New Zémor-Tillich Type Hash Functions Over $\mathrm{GL}_2(\mathbb{F}_{p^n})$

Hayley Tomkins, Monica Nevins, and Hadi Salmasian

University of Ottawa, Canada

June 24, 2019

What is a Cayley Hash?

In 1991 Gilles Zémor introduced the idea of building hash functions from Cayley graphs of large girth.

What is a Cayley Hash?

In 1991 Gilles Zémor introduced the idea of building hash functions from Cayley graphs of large girth.

Associated Cayley hash

Given a group G and $g_1, g_2 \in G$, the **associated [Cayley] hash** H is the map defined for any message $m = m_1 \dots m_k \in \{0,1\}^*$ by $H(m) = H(m_1) \cdots H(m_k) \in G$ where $H(0) = g_1$ and $H(1) = g_2$.

What is a Cayley Hash?

In 1991 Gilles Zémor introduced the idea of building hash functions from Cayley graphs of large girth.

Associated Cayley hash

Given a group G and $g_1, g_2 \in G$, the **associated [Cayley] hash** H is the map defined for any message $m = m_1 \dots m_k \in \{0,1\}^*$ by $H(m) = H(m_1) \cdots H(m_k) \in G$ where $H(0) = g_1$ and $H(1) = g_2$.

Small modifications property

Given any collision $H(m) = H(m')$, $\min\{|m|, |m'|\} \geq n$.

In Cayley hashes notions such as collision, second preimage, and preimage resistance are able to be restated as mathematical problems that are believed to be hard.

In Cayley hashes notions such as collision, second preimage, and preimage resistance are able to be restated as mathematical problems that are believed to be hard.

Some examples

- Zémor's original suggestion was to use $g_1 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $g_2 = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ in $\mathrm{SL}_2(\mathbb{F}_p)$ for p a large prime
- Cayley hashes from expander graphs
- Bromberg et. al. suggested using pairs of the form $g_1 = \left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right]$ and $g_2 = \left[\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix}\right]$ in $\mathrm{SL}_2(\mathbb{F}_p)$

The Zémor-Tillich hash function

The **Zémor-Tillich hash function**

The **Zémor-Tillich hash function** is defined as the associated hash function of $G = \mathrm{SL}_2(\mathbb{F}_{2^n})$, $g_1 = \left[\begin{smallmatrix} x & 1 \\ 1 & 0 \end{smallmatrix}\right]$, and $g_2 = \left[\begin{smallmatrix} x & x+1 \\ 1 & 1 \end{smallmatrix}\right]$, where x is the root of the defining polynomial of $\mathbb{F}_{2^n}$.

The Zémor-Tillich hash function

The **Zémor-Tillich hash function**

The **Zémor-Tillich hash function** is defined as the associated hash function of $G = \mathrm{SL}_2(\mathbb{F}_{2^n})$, $g_1 = \left[\begin{smallmatrix} x & 1 \\ 1 & 0 \end{smallmatrix}\right]$, and $g_2 = \left[\begin{smallmatrix} x & x+1 \\ 1 & 1 \end{smallmatrix}\right]$, where x is the root of the defining polynomial of $\mathbb{F}_{2^n}$.

- viably fast
- tends to uniform distribution

The Zémor-Tillich hash function

The **Zémor-Tillich hash function**

The **Zémor-Tillich hash function** is defined as the associated hash function of $G = \mathrm{SL}_2(\mathbb{F}_{2^n})$, $g_1 = \left[\begin{smallmatrix} x & 1 \\ 1 & 0 \end{smallmatrix}\right]$, and $g_2 = \left[\begin{smallmatrix} x & x+1 \\ 1 & 1 \end{smallmatrix}\right]$, where x is the root of the defining polynomial of $\mathbb{F}_{2^n}$.

- viably fast
- tends to uniform distribution

Attacks

- small order attacks (Charnes and Piepryzk, Steinwandt et. al.)
- Geiselmann's embedding attack
- Grassl et. al's palindrome attack

Our contribution

Our hash function construction: *Let* $A, B \in \mathrm{M}_{2\times 2}\left(\mathbb{F}_p[x]\right)$ *and set* $\mathcal{D}$ *to be* $\left\{M \in \mathrm{M}_{2\times 2}\left(\mathbb{F}_p[x]\right) \mid r_n \nmid \det(M)\right\}$. *Define the projection map*

$$\pi_{r_n} : \mathcal{D} \to \mathrm{GL}_2\left(\mathbb{F}_q\right)$$

to be the map taking entries of a matrix to their projection in $\mathbb{F}_q$ *under the quotient by* $\langle r_n \rangle$. *We then construct a hash function* H *by taking the associated hash for* $g_1 = \pi_{r_n}(A)$ *and* $g_2 = \pi_{r_n}(B)$ *and* $G = \mathrm{GL}_2\left(\mathbb{F}_{p^n}\right)$.

Our contribution

Our hash function construction: *Let* $A, B \in \mathrm{M}_{2\times 2}\left(\mathbb{F}_p[x]\right)$ *and set* $\mathcal{D}$ *to be* $\left\{M \in \mathrm{M}_{2\times 2}\left(\mathbb{F}_p[x]\right) \mid r_n \nmid \det(M)\right\}$. *Define the projection map*

$$\pi_{r_n} : \mathcal{D} \to \mathrm{GL}_2\left(\mathbb{F}_q\right)$$

to be the map taking entries of a matrix to their projection in $\mathbb{F}_q$ *under the quotient by* $\langle r_n \rangle$. *We then construct a hash function* H *by taking the associated hash for* $g_1 = \pi_{r_n}(A)$ *and* $g_2 = \pi_{r_n}(B)$ *and* $G = \mathrm{GL}_2\left(\mathbb{F}_{p^n}\right)$.

Our idea:

Use freeness to retain the small modifications property.

The field of **formal Laurent series** over $\mathbb{F}_p$

The elements of $\mathbb{F}_p((x))$ are series of the form

$$g(x) = \sum_{k=m}^{\infty} g_k x^k$$

for $g_i \in \mathbb{F}_p$ and $m \in \mathbb{Z}$.

The field of **formal Laurent series** over $\mathbb{F}_p$

The elements of $\mathbb{F}_p((x))$ are series of the form

$$g(x) = \sum_{k=m}^{\infty} g_k x^k$$

for $g_i \in \mathbb{F}_p$ and $m \in \mathbb{Z}$.

- $\mathrm{PGL}_2\left(\mathbb{F}_p((x))\right)$

The field of **formal Laurent series** over $\mathbb{F}_p$

The elements of $\mathbb{F}_p((x))$ are series of the form

$$g(x) = \sum_{k=m}^{\infty} g_k x^k$$

for $g_i \in \mathbb{F}_p$ and $m \in \mathbb{Z}$.

- $\mathrm{PGL}_2\left(\mathbb{F}_p((x))\right)$
- $\mathrm{GL}_2\left(\mathbb{F}_p((x))\right)$

The field of **formal Laurent series** over $\mathbb{F}_p$

The elements of $\mathbb{F}_p((x))$ are series of the form

$$g(x) = \sum_{k=m}^{\infty} g_k x^k$$

for $g_i \in \mathbb{F}_p$ and $m \in \mathbb{Z}$.

- $\mathrm{PGL}_2\left(\mathbb{F}_p((x))\right)$
- $\mathrm{GL}_2\left(\mathbb{F}_p((x))\right)$
- $\mathbb{P}^1$

Free Generators Theorem

Free Generators Theorem (T. 2018)

Let p be a prime and let $d \in \mathbb{N}_0$. Suppose there exist $a, b, c, \tilde{a}, \tilde{b} \in \mathbb{F}_p((x))$, $f, \tilde{f} \in \mathbb{F}_p((x))^\times$, such that Ξ_1, Ξ_2 and Ξ_3 hold (see next slide). Then the matrices

$$A = \begin{bmatrix} ab - cf & a(f-1) \\ cb(1-f) & abf - c \end{bmatrix} \text{ and } B = \begin{bmatrix} \tilde{b} - \tilde{a}\tilde{f} & \tilde{f} - 1 \\ \tilde{a}\tilde{b}(1-\tilde{f}) & \tilde{b}\tilde{f} - \tilde{a} \end{bmatrix} \tag{1}$$

generate a free group in $\mathrm{PGL}_2\big(\mathbb{F}_p((x))\big)$. In particular, any inverse images of A, B in $\mathrm{GL}_2\big(\mathbb{F}_p((x))\big)$ also generate a free group.

Conditions of the Free Generators Theorem

Ξ_1 : $d([u],[v]) > \frac{1}{p^{d+1}}$ for each pair of $[u],[v]$ in $\left\{[a:c],[1:b],[1:\tilde{a}],[1:\tilde{b}]\right\}$

Ξ_2 : $\min\{|f|,|f^{-1}|\} \leq \frac{1}{p^{2d+1}}$, and $\min\{|\tilde{f}|,|\tilde{f}^{-1}| \leq \frac{1}{p^{2d+1}}\}$

Ξ_3 : There exists $[z] \in \mathbb{P}^1$ such that $d([z],[u]) > \frac{1}{p^{d+1}}$ for each $[u]$ in $\left\{[a:c],[1:b],[1:\tilde{a}],[1:\tilde{b}]\right\}$.

Remark

We can find infinitely many parameters satisfying our theorem for all $d \geq 0$ when p is odd, and all $d > 0$ when $p = 2$.

Some constructions using the Free Generators Theorem

Table: The matrices A and B produced using the Free Generators Theorem for $p > 2$, $d = 0$, $a = 0$, $c = 1$, $f, \tilde{f} \in x\mathbb{F}_p[x]$, and given choices of b, $\tilde{a}$, and $\tilde{b}$.

$\{A, B\}$	A	B	b	$\tilde{a}$	$\tilde{b}$
$G_1(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f}+1 & 1-\tilde{f} \\ 1-\tilde{f} & \tilde{f}+1 \end{pmatrix}$	0	1	-1
$G_2(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f}+1 & \tilde{f}-1 \\ \tilde{f}-1 & \tilde{f}+1 \end{pmatrix}$	0	-1	1
$G_3(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ f-1 & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f} & \tilde{f}-1 \\ 0 & 1 \end{pmatrix}$	1	-1	0
$G_4(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ f-1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1-\tilde{f} \\ 0 & \tilde{f} \end{pmatrix}$	1	0	-1
$G_5(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 1-f & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f} & 1-\tilde{f} \\ 0 & 1 \end{pmatrix}$	-1	1	0
$G_6(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 1-f & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & \tilde{f}-1 \\ 0 & \tilde{f} \end{pmatrix}$	-1	0	1

Benefits of this method

The Free Generators Theorem

- provides many choices of g_1 and g_2 over *any* characteristic
- offers a great amount of control of the degrees and form of the entries in our generators
- extends to an arbitrary number of generators

Benefits of this method

The Free Generators Theorem

- provides many choices of g_1 and g_2 over *any* characteristic
- offers a great amount of control of the degrees and form of the entries in our generators
- extends to an arbitrary number of generators

Our approach provides

- a stronger version of the small modifications property
- a method to prevent against specific small relations
- precise conditions on our parameters for generating a large enough set of hash values

As Cayley hashes, our hash functions are

- scalable
- posses the concatenation property, so in particular can be computed in parallel

As Cayley hashes, our hash functions are

- scalable
- posses the concatenation property, so in particular can be computed in parallel

The methods in our theorem

- can extend to the p-adic field $\mathrm{GL}_2(\mathbb{Q}_p)$
- would work for GL_n for other n
- yield the potential for a keyed hash function

Some Definitions

Note

The following work has been inspired by Breuillard and Gelander's application of Tits' Ping-Pong Lemma.

Some Definitions

Note

The following work has been inspired by Breuillard and Gelander's application of Tits' Ping-Pong Lemma.

Absolute value

If $g_m \neq 0$, the **valuation** of g, $v(g)$, is m and the **absolute value** is $|g| = p^{-v(g)} = p^{-m}$.

Some Definitions

Note

The following work has been inspired by Breuillard and Gelander's application of Tits' Ping-Pong Lemma.

Absolute value

If $g_m \neq 0$, the **valuation** of g, $v(g)$, is m and the **absolute value** is $|g| = p^{-v(g)} = p^{-m}$.

Distance

Let $[u], [v] \in \mathbb{P}^1$ be such that $[u] = [u_1 : u_2]$ and $[v] = [v_1 : v_2]$. Then the **distance** between $[u]$ and $[v]$ is

$$d([u],[v]) = \frac{||u \wedge v||}{||u||\,||v||} = \frac{|u_1 v_2 - u_2 v_1|}{\max\{|u_1|,|u_2|\}\max\{|v_1|,|v_2|\}}.$$

Neighbourhoods in $\mathbb{P}^1$

For $[u] \in \mathbb{P}^1$ we define $N\left([u], \frac{1}{p^{d+1}}\right)$ to be the closed neighbourhood of radius $\frac{1}{p^{d+1}}$.

Neighbourhoods in $\mathbb{P}^1$

For $[u] \in \mathbb{P}^1$ we define $N\left([u], \frac{1}{p^{d+1}}\right)$ to be the closed neighbourhood of radius $\frac{1}{p^{d+1}}$.

Proposition

For each $d \in \mathbb{N}_0$ there exist $p^d(p+1)$ disjoint neighbourhoods of radius $\frac{1}{p^{d+1}}$ such that for any point $[u] \in \mathbb{P}^1$, $N\left([u], \frac{1}{p^{d+1}}\right)$ is precisely one of these neighbourhoods. They are

1. for each $(a_0, a_1, ..., a_d) \in \mathbb{F}_p^{d+1}$, $\{[1 : a_0 + a_1 x + \ldots + a_d x^d + r] \mid r \in x^{d+1}\mathcal{O}\}$, and
2. for each $(0, a_1, ..., a_d) \in \mathbb{F}_p^{d+1}$, $\{[a_1 x + \ldots + a_d x^d + r : 1] \mid r \in x^{d+1}\mathcal{O}\}$.

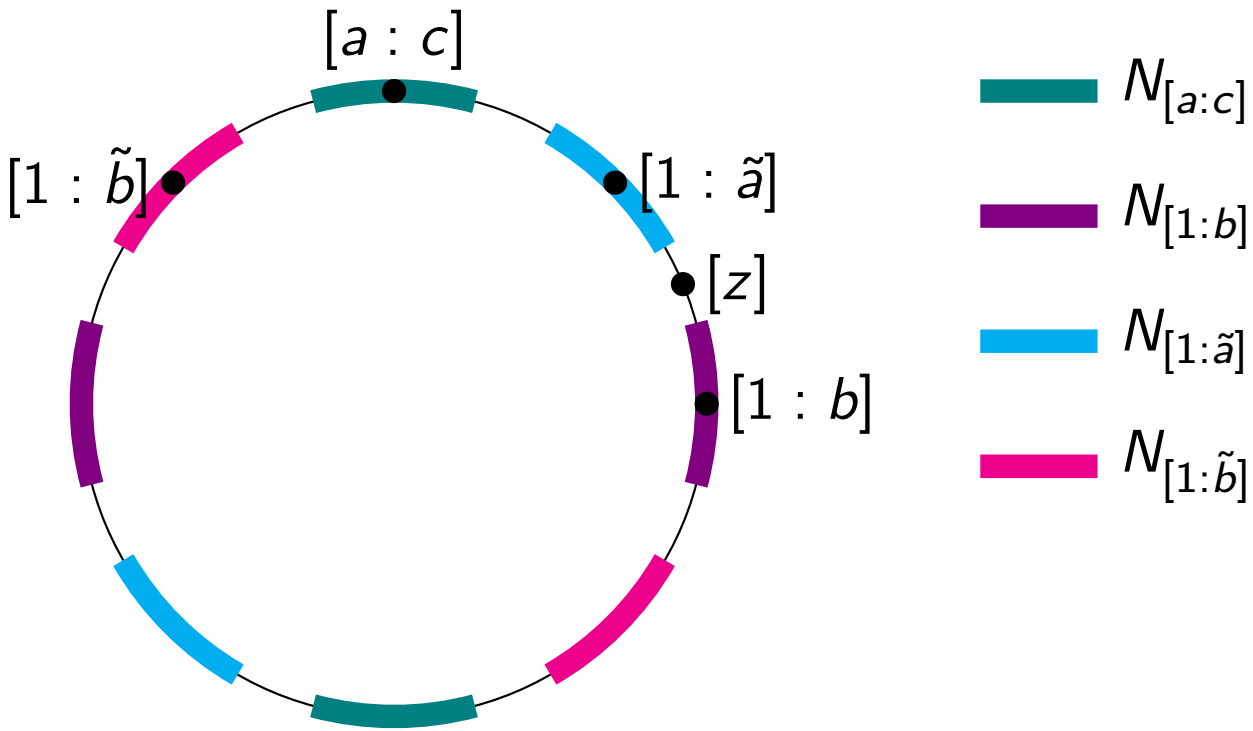


Figure: A visual representation of the $\frac{1}{p^{d+1}}$-neighbourhoods of the eigenvectors of A and B and the point $[z]$. Conditions Ξ_1 and Ξ_3 of Theorem 1 ensure these neigbourhoods are disjoint and the point $[z]$ must lie outside each neighbourhood.

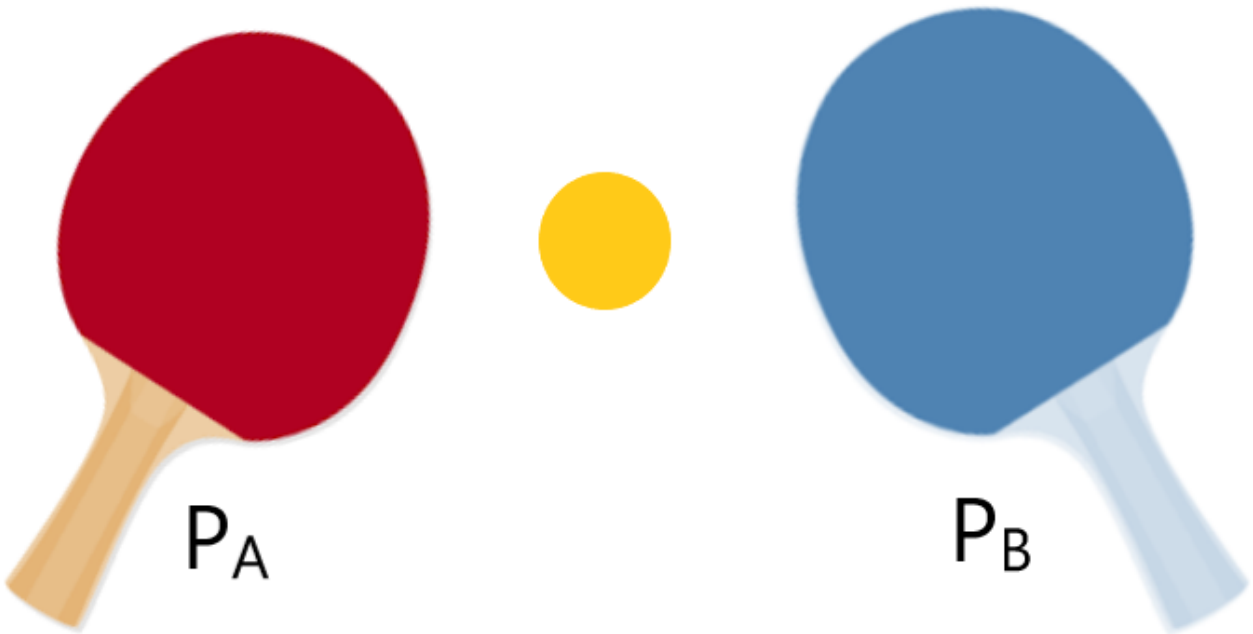
Ping-Pong Lemma (Jacques Tits, 1972)

Given two cyclic groups $\langle A \rangle$ and $\langle B \rangle$, acting on $\mathbb{P}^1$ with associated disjoint sets P_A and P_B in $\mathbb{P}^1$ with the property

- for any $g \in \langle A \rangle$, $g : \mathbb{P}^1 \setminus P_A \to P_A$ and
- for any $g \in \langle B \rangle$, $g : \mathbb{P}^1 \setminus P_B \to P_B$

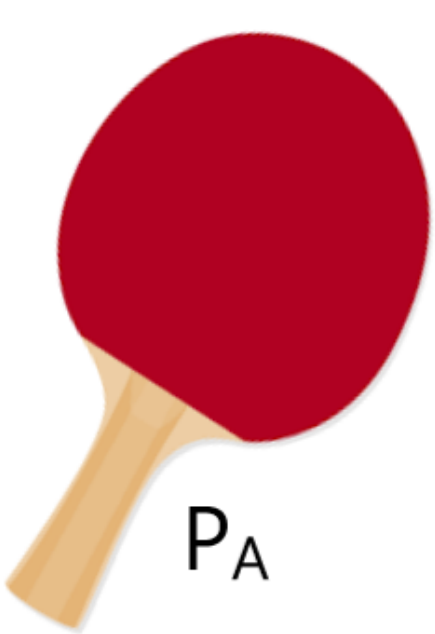
Then, any nontrivial word w in $\{A, B\}$ must necessarily map a point outside of $P_A \cup P_B$ to either P_A or P_B, and thus cannot be identity.

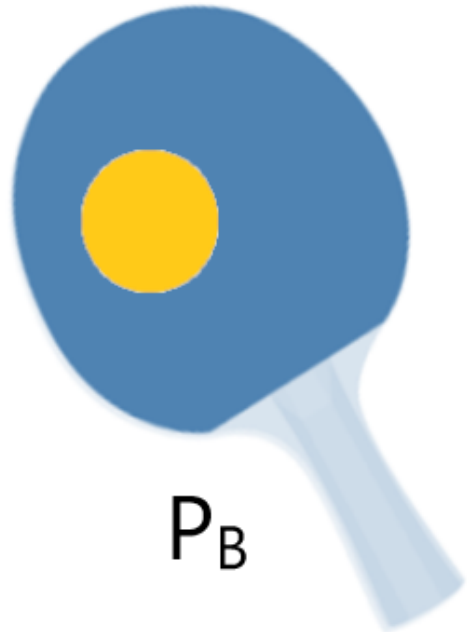
Consider the action of the word $A^2B^{-1}A^5B^4$ on $[z]$



$[z]$

B^4 maps $[z]$ to P_B





$$B^4 \cdot [z]$$

A^5 maps $B^4 \cdot [z]$ to P_A

$$A^5 B^4 \cdot [z]$$

B^{-1} maps $A^5B^4 \cdot [z]$ to P_B

$$B^{-1}A^5B^4 \cdot [z]$$

A^2 maps $B^{-1}A^5B^4 \cdot [z]$ to P_B

$$A^2B^{-1}A^5B^4 \cdot [z]$$

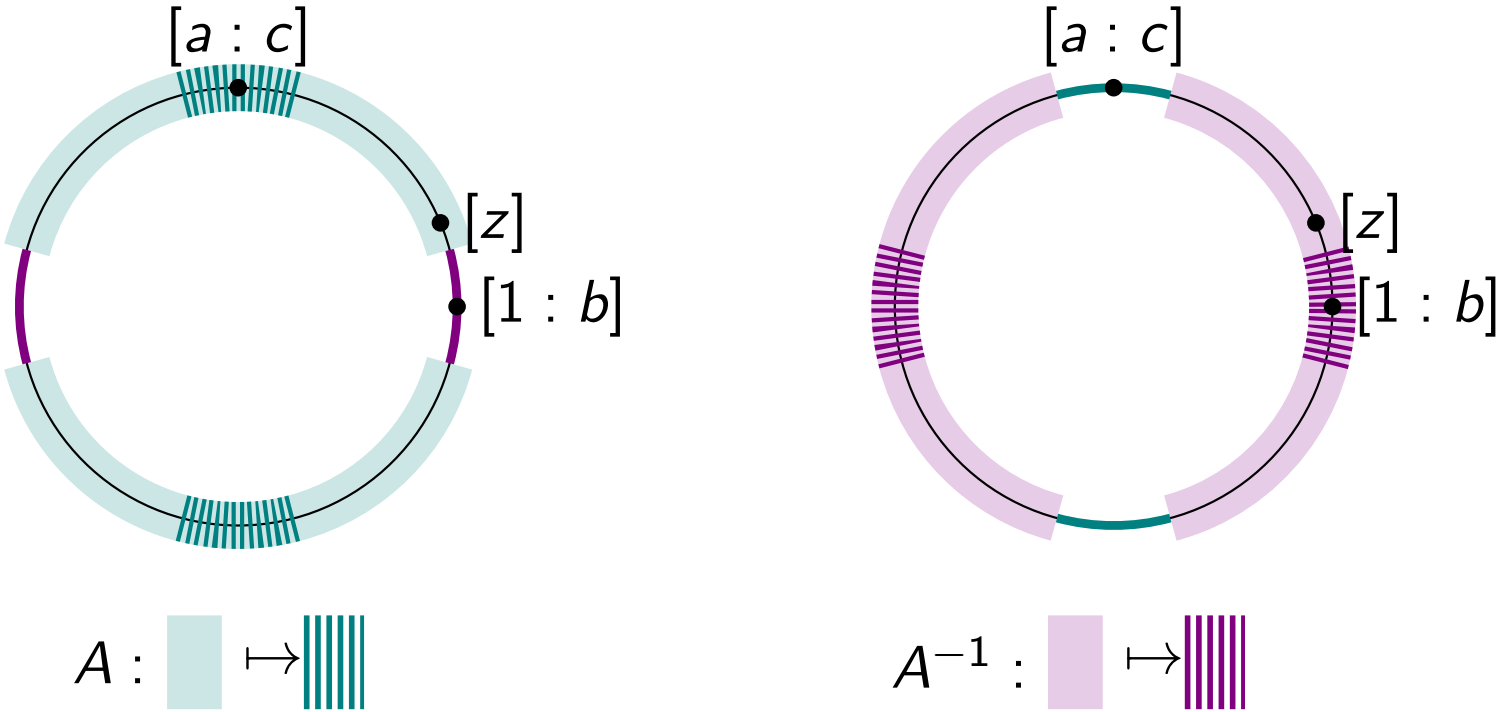


Figure: A visual representation of the action of A and the action of A^{-1} on $\mathbb{P}^1$. We see that A maps $\mathbb{P}^1 \setminus N_{[1:b]}$ to $N_{[a:c]}$ and A^{-1} maps $\mathbb{P}^1 \setminus N_{[a:c]}$ to $N_{[1:b]}$.

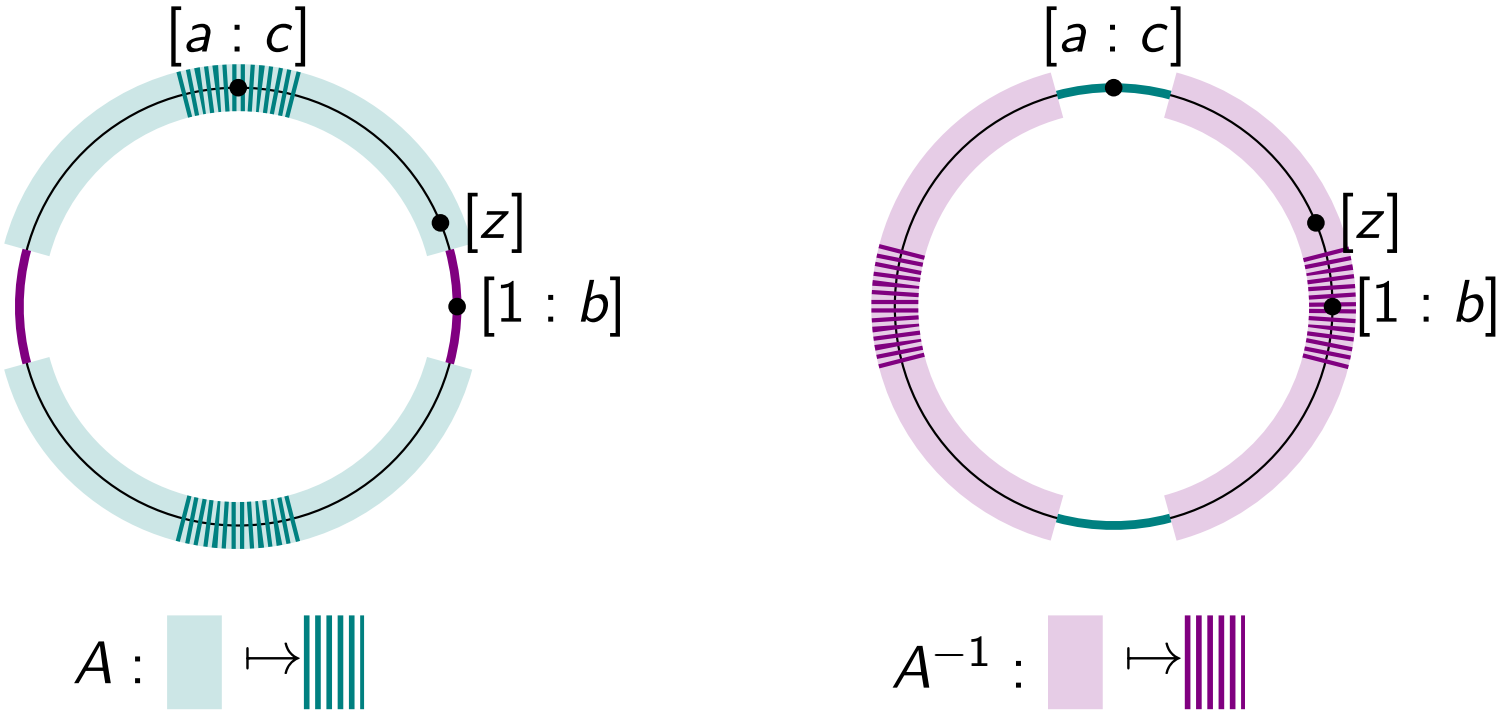


Figure: A visual representation of the action of A and the action of A^{-1} on $\mathbb{P}^1$. We see that A maps $\mathbb{P}^1 \setminus N_{[1:b]}$ to $N_{[a:c]}$ and A^{-1} maps $\mathbb{P}^1 \setminus N_{[a:c]}$ to $N_{[1:b]}$.

We choose $P_A = N_{[a:c]} \cup N_{[1:b]}$ and $P_B = N_{[1:\tilde{a}]} \cup N_{[1:\tilde{b}]}$ and let $[z]$ be a point outside of P_A or P_B. This gives that $\langle A \rangle$ maps $\mathbb{P}^1 \setminus P_A$ to P_A.

Final Remarks

- potential issues from the introduction of the determinant are fixed by padding or choosing $\det(A) = \det(B)$
- our hash function constructions are resistant to attacks on the Zémor-Tillich hash function

Final Remarks

- potential issues from the introduction of the determinant are fixed by padding or choosing $\det(A) = \det(B)$
- our hash function constructions are resistant to attacks on the Zémor-Tillich hash function

Thank you!

References

- G. Zémor. Hash functions and graphs with large girths. In *Advances in Cryptology EUROCRYPT91*, pages 508-511. Springer (1991).
- L. Bromberg, V. Shpilrain, and A. Vdovina. Navigating in the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$ and applications to hashing. *Semigroup forum*, 94(2) 314-324 (2017).
- J.P. Tillich and G. Zémor. Hashing with SL_2. In *Annual International Cryptology Conference*, pages 40-49. Springer, 1994.
- C. Charnes and J. Pieprzyk. Attacking the SL_2 hashing scheme. In *Advances in Cryptology ASIACRYPR'94*, pages 322-330 (1995).
- R. Steinwandt, M. Grassl, W. Geiselmann, and T. Beth. Weaknesses in the $\mathrm{SL}_2(\mathbb{F}_{2^n})$ hashing scheme. In *Annual International Cryptology Conference* pages 287-299. Springer (2000).

- W. Geiselmann. A note on the hash function of Tillich and Zémor. In *Cryptography and coding (Cirencester, 1995)*, Lecture Notes in Comput. Sci., vol. 1025, pages 257-263. Springer, Berlin (1995).
- M. Grassl, I. Ilić, S. Magliveras, and R. Steinwandt. Cryptanalysis of the Tillich-Zémor Hash Function. *Journal of Cryptology*, 24(1):148-156, 2011.
- J. Tits. Free subgroups in linear groups. *Journal of Algebra*, 20(2):250-270, 1972.
- E. Breuillard and T. Gelander. On dense free subgroups of Lie groups. *Journal of Algebra*, 261(2):448-467, 2003.