The Critical Group from a Cryptographic Perspective

Norman Biggs

Centre for Discrete and Applicable Mathematics
London School of Economics
Houghton Street
London WC2A 2AE
U.K.
n.l.biggs@lse.ac.uk

June 2006

CDAM Research Reports Series LSE-CDAM 2006-07

Abstract

The critical group of a graph is an abelian group that arises in several contexts, and there are some similarities with the groups that are used in cryptography. We construct a family of graphs whose critical groups are cyclic, and discuss the associated computational problems using algorithms based on the theory of 'chip-firing'.

MSC: 05C25, 05E99, 94A60

The Critical Group from a Cryptographic Perspective

1. Introduction

What do we mean when say that a finite abelian group K is *given*? In practice, we must be able to (i) represent the elements of K as bit-strings; (ii) recognise the bit-strings that do represent elements of K; (iii) calculate the 'sum' $c = a*b$ of any two elements, and the inverse $-a$; and (iv) compute the number $|K|$.

The 'goodness' of an algorithm for solving a specific problem in K is relative to these basic operations. For example, given any $k \in K$ and $n \in \mathbb{N}$ there is a well-known algorithm for calculating $n.k = k * k * \ \cdots\ * k \ \in \ K$. This method requires $O(\log n)$ sum operations, and is regarded as 'good'. On the other hand, suppose we are given k and h in K and we know that $h = n.k$ for some $n \in \mathbb{N}$; for example, because K is cyclic and k is a generator. The problem of finding the value of n is known as the *The Discrete Logarithm Problem*, and in many cases no 'good' algorithm for it is known.

This situation is the basis of a system of public-key cryptography, using formulae proposed by ElGamal [**5**]. Briefly, suppose a cyclic group K and a generator k are given. A typical user (Bob) chooses a *private key* $b' \in \mathbb{N}$ and calculates a public key $b = b'.k \in K$. If another user (Alice) wishes to send Bob a message m (coded as an element of K), she chooses a temporary tag $t \in \mathbb{N}$ and sends the two-part code $h = t.k$, $c = m * t.b$. Bob can decode (h, c) because $c - b'.h = m$. But another user (Eve) cannot apply this formula unless she can find b', and that is an instance of the Discrete Logarithm Problem. In the original implementation of the ElGamal system K was taken to be the multiplicative group of a finite field $\mathbb{F}_q$, which is cyclic of order $q - 1$. A great deal of work has been done on the Discrete Logarithm Problem in this context. Sub-exponential algorithms are known, and in practice this means that very large numbers must be used in order to achieve an acceptable level of security.

For that reason, there has been considerable interest in the case when K is a subgroup of the Jacobian of a hyperelliptic curve $y^2 = \phi(x)$ over a finite field $\mathbb{F}_q$, where ϕ is a polynomial of degree $2g + 1$. In the case $g = 1$ the curve is an *elliptic curve* and the Jacobian is essentially the curve itself. The basic operations can be defined by simple formulae, but the determination of a suitable subgroup K is an art, rather than a science. However, suitable choices have been found, and the method is popular because no one has yet discovered a 'good' algorithm for the Discrete Logarithm Problem in this context.

In this paper the *critical group* (also known as the *sandpile group*) of a finite graph will be studied from this point of view. Specifically, a family of graphs with cyclic critical groups will be constructed, and the associated computational problems will be discussed.

2. The critical group of a graph

Let G be a connected graph with vertex-set V and edge-set E. We impose an arbitrary *orientation* $h, t : E \to V$, so that $h(e)$ and $t(e)$ are the *head* and *tail* of e.

Let $C^0(G;\mathbb{R})$, $C^1(G;\mathbb{R})$ denote the sets of real-valued functions defined on V and E, endowed with the standard structure as vector spaces with an inner product. The linear transformation $D : C^1(G;\mathbb{R}) \to C^0(G;\mathbb{R})$ defined by

$$(Df)(v) = \sum_{h(e)=v} f(e) \; - \sum_{t(e)=v} f(e),$$

is represented by the *incidence matrix* of G. Its kernel $Z = \mathrm{Ker}D$ is the *flow space*, and the orthogonal complement of Z, $B = Z^\perp$ is the *cut space*. By definition $C^1(G;\mathbb{R}) = Z \oplus B$.

The orthogonal projection $P : C^1(G;\mathbb{R}) \to B$ can be defined explicitly in terms of the spanning trees of G, an observation that goes back to Kirchhoff in 1847. A discussion in modern terms is given in [**2**], where the formula is written in the form $P = \kappa^{-1}XD$. Here κ is the tree number of G and $X : C^0(G;\mathbb{R}) \to C^1(G;\mathbb{R})$ is defined in terms of the set of spanning trees. This formula enables us to express every real-valued function on the edges of G as the sum of a (real-valued) flow and a (real-valued) cut.

The situation regarding integer-valued functions is more complicated. Define the abelian groups

$$C_I = C^1(G;\mathbb{Z}), \quad Z_I = Z \cap C_I, \quad B_I = B \cap C_I.$$

A typical $c \in C_I$ can be written as $c = (c - Pc) + Pc$, which is in $Z_I \oplus B_I$ if and only if Pc is in B_I. The formula $P = \kappa^{-1}XD$ shows that Pc has non-integral values, in general, and so $Z_I \oplus B_I$ is a proper subgroup of C_I. The quotient group is the *critical group* of G:

$$\mathcal{K}(G) = \frac{C_I}{Z_I \oplus B_I}.$$

Bacher, de la Harpe and Nagnibeda [**1**] showed that the critical group arises in several contexts. It is isomorphic to the *Picard group*

$$\mathcal{P}(G) = \frac{D(C_I)}{D(B_I)},$$

where $D(C_I)$ is in fact the same as the group of integer-valued functions f on V for which $\sum_v f(v) = 0$, otherwise known as the *divisors of degree* 0. In the same vein, the elements of $D(B_I)$ are *principal divisors.* The critical group is also isomorphic to the *Jacobian group*

$$\mathcal{J}(G) = \frac{Z_I^\sharp}{Z_I},$$

where $Z_I^\sharp$ is the dual of Z_I considered as a lattice in Z, the vector space of real-valued functions.

These isomorphisms lead to important theoretical results about $\mathcal{K}(G)$. Most interesting is the fact that the order of $\mathcal{K}(G)$ is equal to the tree number κ of G. This fact also has practical importance, because κ is determined by the spectrum of G, and can be computed by 'good' algorithms.

On the other hand, the isomorphism class of $\mathcal{K}(G)$ is not determined by the spectrum of G. The classification theorem for finite abelian groups asserts that $\mathcal{K}(G)$ can be expressed as a direct sum of cyclic groups

$$\mathcal{K}(G) \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ \cdots \ \oplus \mathbb{Z}_{n_r},$$

where $n_i \mid n_{i+1}$ $(1 \leq i \leq r-1)$. The standard method of determining the integers n_i is to reduce a 'relations matrix' to its *Smith normal form.* In the case of $\mathcal{K}(G)$ the Picard definition implies that a relations matrix L_r can be obtained from the discrete Laplacian matrix DD' by deleting any one row and column. It follows that if the Smith normal form of L_r is

$$\mathrm{diag}(n_1, n_2, \ \ldots \ n_r),$$

then the n_i are the integers that occur in the canonical form of $\mathcal{K}(G)$. Equivalently, $\mathcal{K}(G)$ is the cokernel of the reduced Laplacian L_r.

We shall use an alternative to L_r, due to Kotani and Sunada [**8**]. They define, for a given spanning tree T of G, a matrix F that represents the intersections of the fundamental cycles determined by T. It can be shown that

$$\mathcal{K}(G) = \text{coker } L_r = \text{coker } F.$$

3. A family of graphs with cyclic critical groups

The *wheel graph* is obtained from a cycle by adding one new vertex, and new edges joining it to each vertex of the cycle. We shall refer to the cycle as the *rim*, and the new edges as the *spokes.* It is known [**3**] that the critical group of a wheel graph with $2n+1$ spokes is the direct sum of two cyclic groups of order ℓ_{2n+1}, where ℓ_{2n+1} is the Lucas number defined below.

The *Fibonacci numbers* f_n are defined by the recursion $f_1 = 1$, $f_2 = 1$ and $f_n = f_{n-1}+f_{n-2}$ $(n \geq 3)$. The *Lucas numbers* ℓ_n are defined by $\ell_1 = 1, \ell_2 = 3$ and $\ell_n = \ell_{n-1} + \ell_{n-2}$ $(n \geq 3)$. These numbers are related by the identity $\ell_n = f_{n+1} + f_{n-1}$, and they satisfy many other identities, some of which we shall use in the proofs that follow. A useful summary is given by Honsberger [**7**].

We shall show that, given a wheel W with an $2n+1$ spokes, inserting a new vertex in a single rim edge produces a graph $W^\dagger$ whose critical group is cyclic of order $2\ell_{2n+1}f_{2n+2}$. (In fact, a general result of Chen and Ye [**4**] asserts that for any given graph there is a homeomorphic graph with cyclic critical group.) Our result will be proved by examining the matrices that reduce the respective cycle intersection matrices to their Smith normal forms.

Let T be the spanning tree in formed by the spokes in W. There are $2n+1$ fundamental cycles with respect to T, each of length 3, and the cycle intersection matrix is the circulant of size $2n+1$,

$$W = \text{circ}(3, -1, 0, \ldots, 0, -1).$$

Note that we denote the graph and the intersection matrix of its fundamental cycles by the same letter. In the case of W, the matrix is the same as the reduced Laplacian, because the graph is planar and self-dual.

Let $T^\dagger$ be the spanning tree of $W^\dagger$ formed by the spokes and one of the edges incident with the new vertex x. The other edge incident with x defines a cycle of length 4 with respect to $T^\dagger$, and the cycle intersection matrix is obtained from W by adding 1 to the appropriate diagonal entry, which we shall take as the last one. We shall denote this matrix by $W^\dagger$.

Let U, V be the matrices in $GL(2n+1, \mathbb{Z})$ that reduce W to its Smith normal form:

$$UWV = S = \mathrm{diag}(1, 1, 1, \ldots, 1, \ell_{2n+1}, \ell_{2n+1}).$$

We study the matrices $Y = U^{-1}$ and $Z = V^{-1}$, which are such that

$$YSZ = W = \mathrm{circ}(3, -1, 0, \ldots, 0, 0, -1).$$

Suppose that the rows and columns of Y and Z are partitioned into blocks of size $2n-1$ and 2, and the resulting partitioned matrices are

$$Y = \begin{pmatrix} A & B \\ C & M \end{pmatrix}, \qquad Z = \begin{pmatrix} P & Q \\ N & R \end{pmatrix}.$$

For example, A is a square matrix of size $2n-1$, and R is a square matrix of size 2. In Theorem 1 we give explicit definitions of the submatrices A, B, C, M, P, Q, N, R, valid for all $n \geq 5$. (The cases $n = 1, 2, 3, 4$ are similar, but irregular.) In Theorem 2 we shall prove that the corresponding submatrices for the modified wheel can be obtained by changing only the matrix R and six parameters, specifically those denoted by $\alpha, \beta, \gamma, \delta, \lambda, \mu$ in the following definitions.

Theorem 1 Define matrices A, B, C, M, P, Q, N, R as follows.

$$A = \begin{pmatrix} 3 & -1 & 0 & 0 & . & . & 0 & 0 & 0 \\ -1 & 3 & -1 & -f_4 & . & . & -f_{4n-10} & -f_{4n-8} & -f_{4n-6} \\ 0 & -1 & 3 & f_6 & . & . & f_{4n-8} & f_{4n-6} & f_{4n-4} \\ 0 & 0 & -1 & 0 & . & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & . & . & 0 & -1 & 0 \end{pmatrix}; \quad B = \begin{pmatrix} 0 & 0 \\ \alpha & \beta \\ \gamma & \delta \\ 0 & 0 \\ . & . \\ . & . \\ 0 & 0 \\ 0 & 0 \end{pmatrix};$$

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & . & . & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & . & . & 0 & 0 & 0 \end{pmatrix}; \qquad M = O;$$

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & . & . & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & . & . & 0 & 0 \\ 0 & 0 & 1 & -3 & 1 & . & . & 0 & 0 \\ 0 & 0 & 0 & 1 & -3 & . & . & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 & . & . & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 & . & . & 0 & 1 \end{pmatrix}; \quad Q = \begin{pmatrix} 1 & \lambda \\ 3 & \mu \\ 0 & 0 \\ 0 & 0 \\ . & . \\ 0 & 0 \\ 1 & 0 \\ -3 & 1 \end{pmatrix};$$

$$N = O; \quad R = \begin{pmatrix} 1 & 0 \\ 4 & -1 \end{pmatrix}.$$

Then, for all $n \geq 5$, values of the parameters can be found so that the resulting matrices Y and Z belong to $\mathrm{GL}(2n+1, \mathbb{Z})$ and satisfy $YSZ = W$. In fact we can take $\lambda = -3$, $\mu = -8$ and

$$\alpha = \ell_{2n-8}, \quad \beta = -f_{2n-7}, \quad \gamma = -\ell_{2n-6}, \quad \delta = f_{2n-5}.$$

Proof Putting $\lambda = -3$ and $\mu = -8$, direct calculation of AP and CQ establishes that

$$W = \mathrm{circ}(3, -1, 0, \ldots, 0, -1) = \begin{pmatrix} AP & C' \\ C & CQ \end{pmatrix}.$$

Putting $\ell = \ell_{2n+1}$ we have

$$S = \mathrm{diag}(1, 1, 1, \ldots, \ell, \ell) = \begin{pmatrix} I & O \\ O & \ell I \end{pmatrix}.$$

Given that M and N are zero matrices, the condition $YSZ = W$ is therefore equivalent to

$$\begin{pmatrix} AP & AQ + B\ell R \\ CP & CQ \end{pmatrix} = \begin{pmatrix} AP & C' \\ C & CQ \end{pmatrix}.$$

Thus we have to check that $CP = C$ and $AQ + B\ell R = C'$, and the only nontrivial equations arise from the second and third rows of $AQ + B\ell R$. Inserting the given values of λ and μ, and using the identity $f_{m+2} = 3f_m - f_{m-2}$ these equations are

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \ell R = \begin{pmatrix} -f_{4n-4} - 8 & f_{4n-6} + 21 \\ f_{4n-2} + 3 & -f_{4n-4} - 8 \end{pmatrix}.$$

The matrix on the right-hand side can be simplified by observing that $f_4 = 3$, $f_6 = 8$, $f_8 = 21$, and applying the identity $f_{a+k} + f_{a-k} = \ell_a f_k$ (k odd). The result is

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \ell R \;=\; \ell_{2n+1} \begin{pmatrix} -f_{2n-5} & f_{2n-7} \\ f_{2n-3} & -f_{2n-5} \end{pmatrix}.$$

Since $\ell = \ell_{2n+1}$, $R = R^{-1}$, and $\ell_m = f_{m+1} + f_{m-1}$, the solution is $\alpha = \ell_{2n-8}$, $\beta = -f_{2n-7}$, $\gamma = -\ell_{2n-6}$, $\delta = f_{2n-5}$, as claimed.

Finally, it can be proved by elementary means that $\det W = \det S = \ell^2_{2n+1}$, and so $\det Y \det Z = 1$. Since the elements of Y and Z are integers, this implies that Y and Z belong to $\mathrm{GL}(2n+1, \mathbb{Z})$. □

The modifications required to deal with $W^\dagger$ are mainly concerned with finding a suitable replacement for R. The following lemma contains the crucial result.

Lemma 1 If $n \geq 5$ is an odd number, then $x_{2n+1} = f_{2n-2}/3$ is an integer such that

$$x_{2n+1}(f_{2n-2} + f_{2n+2}) = f^2_{2n-1} - 1.$$

Proof If $n = 2m + 1$, then $2n - 2 = 4m$, and f_{4m} is divisible by $f_4 = 3$. Since $f_{2n-2} + f_{2n+2} = 3f_{2n}$ and $f_{2n-2}f_{2n} = f^2_{2n-1} - 1$, it follows that

$$x_{2n+1}(f_{2n-2} + f_{2n+2}) = (f_{2n-2}/3)(3f_{2n}) = f^2_{2n-1} - 1.$$

□

Corollary For all $n \geq 5$ the following matrix $R^\dagger_n$ has determinant 1:

$$\text{if } n \text{ is odd} \quad R^\dagger_n = \begin{pmatrix} \ell_{2n+1} & f_{2n-1} \\ -(x_{2n+1} + f_{2n-1}) & -x_{2n+1} \end{pmatrix},$$

$$\text{if } n \text{ is even} \quad R^\dagger_n = \begin{pmatrix} \ell_{2n+1} & f_{2n-1} \\ x_{2n-1} + f_{2n-3} + \ell_{2n-1} & x_{2n-1} + f_{2n-3} \end{pmatrix}.$$

Proof When n is odd,

$$\begin{aligned} \det R^\dagger_n &= -\ell_{2n+1}x_{2n+1} + f_{2n-1}(x_{2n+1} + f_{2n-1}) \\ &= (-f_{2n+2} - f_{2n} + f_{2n-1})x_{2n+1} + f^2_{2n-1} \\ &= -x_{2n+1}(f_{2n+2} + f_{2n-2}) + f^2_{2n-1} \\ &= 1. \end{aligned}$$

There is a similar calculation when n is even. □

Theorem 2 Let A, B, C, M, P, Q, N be as in Theorem 1, and let $R_n^\dagger$ be as in the Corollary above. Then the parameters $\alpha, \beta, \gamma, \delta, \lambda, \mu$ can be chosen so that, for all $n \geq 5$ the matrices

$$Y = \begin{pmatrix} A & B \\ C & M \end{pmatrix}, \qquad Z^\dagger = \begin{pmatrix} P & Q \\ N & R_n^\dagger \end{pmatrix},$$

belong to $\mathrm{GL}(2n+1, \mathbb{Z})$ and satisfy

$$YS^\dagger Z^\dagger = W^\dagger,$$

where $S^\dagger = \mathrm{diag}(1, 1, 1, \ldots, 1, 1, 2\ell_{2n+1} f_{2n+2})$. In fact, we can take $\lambda = -4$, $\mu = -11$, and, for each odd $n \geq 5$,

$$\alpha = \ell_{2n+1}(x_{2n+1}\ell_{4n-6} + f_{2n-1}f_{2n-7}) + 8(x_{2n+1} + f_{2n-1}), \quad \beta = f_{2n-7},$$

$$\gamma = -\ell_{2n+1}(x_{2n+1}\ell_{2n-4} + f_{2n-1}f_{2n-5}) - 3(x_{2n+1} + f_{2n-1}), \quad \delta = -f_{2n-5}.$$

Proof Putting $\lambda = -4$ and $\mu = -11$, direct computation of AP and CQ establishes that

$$W^\dagger = \begin{pmatrix} AP & C' \\ C & CQ \end{pmatrix}.$$

Putting $\nu = 2\ell_{2n+1} f_{2n+2}$ we have

$$S^\dagger = \begin{pmatrix} I & O \\ O & D \end{pmatrix} \qquad \text{where } D = \begin{pmatrix} 1 & 0 \\ 0 & \nu \end{pmatrix}.$$

Given that M and N are zero matrices, the condition $YS^\dagger Z^\dagger = W^\dagger$ is therefore equivalent to

$$\begin{pmatrix} AP & AQ + BDR_n^\dagger \\ CP & CQ \end{pmatrix} = \begin{pmatrix} AP & C' \\ C & CQ \end{pmatrix}.$$

Thus it remains only to check that $AQ + BDR_n^\dagger = C'$. As in Theorem 1, the only parts that require explanation are the equations given by the second and third rows. Inserting the given values of λ and μ, and applying the identities used in the proof of Theorem 1, these equations are

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} DR_n^\dagger = \begin{pmatrix} -f_{4n-4}-8 & f_{4n-6}+29 \\ f_{4n-2}+3 & -f_{4n-4}-11 \end{pmatrix} = \begin{pmatrix} -\ell_{2n+1}f_{2n-5} & \ell_{2n+1}f_{2n-7}+8 \\ \ell_{2n+1}f_{2n-3} & -\ell_{2n+1}f_{2n-5}-3 \end{pmatrix}.$$

First, consider the case when n is odd. Since $\det R_n^\dagger = 1$ we have

$$(DR_n^\dagger)^{-1} = \begin{pmatrix} -x_{2n+1} & -f_{2n-1}/\nu \\ x_{2n+1}+f_{2n-1} & \ell_{2n+1}/\nu \end{pmatrix}.$$

Thus we have explicit formulae for $\alpha, \beta, \gamma, \delta$. The formulae can be simplified in various ways, but for our purposes it is enough to show that the values are integers, which is obvious for α and γ. For β, we use the identity $f_{k+4}f_{k-4} - f_{k+2}f_{k-2} = 8$ (k odd) with $k = 2n-3$. Thus $f_{2n-5}f_{2n-1} + 8 = f_{2n+1}f_{2n-7}$, and we can argue as follows:

$$\begin{aligned} \beta &= (2f_{2n+2})^{-1}(f_{2n-5}f_{2n-1} + \ell_{2n+1}f_{2n-7} + 8) \\ &= (2f_{2n+2})^{-1}(f_{2n-7}f_{2n+1} + \ell_{2n+1}f_{2n-7}) \\ &= (2f_{2n+2})^{-1}f_{2n-7}(f_{2n+1} + \ell_{2n+1}) \\ &= f_{2n-7}. \end{aligned}$$

A similar calculation shows that $\delta = -f_{2n-5}$. In the case when n is even, the alternative form of $R_n^\dagger$ given the Corollary to Lemma 1 gives a similar result. In both cases it follows that Y and $Z^\dagger$ are in $\mathrm{GL}(2n+1, \mathbb{Z})$, as in Theorem 1. □

Corollary The critical group of the modified wheel with $2n+1$ spokes is a cyclic group of order $2\ell_{2n+1}f_{2n+2}$. □

4. Computation in $\mathcal{K}(W^\dagger)$

In this section we review briefly how the critical group $\mathcal{K}(G)$ meets the computational criteria discussed in the introduction. The most significant point is that there is a canonical representation of the elements of the group, and a simple algorithm for finding the sum of two elements in this representation. These facts follows from the theory [**3**] of a 'chip-firing' process on G, which will now be described briefly.

Let G be a connected graph with a distinguished vertex q. A *configuration* on G is a function $s : V \to \mathbb{Z}$ such that

$$s(v) \geq 0 \ (v \neq q), \qquad s(q) = -\sum_{v \neq q} s(v).$$

This situation can be described by a scenario in which $s(v)$ is a number of dollars held by v. The vertex q is the government, whose debt $-s(q)$ is equal to the total number of dollars in circulation. Dollars can be transferred only by 'firing' a vertex, that is, by sending one dollar along each edge incident with that vertex. The rules are: (i) a vertex $v \neq q$ can only be fired when $s(v)$ is at least equal to the degree of v; (ii) the vertex q can only be fired (and must be fired) when no other vertex can be fired. A configuration in which q must be fired is said to be *stable*, and a stable configuration s is said to be *critical* if there is a legal sequence of firings that starts with s and eventually produces s again. The main theorem of the subject asserts that, given any initial configuration s, there is a unique critical configuration $\gamma(s)$ that can be achieved by any legal sequence of firings.

The function γ induces an bijection between the Picard group $\mathcal{P}(G)$ and the set of critical configurations on G. The latter is therefore a group, with the operation defined by $c_1 * c_2 = \gamma(c_1 + c_2)$, where $+$ is the ordinary addition of integer-valued functions. In other words, to obtain $c_1 * c_2$ we add the configurations and apply any legal sequence of firings until a critical configuration is reached. This algorithm can be regarded as the reduction of a configuration to standard form, using the relations provided by the reduced Laplacian. A theorem of van den Heuvel [**6**] shows that the number of firings needed to find $\gamma(s)$ is $O(n^2(|s| + m))$ for graphs with n vertices, m edges, and fixed edge-connectivity, where $|s| = -s(q)$.

Let us now consider the special case when $G = W^{\dagger}$, taking the distinguished vertex q to be the 'hub' of the wheel. A critical configuration c is represented by the $2n + 2$ non-negative integers $c(v)$, $v \neq q$. Since c must be stable, the possible values of $c(v)$ are $0, 1, 2$, except for the single vertex of degree 2, for which the possible values are $0, 1$. Hence there is an efficient representation of the group elements. There is no immediate rule for recognizing which stable configurations are, in fact, critical. But a standard result asserts that if a stable configuration recurs, then it does so after firing each vertex exactly once.

For the modified wheel with $2n + 1$ spokes, the numbers of vertices, edges, and the maximum value of $|s|$ for a stable configuration are all linear in

n. Hence the theorem of van den Heuvel implies that the calculation of $c_1 * c_2 = \gamma(c_1 + c_2)$ requires $O(n^3)$ firings. Finally, we have an explicit formula for the order of the group $\mathcal{K}(W^\dagger)$.

It is possible that the Discrete Logarithm Problem in $K(W^\dagger)$ is nontrivial. One curious phenomenon arising from the analysis in Section 3 is worth mentioning. Although almost all the entries in the reducing matrices Y and $Z^\dagger$ are well-behaved, there are two, α and γ, that grow far more rapidly than the others. For example, when $n = 7$, we have $\beta = f_7 = 13$ and $\delta = -f_9 = -34$, whereas $\alpha = 7210988$ and $\gamma = -18859507$.

References

1. R. Bacher, P. de la Harpe, T. Nagnibeda, 'The lattice of integral flows and the lattice of integral coboundaries on a finite graph', *Bull. Math. Soc. de France* 125 (1997) 167-198.

2. N.L. Biggs, 'Algebraic potential theory on graphs', *Bull. London Math. Soc.*, 29 (1997) 641-682.

3. N.L. Biggs, 'Chip-firing and the critical group of a graph', *J. Algebraic Combinatorics* 9 (1999) 25-45.

4. S. Chen, S.K. Ye, 'Critical groups for homeomorphism classes of graphs' (to appear).

5. T. ElGamal, 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans. Info. Theory* 31 (1985) 469-472.

6. J. van den Heuvel, 'Algorithmic aspects of a chip-firing game', *Combinatorics, Probability and Computing* 10 (2001) 505-529.

7. R. Honsberger, 'A second look at the Fibonacci and Lucas numbers', *Mathematical Gems III, Dolciani Mathematical Expositions 9*, MAA (1985) 102-138.

8. M. Kotani, T. Sunada, 'Jacobian tori associated with a finite graph and its abelian covering graphs', *Advances in Applied Mathematics* 24 (2000) 89-110.