements of order 3.

And some perfect groups do satisfy FSC!

**Example**

PSL$(2, q)$ for all appropriate $q$ from 4 through 27.


The End