20th Central European Conference on Cryptology
June 24-26, 2020

Discrete logarithm problem in sandpile groups

Krisztián Dsupin
This is a joint work with Dr. Szabolcs Tengely

University of Debrecen

Table of contents

Discete logarithm problem

General problem

Let G a multiplicative group, $g, h \in G$. The problem is to find an x such that $g^x = h$.

In additive groups

Let G be an additive group, $g, h \in G$, The problem is to find an x such that $x \cdot g = h$.

Sandpile graph

A (V, E, s) triplet is called sandpile graph, if (V, E) is a directed multigraph and $s \in V$ is a globally accessible vertex.

A vertex is globally accessible or sink, if it can be accessed from each of the vertices of the graph G.

Configurations

Configuration

A configuration over G is a $c : V \to \mathbb{Z}$ function, such that $c(v) \geqslant 0$ for all $v \in V^*$, furthermore $c(s) = -\sum_{v \in \tilde{V}} c(v)$, and denoted by $c = (c_1, \ldots, c_n)$.

Stable configuration

A c configuration is stable in $v \in V \backslash \{s\}$, if $c(v) \leqslant d^-(v)$. Otherwise, c is unstable.

Stabilization

An unstable c configuration can be fired, which gives a $\tilde{c}$ configuration. It means we reduce $c(v)$ by $d^-(v)$, and every adjacent u vertex of v increases by 1. So that

$$\tilde{c}(v) = \begin{cases} c(u) - d^-(u), & \text{if } u = v, \\ c(u) + 1, & \text{if } u \text{ and } v \text{ are adjacent}, \\ c(v), & \text{other}. \end{cases}$$

We say a firing is legal, if c is unstable at v.

Sandpile group

Stable addition

Let $\mathcal{M}$ denote the set of nonnegative stable configurations on G. Then $\mathcal{M}$ is a commutative monoid under stable addition

$$a \circledast b := (a + b)^{\circ}.$$

A stable addition is a vector addition in $\mathbb{N}\tilde{V}$ followed by stabilization.

Accesible configuration

A configuration c is accessible if for each configuration a, there exists a configuration b such that $a + b \to c$.

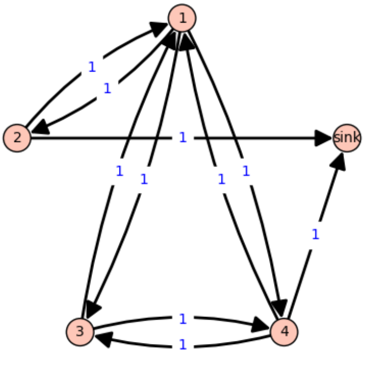
Recurrent configuration

A configuration c is recurrent if it is nonnegative, accessible, and stable.

Sandpile group

The collection of recurrent configurations of G forms a group under stable addition, that is called the sandpile group of G and denoted by $\mathcal{S}(G)$.

Example



Elements of sandpile group

$$
\begin{aligned}
c_1 &= (2,1,1,2)\\
c_2 &= (2,0,1,2)\\
c_3 &= (1,1,1,2)\\
c_4 &= (1,0,1,2)\\
c_5 &= (0,1,1,2)\\
c_6 &= (1,1,0,2)\\
c_7 &= (2,0,0,2)\\
c_8 &= (2,1,0,2)\\
c_9 &= (2,1,0,1)\\
c_{10} &= (2,1,1,1)\\
c_{11} &= (2,1,1,0)
\end{aligned}
$$

Divisor

The D divisors of the G groups are the elements of

$$Div(G) = \{ \sum_{v \in V(G)} a_v(v) \mid a_v \in \mathbb{Z} \}$$

Monodromy pairing

Let P be an arbitrary pseudoinverse of the L Laplacian matrix, then monodromy pairing can define as the following:

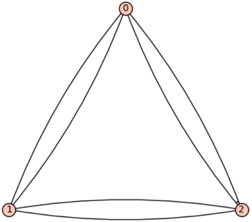
$$\langle D_1, D_2 \rangle = [D_1]^T P [D_2] \pmod{\mathbb{Z}}.$$

Solving DLP

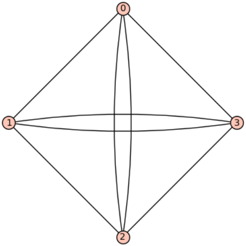
Input: $D_1, D_2 \in Div^0(G)$, where $\overline{D_2} = x \cdot \overline{D_1}$ in $\mathrm{Jac}(G)$
Output: $x \pmod{ord(\overline{D_1})}$

1. Compute $\langle \overline{D_1}, g \rangle = r_1 + \mathbb{Z}$ and $\langle \overline{D_2}, g \rangle = r_2 + \mathbb{Z}$.
2. Solve the $r_2 = r_1 x + y$ Diophantine equation to get $x \pmod{ord(\overline{D})}$.

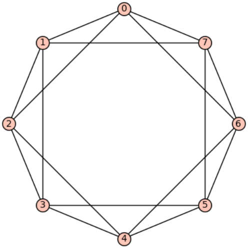
C_n^2 Square cycle



(a) $n = 3$



(b) $n = 4$



(c) $n = 8$

Square cycle

Let n be a positive integer, and C_n a cycle graph with $V = \{v_1, \dots, v_n\}$ vertices. Than C_n^2 square cycle is a 4-regular graph with vertex set V, and ith vertex is adjacent to $i \pm 1 \pmod{n}$ and $i \pm 2 \pmod{n}$ vertices.

Structure of $\mathcal{S}(C_n^2)$

The sandpile group of C_n^2 is the direct sum of two or three cyclic groups, which are the followings:

$$\mathcal{S}(C_n^2) \cong \mathbb{Z}_{(n,F_n)} \oplus \mathbb{Z}_{F_n} \oplus \mathbb{Z}_{\frac{nF_n}{(n,F_n)}}.$$

Solving DLP

1. Compute $L = D - A$ Laplace-matrix and P pseudoinverse
2. Specify $D_{g_1}, D_{g_2}, D_{g_3}$ divisors of g_1, g_2, g_3 generators
3. Compute divisors of c_1 and c_2 configurations

Solving DLP in cyclic groups

4. $D_{c_1} \cdot P \cdot D_{g_1}$ and $D_{c_2} \cdot P \cdot D_{g_1}$
   $D_{c_1} \cdot P \cdot D_{g_2}$ and $D_{c_2} \cdot P \cdot D_{g_2}$
   $D_{c_1} \cdot P \cdot D_{g_3}$ and $D_{c_2} \cdot P \cdot D_{g_3}$
   pairings gives solutions for Diophantine equations modulo $ord(g_1), ord(g_2), ord(g_3)$

5. Solving that congruence system with Chinese remainder theorem, the solution of the DLP can be given.

Generalised inverse

k-circulant matrix

A square $A = (a_{ij})$ matrix is k-circulant, it there exists a k such that the matrix has the form of

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ ka_{n-1} & ka_0 & a_1 & \dots & a_{n-2} \\ ka_{n-2} & ka_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ka_1 & ka_2 & ka_3 & \dots & a_0 \end{pmatrix}.$$

Generalised inverse

Let A an $n \times n$ k-circulant matrix with first row $a_0, \dots, a_{n-1}$ and with $\mu_0, \dots, \mu_{n-1}$ eigenvalues. Let ω be primitive nth root of unity, and suppose $\lambda^n = k$. Then the first row $b_0, \dots, b_{n-1}$ of A^s is given by

$$b_i = \frac{1}{n} \sum_{j=0}^{n-1} \beta_j (\lambda \omega^j)^{-i}, \quad i = 0, 1, \dots, n-1,$$

where

$$\beta_j = \begin{cases} 0 & \text{if } \mu_j = 0; \\ \frac{1}{\mu_j} & \text{if } \mu_j \neq 0. \end{cases}$$

Suppose that the generators of C_n^2 are g_i, the input configurations of the DLP problems are c_j, than the monodromy pairings are given by the following form.

$$P \cdot g_i = \begin{pmatrix} v_{i,0} \\ v_{i,1} \\ \vdots \\ v_{i,n-1} \end{pmatrix}, \text{where}$$

$$v_{i,k} = \begin{cases} \sum_{l=0}^{n-1} p_l \cdot g_l & \text{if } k = 0; \\ \sum_{l=0}^{n-1} \cdot p_{l-k \pmod n} \cdot g_l & \text{if } k \neq 0. \end{cases}$$

Monodromy pairing in C_n^2

The monodromy pairing can also be given by

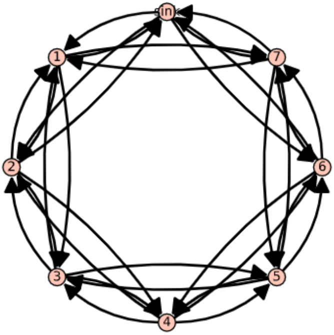
$$c_j \cdot P \cdot g_i = \sum_{l=0}^{n-1} c_{j,l} \cdot v_{i,l} = c_0 \cdot \sum_{l=0}^{n-1} p_l \cdot g_l + \sum_{k=1}^{n-1} c_k \sum_{l=0}^{n-1} p_{l-k \pmod n} \cdot g_l,$$

Conclusion

With this method the monodromy pairing can express explicitly, and the solution of the DLP is depending on solving at most three Diophantine equations and the congruence system.

Size of the graph 8

Input configurations [(2, 2, 3, 2, 3, 1, 3), (3, 3, 0, 3, 1, 2, 1)]



The L pseudoinverse of $\mathcal{S}(G)$=
$$\begin{pmatrix}
\frac{145}{672} & \frac{1}{224} & -\frac{1}{96} & -\frac{15}{224} & -\frac{47}{672} & -\frac{15}{224} & -\frac{1}{96} & \frac{1}{224} \\
\frac{1}{224} & \frac{145}{672} & \frac{1}{224} & -\frac{1}{96} & -\frac{15}{224} & -\frac{47}{672} & -\frac{15}{224} & -\frac{1}{96} \\
-\frac{1}{96} & \frac{1}{224} & \frac{145}{672} & \frac{1}{224} & -\frac{1}{96} & -\frac{15}{224} & -\frac{47}{672} & -\frac{15}{224} \\
-\frac{15}{224} & -\frac{1}{96} & \frac{1}{224} & \frac{145}{672} & \frac{1}{224} & -\frac{1}{96} & -\frac{15}{224} & -\frac{47}{672} \\
-\frac{47}{672} & -\frac{15}{224} & -\frac{1}{96} & \frac{1}{224} & \frac{145}{672} & \frac{1}{224} & -\frac{1}{96} & -\frac{15}{224} \\
-\frac{15}{224} & -\frac{47}{672} & -\frac{15}{224} & -\frac{1}{96} & \frac{1}{224} & \frac{145}{672} & \frac{1}{224} & -\frac{1}{96} \\
-\frac{1}{96} & -\frac{15}{224} & -\frac{47}{672} & -\frac{15}{224} & -\frac{1}{96} & \frac{1}{224} & \frac{145}{672} & \frac{1}{224} \\
\frac{1}{224} & -\frac{1}{96} & -\frac{15}{224} & -\frac{47}{672} & -\frac{15}{224} & -\frac{1}{96} & \frac{1}{224} & \frac{145}{672}
\end{pmatrix}$$

Generators of $\mathcal{S}(G)$:
$(3, 2, 3, 2, 2, 0, 2)$
$(1, 3, 3, 2, 3, 3, 0)$

Using the 1. generator:

$$D_{c_1} \cdot P \cdot D_g = \frac{1376}{21} = 65 + \frac{11}{21}$$

$$D_{c_2} \cdot P \cdot D_g = \frac{353}{7} = 50 + \frac{3}{7}$$

Solving the following Diophantine equation: $\frac{11}{21}x + y = \frac{3}{7}$

It's solution:
$x_1 = 18\ (mod\ 21)$

Using the 2. generator:

$$D_{c_1} \cdot P \cdot D_g = \frac{11911}{168} = 70 + \frac{151}{168}$$

$$D_{c_2} \cdot P \cdot D_g = \frac{3097}{56} = 55 + \frac{17}{56}$$

Solving the following Diophantine equation: $\frac{151}{168}x + y = \frac{17}{56}$

It's solution:
$x_2 = 165\ (mod\ 168)$

Using the the solutions of the Diophantine equations and the Chinese remainder theorem
Solution of the DLP is $x = 165$.

References

- Hou, Yaoping and Woo, Chingwah and Chen, Pingge, *On the sandpile group of the square cycle C_n^2*, Linear Algebra and its Applications,(2006).
- R.E. Cline and R.J. Plemmons and G. Worm, *Generalized inverses of certain Toeplitz matrices*, Linear Algebra and its Applications,(1974).
- F. Shokrieh, *The monodromy pairing and discrete logarithm on the Jacobian of finite graphs*, Journal of Mathematical Cryptology,(2009).

Thank you for your attention!