Randomness properties of $\mathbb{Z}_v$ ElGamal sequences

Daniel Panario[*] Lucas Pandolfo Perin[†] Brett Stevens[*]

[*]Carleton University — Canada
[†]Universidade Federal de Santa Catarina — Brazil
[†]Technical Innovation Institute — United Arab Emirates

2020-08-05

Outline

Introduction

Sidon sets and statistics of the ElGamal function
boppre2020sidon

- Started in 2016 as a research challenge by Joachim von zur Gathen;
- Boppré and Perin wrote a report with experimental analysis;
- By 2017, Ana and Joachim wrote the Sidon Set part and submited to arxiv.
- In 2020, the paper was published in Cryptologia.

ElGamal Permutations

Let $G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ be a cyclic group of order $p-1$

p prime

ElGamal Permutations

Let $G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ be a cyclic group of order $p-1$
p prime

- ElGamal signatures uses the fact that $G = \{g^x : x \in \mathbb{Z}_{p-1}\}$, where g is a generator of G;
- g^x is a unique representation of x, and thus it spans a permutation of G.

ElGamal Permutations

Let $G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ be a cyclic group of order $p-1$
p prime

- ElGamal signatures uses the fact that $G = \{g^x : x \in \mathbb{Z}_{p-1}\}$, where g is a generator of G;
- g^x is a unique representation of x, and thus it spans a permutation of G.

We are interested on the randomness properties of the *ElGamal* map from $\mathbb{Z}_{p-1}$ to G with $b \to g^b$
Lucas: USE BETTER NOTATION FROM PAPER HERE

ElGamal Permutations

Example: Let $p = 5$, then 2 and 3 are generators of $G = \mathbb{Z}_p^\times$.

x	g^x
1	$g^1 = 2$
2	$g^2 = 4$
3	$g^3 = 3$
4	$g^4 = 1$

Table 1: g^x with x in $\mathbb{Z}_5^\times$ and $g = 2$

cycles = {{1,2,4},{3}}

x	g^x
1	$g^1 = 3$
2	$g^2 = 4$
3	$g^3 = 2$
4	$g^4 = 1$

Table 2: g^{x^*} with x in $\mathbb{Z}_5^\times$ and $g = 3$

cycles = {1,2,3,4}

ElGamal Permutations

Example: Let $p = 5$, then 2 and 3 are generators of G = $\mathbb{Z}_p^\times$.

x	g^x
1	$g^1 = 2$
2	$g^2 = 4$
3	$g^3 = 3$
4	$g^4 = 1$

Table 1: g^x with x in $\mathbb{Z}_5^\times$ and $g = 2$

x	g^x
1	$g^1 = 3$
2	$g^2 = 4$
3	$g^3 = 2$
4	$g^4 = 1$

Table 2: g^{x^*} with x in $\mathbb{Z}_5^\times$ and $g = 3$

cycles = {{1,2,4},{3}}

cycles = {1,2,3,4}

- Distinct g produce distinct permutations;
- Distinct g affect the cyclic structures.

Pictorial Representation

Experimentation

Results with Sidon Sets

ElGamal Sequences

- Comparing balanced $\mathbb{Z}_v$-sequences obtained from ElGamal function to random balanced sequences **elgamalsequences**

Randomness properties

- Balance
- Period
- $\lambda(z) = \#\{i \in [0, p-1] : \sigma(i +_n \iota) = z(\iota),\ 0 \leq \iota < t\}$
- $\rho(b, t) =$
  $\#\{i \in [0, p-1] : \sigma(i -_n 1), \sigma(i +_n t) \neq b = \sigma(i +_n \iota),\ 0 \leq \iota < t\}$

ElGamal Run ratio Experiment

Show experiment with ratio against expected from golomb's postulates

Balance

The number of $x \equiv i \mod v$ in $[1, p-1]$ is

$$\lceil (p - 1 - ((i-1) \bmod v))/v \rceil$$

Proposition

Let π be a permutation in $\mathbb{Z}_p^*$, then π_v is a balanced sequence over $\mathbb{Z}_v$ if and only if $v \mid p - 1$.

Period

Lemma

If $p \equiv \alpha \neq 1 \pmod{v}$, *then* π_v *has period* $N = p - 1$ *for any* $\pi : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$.

Proof.

The difference in the number of occurences of any two symbols must be a multiple of $(p-1)/N$. But

$$|\pi_v|_a = \begin{cases} \lceil (p-1)/v \rceil & 0 \leq a < \alpha - 1, \\ \lfloor (p-1)/v \rfloor & \text{otherwise.} \end{cases}$$

$\square$

Period

Theorem

For every $\epsilon > 0$ there exists an n_ϵ so that for all $p \geq n_\epsilon$, the number T of permutations π_v with period $p - 1$ satisfies

$$(p-1)!(1-\epsilon) \leq T \leq (p-1)!. \tag{1}$$

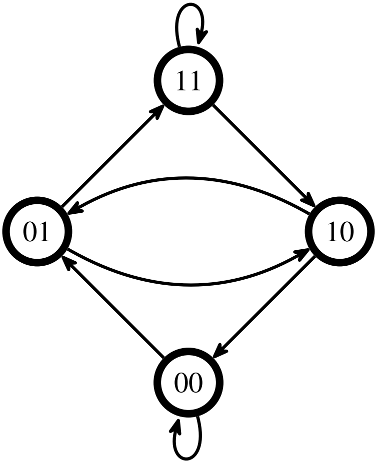
Special case

When q is prime and $p = vq + 1$,

$$(p-1)! - T = v!(q!)^v$$

This includes the case of Sophie Germain primes.

de Bruijn graph



Transfer Matrix

Transfer matrix is directed adjacency matrix of de Bruijn graph with variables

$$T = \begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} ux_0 & ux_0 & 0 & 0 \\ 0 & 0 & x_0 & x_0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

$$C = \begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

$$\sum_{\mathbf{k} \in \mathbb{N}^t} a_n(k) x^{\mathbf{k}} = \sum_{z', z'' \in \mathbb{Z}_v^t} C_{z', z''} T^n_{z', z''}.$$

References I