

# Elliptic Curves and Chip-Firing Games on Graphs

Gregg Musiker (MIT/MSRI)

University of Minnesota Colloquium

December 3, 2009

- 1 Introduction to Algebraic Curves over Finite Fields

- 1 Introduction to Algebraic Curves over Finite Fields
- 2 Elliptic Curves and a Combinatorial Interpretation of  $N_k$ 's

- 1 Introduction to Algebraic Curves over Finite Fields
- 2 Elliptic Curves and a Combinatorial Interpretation of  $N_k$ 's
- 3 Journey into Graph Theory: Spanning Trees

- 1 Introduction to Algebraic Curves over Finite Fields
- 2 Elliptic Curves and a Combinatorial Interpretation of  $N_k$ 's
- 3 Journey into Graph Theory: Spanning Trees
- 4 Chip-Firing Games and Critical Groups

- 1 Introduction to Algebraic Curves over Finite Fields
- 2 Elliptic Curves and a Combinatorial Interpretation of  $N_k$ 's
- 3 Journey into Graph Theory: Spanning Trees
- 4 Chip-Firing Games and Critical Groups
- 5 Connections between Elliptic Curves and Chip-Firing Games

- 1 Introduction to Algebraic Curves over Finite Fields
- 2 Elliptic Curves and a Combinatorial Interpretation of  $N_k$ 's
- 3 Journey into Graph Theory: Spanning Trees
- 4 Chip-Firing Games and Critical Groups
- 5 Connections between Elliptic Curves and Chip-Firing Games
- 6 Elliptic Cyclotomic Polynomials and Other Amusements

- 1 Introduction to Algebraic Curves over Finite Fields
- 2 Elliptic Curves and a Combinatorial Interpretation of  $N_k$ 's
- 3 Journey into Graph Theory: Spanning Trees
- 4 Chip-Firing Games and Critical Groups
- 5 Connections between Elliptic Curves and Chip-Firing Games
- 6 Elliptic Cyclotomic Polynomials and Other Amusements
- 7 Further Horizons: Connections to Tropical Geometry

# Algebraic Curves over Finite Fields

$\mathbb{F}_q$ , a finite field containing  $q$  elements, where  $q$  is a power of a prime.

$\mathbb{F}_{q^k}$  is a field extension;  $\overline{\mathbb{F}_q}$  is an algebraic closure.

Nonsingular Projective Plane Curve (smooth model chosen)

$C : f(x, y) = 0$  plus a single point at infinity.

$$C(\mathbb{F}_q) \subset C(\mathbb{F}_{q^{k_1}}) \subset C(\mathbb{F}_{q^{k_2}}) \subset \cdots \subset C(\overline{\mathbb{F}_q})$$

for any sequence of natural numbers  $1|k_1|k_2|\dots$

# Algebraic Curves over Finite Fields

$\mathbb{F}_q$ , a finite field containing  $q$  elements, where  $q$  is a power of a prime.

$\mathbb{F}_{q^k}$  is a field extension;  $\overline{\mathbb{F}_q}$  is an algebraic closure.

Nonsingular Projective Plane Curve (smooth model chosen)

$C : f(x, y) = 0$  plus a single point at infinity.

$$C(\mathbb{F}_q) \subset C(\mathbb{F}_{q^{k_1}}) \subset C(\mathbb{F}_{q^{k_2}}) \subset \cdots \subset C(\overline{\mathbb{F}_q})$$

for any sequence of natural numbers  $1|k_1|k_2|\dots$

The **Frobenius** map  $\pi$  acts on curve  $C$  over finite field  $\mathbb{F}_q$  via

$$\pi(a, b) = (a^q, b^q) \quad \text{and} \quad \pi(P_\infty) = P_\infty.$$

The **Frobenius** map  $\pi$  acts on curve  $C$  over finite field  $\mathbb{F}_q$  via

$$\pi(a, b) = (a^q, b^q) \quad \text{and} \quad \pi(P_\infty) = P_\infty.$$

### Fact

For point  $P \in C(\overline{\mathbb{F}_q})$ ,

$$\pi(P) \in C(\overline{\mathbb{F}_q}).$$

### Fact

For point  $P \in C(\mathbb{F}_{q^k})$ ,

$$\pi^k(P) = P.$$

Let  $N_k$  be the number of points on curve  $C$ , over finite field  $\mathbb{F}_{q^k}$ .

Alternatively,  $N_k$  counts the number of points in  $C(\overline{\mathbb{F}_q})$  which are fixed by the  $k$ th power of the Frobenius map,  $\pi^k$ .

$N_k = |C(\mathbb{F}_{q^k})|$  counts the number of points in  $C(\overline{\mathbb{F}_q})$  which are fixed by the  $k$ th power of the Frobenius map,  $\pi^k$ .

Using this sequence, we define the **zeta function of an algebraic variety**, which can be written several different ways, including as an exponential generating function.

$$\begin{aligned} Z(C, T) &= \exp\left(\sum_{k=1}^{\infty} N_k \frac{T^k}{k}\right) = 1 + \sum_{k \geq 1} H_k T^k \\ &= \prod_{\mathfrak{p}} \frac{1}{1 - T^{\deg \mathfrak{p}}} \quad \text{where } \mathfrak{p} \text{ is a prime ideal} \\ \zeta(s) &= \prod_{p \text{ prime integer}} \frac{1}{1 - p^{-s}} = \sum_{n \geq 1} \frac{1}{n^s} \end{aligned}$$

## Theorem (Rationality - Weil 1948)

$$Z(C, T) = \frac{(1 - \alpha_1 T)(1 - \alpha_2 T) \cdots (1 - \alpha_{2g-1} T)(1 - \alpha_{2g} T)}{(1 - T)(1 - qT)}$$

for complex numbers  $\alpha_i$ 's, where  $g$  is the genus of the curve  $C$ .  
Furthermore, the numerator of  $Z(C, T)$  has integer coefficients.

## Theorem (Rationality - Weil 1948)

$$Z(C, T) = \frac{(1 - \alpha_1 T)(1 - \alpha_2 T) \cdots (1 - \alpha_{2g-1} T)(1 - \alpha_{2g} T)}{(1 - T)(1 - qT)}$$

for complex numbers  $\alpha_i$ 's, where  $g$  is the genus of the curve  $C$ .  
Furthermore, the numerator of  $Z(C, T)$  has integer coefficients.

## Theorem (Functional Equation - Weil 1948)

$$Z(C, T) = q^{g-1} T^{2g-2} Z(C, 1/qT)$$

$$\begin{aligned} N_k &= p_k [1 + q - \alpha_1 - \cdots - \alpha_{2g}] \\ &= 1 + q^k - \alpha_1^k - \cdots - \alpha_{2g}^k \end{aligned}$$

The Zeta Function of curve  $C$  of genus  $g$ , hence the entire sequence of  $\{N_k\}$ 's, only depends on  $\{q, N_1, N_2, \dots, N_g\}$ .

# Elliptic Curves, and a Combinatorial Interpretation of $N_k$

Specializing to the case of an elliptic curve  $E$ , or a genus one curve, a lot more is known and there is additional structure.

## Facts

- 1  $E$  can be represented as the zero locus in  $\mathbb{P}^2$  of the equation

$$y^2 = x^3 + Ax + B$$

for  $A, B \in \mathbb{F}_q$ . (if  $p \neq 2, 3$ )

# Elliptic Curves, and a Combinatorial Interpretation of $N_k$

Specializing to the case of an elliptic curve  $E$ , or a genus one curve, a lot more is known and there is additional structure.

## Facts

- 1  $E$  can be represented as the zero locus in  $\mathbb{P}^2$  of the equation

$$y^2 = x^3 + Ax + B$$

for  $A, B \in \mathbb{F}_q$ . (if  $p \neq 2, 3$ )

- 2  $E$  has a group structure where two points on  $E$  can be added to yield another point on the curve.

# Elliptic Curves, and a Combinatorial Interpretation of $N_k$

Specializing to the case of an elliptic curve  $E$ , or a genus one curve, a lot more is known and there is additional structure.

## Facts

- ①  $E$  can be represented as the zero locus in  $\mathbb{P}^2$  of the equation

$$y^2 = x^3 + Ax + B$$

for  $A, B \in \mathbb{F}_q$ . (if  $p \neq 2, 3$ )

- ②  $E$  has a group structure where two points on  $E$  can be added to yield another point on the curve.
- ③ The Frobenius map is compatible with the group structure:

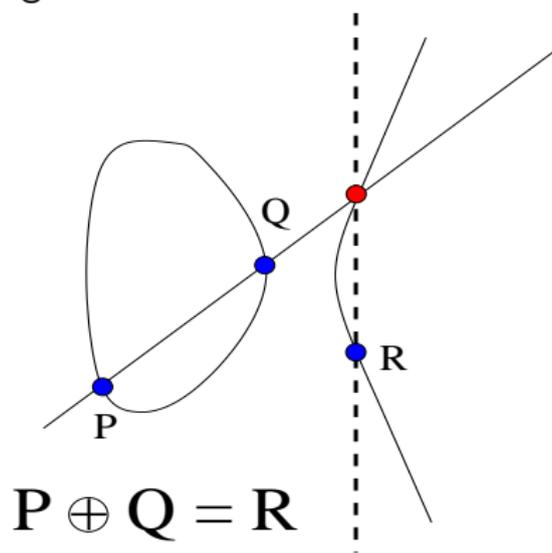
$$\pi(P \oplus Q) = \pi(P) \oplus \pi(Q).$$

Recall that  $\pi(x, y) = (x^q, y^q)$  and

$$\pi^k(P) = P \text{ if and only if } P \in E(\mathbb{F}_{q^k}).$$

# Elliptic Curve Group Law Geometrically

Draw Chord/Tangent Line and then reflect about horizontal axis



# Elliptic Curve Group Law Algebraically

If  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$ , then

$$P_1 \oplus P_2 = P_3 = (x_3, y_3) \text{ where}$$

1) If  $x_1 \neq x_2$  then

$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = m(x_1 - x_3) - y_1 \text{ with } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2) If  $x_1 = x_2$  but ( $y_1 \neq y_2$ , or  $y_1 = 0 = y_2$ ) then  $P_3 = P_\infty$ .

3) If  $P_1 = P_2$  and  $y_1 \neq 0$ , then

$$x_3 = m^2 - 2x_1 \text{ and } y_3 = m(x_1 - x_3) - y_1 \text{ with } m = \frac{3x_1^2 + A}{2y_1}.$$

4)  $P_\infty$  acts as the identity element in this addition.

## Rationality (Hasse 1933)

$$Z(E, T) = \frac{(1 - \alpha_1 T)(1 - \alpha_2 T)}{(1 - T)(1 - qT)} = \frac{1 - (1 + q - N_1)T + qT^2}{(1 - T)(1 - qT)}$$

for complex numbers  $\alpha_1$  and  $\alpha_2$ . (In fact  $|\alpha_1| = |\alpha_2| = \sqrt{q}$ .)

## Functional Equation

$$Z(E, 1/qT) = Z(E, T).$$

$$\begin{aligned} N_k &= p_k[1 + q - \alpha_1 - \alpha_2] \\ &= 1 + q^k - \alpha_1^k - \alpha_2^k \end{aligned}$$

and the Functional Equation implies

$$\alpha_1 \alpha_2 = q.$$

Thus the entire sequence of  $N_k$ 's, for elliptic curve  $E$ , only depends on  $q$  and  $N_1$ .

## Theorem (Garsia 2004)

For an elliptic curve, we can write  $N_k$  as a polynomial in terms of  $N_1$  and  $q$  such that

$$N_k = \sum_{i=1}^k (-1)^{i-1} P_{k,i}(q) N_1^i$$

where each  $P_{k,i}$  is a polynomial in  $q$  with positive integer coefficients.

## Theorem (Garsia 2004)

For an elliptic curve, we can write  $N_k$  as a polynomial in terms of  $N_1$  and  $q$  such that

$$N_k = \sum_{i=1}^k (-1)^{i-1} P_{k,i}(q) N_1^i$$

where each  $P_{k,i}$  is a polynomial in  $q$  with positive integer coefficients.

$$N_2 = (2 + 2q)N_1 - N_1^2$$

$$N_3 = (3 + 3q + 3q^2)N_1 - (3 + 3q)N_1^2 + N_1^3$$

$$N_4 = (4 + 4q + 4q^2 + 4q^3)N_1 - (6 + 8q + 6q^2)N_1^2 + (4 + 4q)N_1^3 - N_1^4$$

$$N_5 = (5 + 5q + 5q^2 + 5q^3 + 5q^4)N_1 - (10 + 15q + 15q^2 + 10q^3)N_1^2 \\ + (10 + 15q + 10q^2)N_1^3 - (5 + 5q)N_1^4 + N_1^5$$

## Question

What is a combinatorial interpretation of these expressions, i.e. of the  $P_{k,i}$ 's?

And now for something completely different ...

## Graph Theory Terminology:

Let  $G = (V, E)$  be a finite graph. (We allow multiple edges between vertices, but not loops.)

A **spanning tree** (of an undirected graph) is a connected subgraph without cycles that is incident to all vertices.

## Graph Theory Terminology:

Let  $G = (V, E)$  be a finite graph. (We allow multiple edges between vertices, but not loops.)

A **spanning tree** (of an undirected graph) is a connected subgraph without cycles that is incident to all vertices.

We now consider **directed graphs**, edges are oriented.

## Graph Theory Terminology:

Let  $G = (V, E)$  be a finite graph. (We allow multiple edges between vertices, but not loops.)

A **spanning tree** (of an undirected graph) is a connected subgraph without cycles that is incident to all vertices.

We now consider **directed graphs**, edges are oriented.

Single out one of the vertices,  $v_0$ . We call this the **root** of  $G$ .

## Graph Theory Terminology:

Let  $G = (V, E)$  be a finite graph. (We allow multiple edges between vertices, but not loops.)

A **spanning tree** (of an undirected graph) is a connected subgraph without cycles that is incident to all vertices.

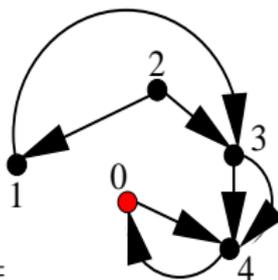
We now consider **directed graphs**, edges are oriented.

Single out one of the vertices,  $v_0$ . We call this the **root** of  $G$ .

A **rooted oriented spanning tree** of  $G$  is a spanning tree of the underlying undirected graph, and orientations of edges along the tree are chosen so that all edges point towards the root.

# More Graph Theory Terminology: The Laplacian Matrix

The **Laplacian** matrix of a graph has diagonal entries  $d_i$  (outdegree of  $v_i$ ) and off-diagonal entries  $-d_{ij}$  (number of directed edges from  $v_i$  to  $v_j$ ).



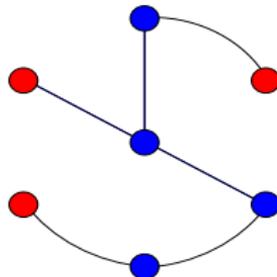
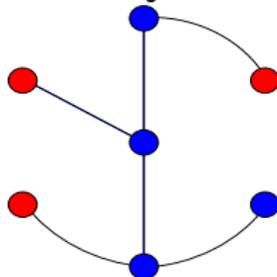
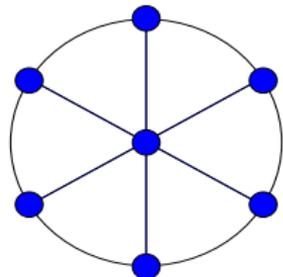
Example: let  $G =$

with the root vertex  $v_0$  in red. Then

$$L(G) = \begin{bmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 2 & -2 \\ -1 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (\text{Rows/Columns indexed as } 0, 1, 2, 3, 4)$$

# A Family of Examples

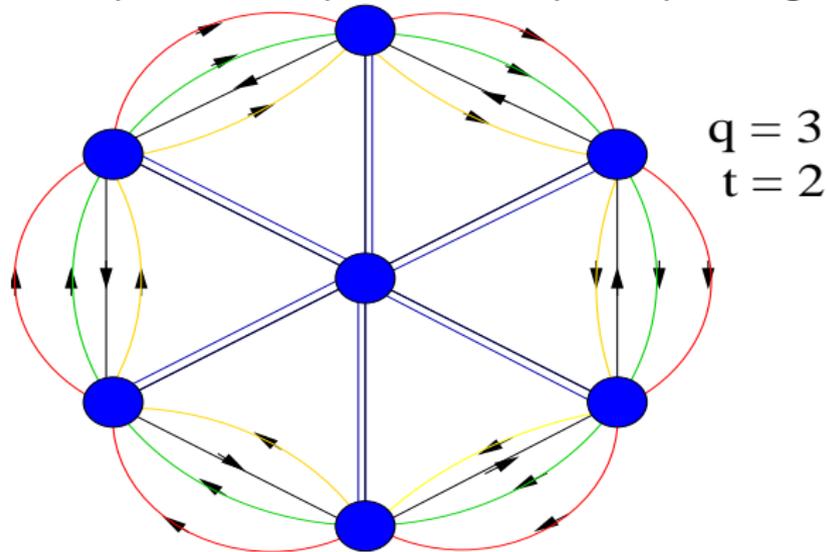
We let  $W_k$  denote the wheel graph which consists of  $k$  vertices on a circle and a central vertex which is adjacent to every other vertex.



Note that a spanning tree will consist of arcs on the rim and spokes. We construct a family of digraphs (directed with multiple edges allowed) whose vertex set equal the  $W_k$ 's.

We replace each rim edge with  $q$  clockwise edges and 1 counter-clockwise edge.

We replace each spoke with  $t$  spokes pointing towards the root.



The  $(q, t)$ -wheel graphs  $W_k(q, t)$  for  $k \geq 1$ .

## Definition

$\mathcal{W}_k(q, t) =$

The number of rooted oriented spanning trees in graph  $\mathcal{W}_k(q, t)$ .

## Theorem (M- 2007)

$\mathcal{W}_k(q, t)$  can be written as a positive bivariate integer polynomial such that the coefficient of  $t^i$  in  $\mathcal{W}_k(q, t)$  equals  $P_{k,i}(q)$  in

$$N_k = \sum_{i=1}^k (-1)^{i-1} P_{k,i}(q) N_1^i.$$

In other words,  $\mathcal{W}_k(q, -N_1) = N_k$ .

# The $\mathcal{W}_k(q, t)$ 's are integer polynomials

$$\mathcal{W}_k(q, t) =$$

The number of rooted oriented spanning trees in graph  $\mathcal{W}_k(q, t)$ .

The Laplacian Matrix for  $\mathcal{W}_k(q, t)$  is

$$L_k = \begin{bmatrix} 1+q+t & -q & 0 & \dots & 0 & -1 & -t \\ -1 & 1+q+t & -q & 0 & \dots & 0 & -t \\ \dots & \dots & \dots & \dots & \dots & \dots & -t \\ 0 & \dots & -1 & 1+q+t & -q & 0 & -t \\ 0 & \dots & 0 & -1 & 1+q+t & -q & -t \\ -q & 0 & \dots & 0 & -1 & 1+q+t & -t \\ -t & -t & -t & \dots & -t & -t & kt \end{bmatrix}.$$

The last row and column correspond to hub vertex, the root.

# Proof of Integrality by the Matrix-Tree Theorem

By the Matrix-Tree theorem, the number of directed rooted spanning trees is  $\det(L_k)_0$  where  $(L_k)_0$  is matrix  $L_k$  with the last row and last column deleted.

# Proof of Integrality by the Matrix-Tree Theorem

By the Matrix-Tree theorem, the number of directed rooted spanning trees is  $\det(L_k)_0$  where  $(L_k)_0$  is matrix  $L_k$  with the last row and last column deleted.

Let  $\overline{M}_1 = [t]$ ,  $\overline{M}_2 = \begin{bmatrix} 1+q+t & -1-q \\ -1-q & 1+q+t \end{bmatrix}$ , and for  $k \geq 3$ , let  $\overline{M}_k$  be the  $k$ -by- $k$  “three-line” circulant matrix

$$\begin{bmatrix} 1+q+t & -q & 0 & \dots & 0 & -1 \\ -1 & 1+q+t & -q & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & -1 & 1+q+t & -q & 0 \\ 0 & \dots & 0 & -1 & 1+q+t & -q \\ -q & 0 & \dots & 0 & -1 & 1+q+t \end{bmatrix}.$$

Theorem (M- 2007)

$$\mathcal{W}_k(q, t) = \det \overline{M}_k \text{ and } N_k(q, t) = -\det \overline{M}_k|_{t=-N_1}$$

# The $\mathcal{W}_k$ 's also are the cardinalities of a sequence of groups

Consider the **quotient group**

$$K(G, v_0) \cong \mathbb{Z}^{|V(G)|-1} / \text{Im } (L_k)_0$$

where  $(L_k)_0$  is the Laplacian matrix of graph  $G$  with the row and column corresponding to  $v_0$  deleted.

$$|K(G, v_0)| = \# \text{Spanning Trees in Graph } G$$

# The $\mathcal{W}_k$ 's also are the cardinalities of a sequence of groups

Consider the **quotient group**

$$K(G, v_0) \cong \mathbb{Z}^{|V(G)|-1} / \text{Im } (L_k)_0$$

where  $(L_k)_0$  is the Laplacian matrix of graph  $G$  with the row and column corresponding to  $v_0$  deleted.

$$|K(G, v_0)| = \#\text{Spanning Trees in Graph } G$$

This group goes by many names, **critical group of graph  $G$**  (w.r.t.  $v_0$ ) from Biggs.

# The $\mathcal{W}_k$ 's also are the cardinalities of a sequence of groups

Consider the **quotient group**

$$K(G, v_0) \cong \mathbb{Z}^{|V(G)|-1} / \text{Im } (L_k)_0$$

where  $(L_k)_0$  is the Laplacian matrix of graph  $G$  with the row and column corresponding to  $v_0$  deleted.

$$|K(G, v_0)| = \#\text{Spanning Trees in Graph } G$$

This group goes by many names, **critical group of graph  $G$**  (w.r.t.  $v_0$ ) from Biggs. Also known as the **Jacobian** of a graph, studied by Baker-Norine,

# The $\mathcal{W}_k$ 's also are the cardinalities of a sequence of groups

Consider the **quotient group**

$$K(G, v_0) \cong \mathbb{Z}^{|V(G)|-1} / \text{Im } (L_k)_0$$

where  $(L_k)_0$  is the Laplacian matrix of graph  $G$  with the row and column corresponding to  $v_0$  deleted.

$$|K(G, v_0)| = \#\text{Spanning Trees in Graph } G$$

This group goes by many names, **critical group of graph  $G$**  (w.r.t.  $v_0$ ) from Biggs. Also known as the **Jacobian** of a graph, studied by Baker-Norine, **Group of components** by Lorenzini,

# The $\mathcal{W}_k$ 's also are the cardinalities of a sequence of groups

Consider the **quotient group**

$$K(G, v_0) \cong \mathbb{Z}^{|V(G)|-1} / \text{Im } (L_k)_0$$

where  $(L_k)_0$  is the Laplacian matrix of graph  $G$  with the row and column corresponding to  $v_0$  deleted.

$$|K(G, v_0)| = \#\text{Spanning Trees in Graph } G$$

This group goes by many names, **critical group of graph**  $G$  (w.r.t.  $v_0$ ) from Biggs. Also known as the **Jacobian** of a graph, studied by Baker-Norine, **Group of components** by Lorenzini, and **Sandpile group** by Dhar, Gabrielov, among others.

# The $\mathcal{W}_k$ 's also are the cardinalities of a sequence of groups

Consider the **quotient group**

$$K(G, v_0) \cong \mathbb{Z}^{|V(G)|-1} / \text{Im } (L_k)_0$$

where  $(L_k)_0$  is the Laplacian matrix of graph  $G$  with the row and column corresponding to  $v_0$  deleted.

$$|K(G, v_0)| = \#\text{Spanning Trees in Graph } G$$

This group goes by many names, **critical group of graph**  $G$  (w.r.t.  $v_0$ ) from Biggs. Also known as the **Jacobian** of a graph, studied by Baker-Norine, **Group of components** by Lorenzini, and **Sandpile group** by Dhar, Gabrielov, among others.

Alternative definition with **explicit coset representatives** shortly.

# Critical Group of The Complete Graph $K_n$

The complete graph  $K_n$  has  $n$  vertices and  $\binom{n}{2}$  edges, one between each pair of vertices.

# Critical Group of The Complete Graph $K_n$

The complete graph  $K_n$  has  $n$  vertices and  $\binom{n}{2}$  edges, one between each pair of vertices. The number of spanning trees of  $K_n$  is  $n^{n-2}$ .

# Critical Group of The Complete Graph $K_n$

The complete graph  $K_n$  has  $n$  vertices and  $\binom{n}{2}$  edges, one between each pair of vertices. The number of spanning trees of  $K_n$  is  $n^{n-2}$ .

**Theorem (Lorenzini 1991)**

*The critical group  $K(K_n)$  decomposes as  $(\mathbb{Z}/n\mathbb{Z})^{n-2}$ .*

# Critical Group of The Complete Graph $K_n$

The complete graph  $K_n$  has  $n$  vertices and  $\binom{n}{2}$  edges, one between each pair of vertices. The number of spanning trees of  $K_n$  is  $n^{n-2}$ .

## Theorem (Lorenzini 1991)

*The critical group  $K(K_n)$  decomposes as  $(\mathbb{Z}/n\mathbb{Z})^{n-2}$ .*

For a given family of graphs (e.g.  $W_k$ ,  $C_n$ ,  $P_n$ , products (such as hypercube  $Q_n$ )), can be nontrivial to find  $K(G)$ .

# Critical Group of The Complete Graph $K_n$

The complete graph  $K_n$  has  $n$  vertices and  $\binom{n}{2}$  edges, one between each pair of vertices. The number of spanning trees of  $K_n$  is  $n^{n-2}$ .

## Theorem (Lorenzini 1991)

*The critical group  $K(K_n)$  decomposes as  $(\mathbb{Z}/n\mathbb{Z})^{n-2}$ .*

For a given family of graphs (e.g.  $W_k$ ,  $C_n$ ,  $P_n$ , products (such as hypercube  $Q_n$ )), can be nontrivial to find  $K(G)$ .

For example, decomposition of  $K(W_k)$  involves Fibonacci numbers (Biggs).

# Chip-Firing: (Björner, Lovász, Shor 1991)

- 1 Assign a nonnegative integer value  $C_i$  to each vertex  $v_i$  (number of chips).
- 2 Start with vertex  $v_1$ .
- 3 If  $C_i$ , the number of chips on  $v_i$ , is greater than or equal to the outdegree of  $v_i$ , then vertex  $v_i$  **fires**. Otherwise move on to  $v_{i+1}$ .
- 4 If vertex  $v_i$  fires, then we take  $d_i$  chips off of  $v_i$  and distribute them to  $v_i$ 's neighbors.
- 5 Now  $C_i := C_i - d_i$  and  $C_j := C_j + d_{ij}$  if  $v_j$  is a neighbor of  $v_i$ .
- 6 We continue until we get to  $v_n$ .

# Chip-Firing: (Björner, Lovász, Shor 1991)

- 1 Assign a nonnegative integer value  $C_i$  to each vertex  $v_i$  (number of chips).
- 2 Start with vertex  $v_1$ .
- 3 If  $C_i$ , the number of chips on  $v_i$ , is greater than or equal to the outdegree of  $v_i$ , then vertex  $v_i$  **fires**. Otherwise move on to  $v_{i+1}$ .
- 4 If vertex  $v_i$  fires, then we take  $d_i$  chips off of  $v_i$  and distribute them to  $v_i$ 's neighbors.
- 5 Now  $C_i := C_i - d_i$  and  $C_j := C_j + d_{ij}$  if  $v_j$  is a neighbor of  $v_i$ .
- 6 We continue until we get to  $v_n$ .
- 7 We then start over with  $v_1$  and repeat.
- 8 We continue forever or terminate when all  $C_i < d_i$ .

We consider a variant due to Norman Biggs known as the **Dollar Game**:

We consider a variant due to Norman Biggs known as the **Dollar Game**:

- 1 We designate one vertex  $v_0$  to be the bank, and allow  $C_0$  to be negative. All the other  $C_i$ 's still must be nonnegative.

We consider a variant due to Norman Biggs known as the **Dollar Game**:

- 1 We designate one vertex  $v_0$  to be the bank, and allow  $C_0$  to be negative. All the other  $C_i$ 's still must be nonnegative.
- 2 To limit extraneous configurations, we presume that the sum  $\sum_{i=0}^{\#V-1} C_i = 0$ . (Thus in particular,  $C_0$  will be non-positive.)

We consider a variant due to Norman Biggs known as the **Dollar Game**:

- 1 We designate one vertex  $v_0$  to be the bank, and allow  $C_0$  to be negative. All the other  $C_i$ 's still must be nonnegative.
- 2 To limit extraneous configurations, we presume that the sum  $\sum_{i=0}^{\#V-1} C_i = 0$ . (Thus in particular,  $C_0$  will be non-positive.)
- 3 The bank, i.e. vertex  $v_0$ , is only allowed to fire if no other vertex can fire. Note that since we now allow  $C_0$  to be negative,  $v_0$  is allowed to fire even when it is smaller than its outdegree.

A configuration is **stable** if  $v_0$  is the only vertex that can fire

A configuration  $C$  is **recurrent** if there is firing sequence which will lead back to  $C$ .

(Note that this will necessarily require the use of  $v_0$  firing.)

We call a configuration **critical** if it is both stable and recurrent.

A configuration is **stable** if  $v_0$  is the only vertex that can fire

A configuration  $C$  is **recurrent** if there is firing sequence which will lead back to  $C$ .

(Note that this will necessarily require the use of  $v_0$  firing.)

We call a configuration **critical** if it is both stable and recurrent.

### Theorem (Gabrielov 1993)

*For any initial configuration  $C$  with  $\sum_{i=0}^k C_i = 0$  and  $C_i \geq 0$  for all  $1 \leq i \leq k$ , there exists a **unique** critical configuration that can be reached by an allowable firing sequence.*

# Coset Representatives for Critical Group

We can define  $K(G, v_0)$  to be the set of *critical configurations*, with addition given by  $C_1 \oplus C_2 = \overline{C_1 + C_2}$ .

Here  $+$  signifies the usual pointwise vector addition and  $\overline{C}$  represents the unique critical configuration in the same coset as  $C$ , modulo the Laplacian.

When  $v_0$  is understood, we will abbreviate this group as the critical group of graph  $G$ , and denote it as  $K(G)$ .

# Coset Representatives for Critical Group

We can define  $K(G, v_0)$  to be the set of *critical configurations*, with addition given by  $C_1 \oplus C_2 = \overline{C_1 + C_2}$ .

Here  $+$  signifies the usual pointwise vector addition and  $\overline{C}$  represents the unique critical configuration in the same coset as  $C$ , modulo the Laplacian.

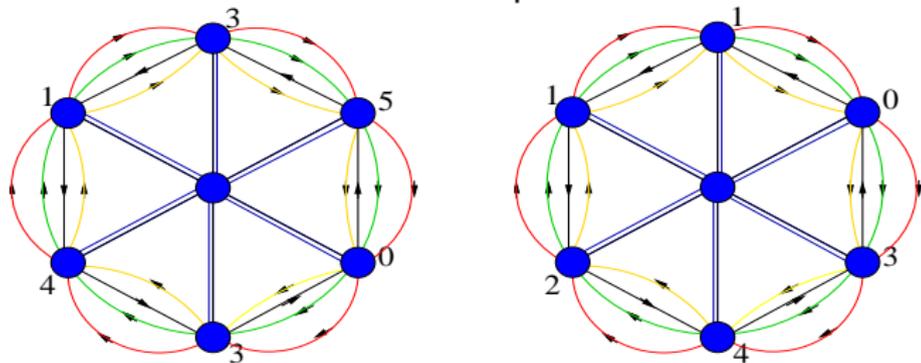
When  $v_0$  is understood, we will abbreviate this group as the critical group of graph  $G$ , and denote it as  $K(G)$ .

## Corollary (Gabrielov 1993)

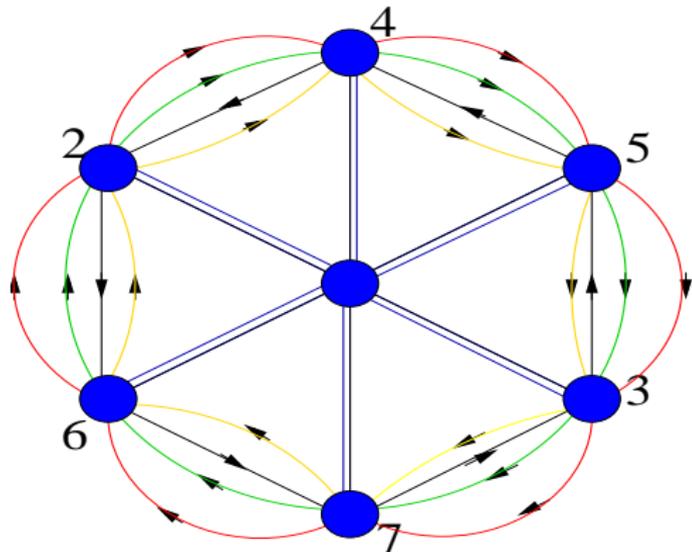
$K(G)$  is an abelian (associative) group.

For example, consider the following two wheels with chip distributions as given. These are both critical configurations.

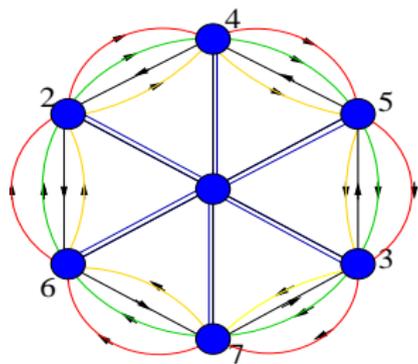
We do not label the number of chips on the hub vertex since forced.

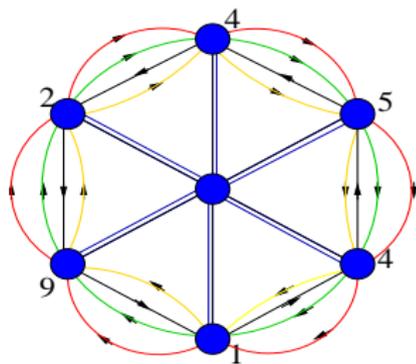
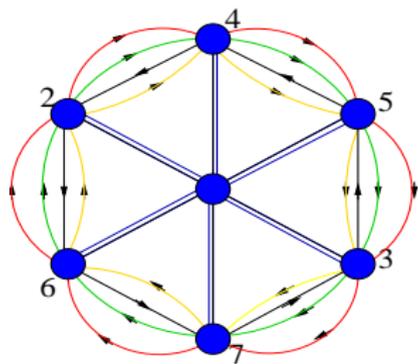


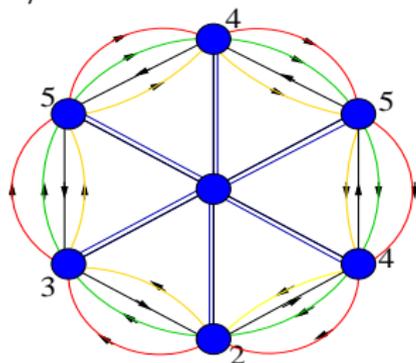
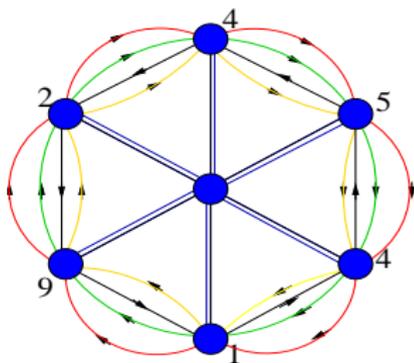
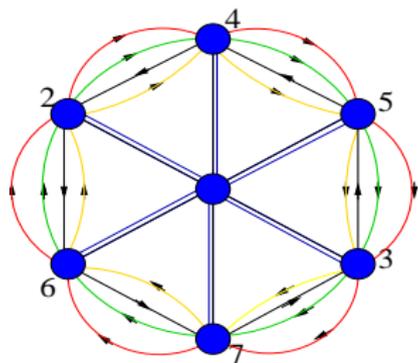
If we add these together pointwise we obtain



This is not a critical configuration, but by the theorem, reduces to a unique critical configuration.







This last one is critical.

# Critical Groups of $(q, t)$ -Wheel Graphs

We want to analogize theory of elliptic curves: For example, there is a tower of groups

$$E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^{k_1}}) \subset E(\mathbb{F}_{q^{k_2}}) \subset \cdots \subset E(\overline{\mathbb{F}_q})$$

# Critical Groups of $(q, t)$ -Wheel Graphs

We want to analogize theory of elliptic curves: For example, there is a tower of groups

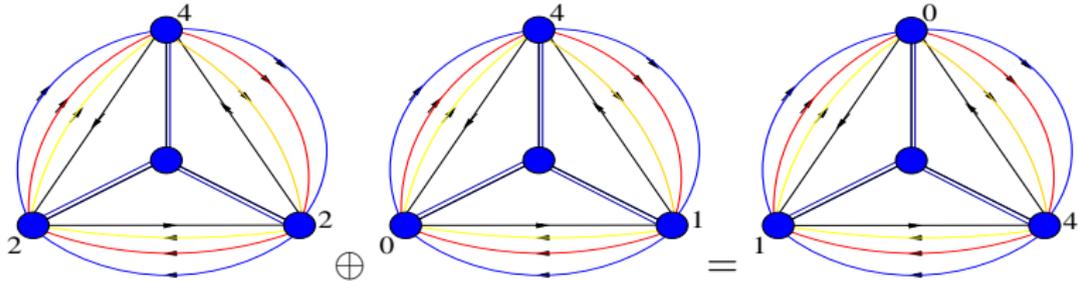
$$E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^{k_1}}) \subset E(\mathbb{F}_{q^{k_2}}) \subset \cdots \subset E(\overline{\mathbb{F}_q})$$

Understanding the sequence of Critical Groups:

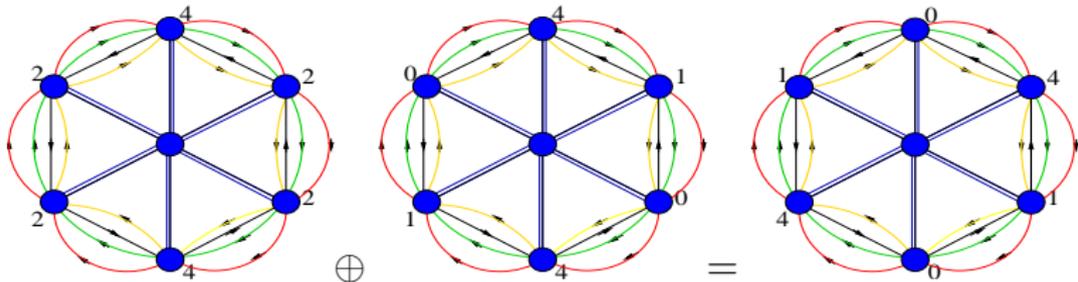
$$K(W_1(q, t)), K(W_2(q, t)), K(W_3(q, t)), \dots$$

The set  $\left\{ \text{Elements of the critical group } K(W_k(q, t)) \right\}$  is a subset of the set of length  $k$  words in alphabet  $\{0, 1, 2, \dots, q + t\}$ .

Example:  $[2, 4, 2] \oplus [0, 4, 1] \equiv [1, 0, 4]$  in  $W_3(q = 3, t = 2)$  versus



$[2, 4, 2, 2, 4, 2] \oplus [0, 4, 1, 0, 4, 1] \equiv [1, 0, 4, 1, 0, 4]$  in  $W_6(q = 3, t = 2)$



Chip-firing is a local process.

## Proposition

*The map  $\psi : w \rightarrow www \dots w$  is an injective group homomorphism between  $K(W_{k_1}(q, t))$  and  $K(W_{k_2}(q, t))$  whenever  $k_1 | k_2$ . Here map  $\psi$  replaces  $w$  with  $k_2/k_1$  copies of  $w$ .*

## Proposition

*The map  $\psi : w \rightarrow www \dots w$  is an injective group homomorphism between  $K(W_{k_1}(q, t))$  and  $K(W_{k_2}(q, t))$  whenever  $k_1 | k_2$ . Here map  $\psi$  replaces  $w$  with  $k_2/k_1$  copies of  $w$ .*

Define  $\rho$  to be the counter-clockwise rotation map on  $K(W_k(q, t))$ .

$$\rho([C_1, C_2, \dots, C_k]) = [C_2, C_3, \dots, C_k, C_1].$$

## Proposition

*The map  $\psi : w \rightarrow www \dots w$  is an injective group homomorphism between  $K(W_{k_1}(q, t))$  and  $K(W_{k_2}(q, t))$  whenever  $k_1 | k_2$ . Here map  $\psi$  replaces  $w$  with  $k_2/k_1$  copies of  $w$ .*

Define  $\rho$  to be the counter-clockwise rotation map on  $K(W_k(q, t))$ .

$$\rho([C_1, C_2, \dots, C_k]) = [C_2, C_3, \dots, C_k, C_1].$$

## Proposition

*The kernel of  $(1 - \rho^{k_1})$  acting on  $K(W_{k_2}(q, t))$  is isomorphic to the subgroup  $K(W_{k_1}(q, t))$  whenever  $k_1 | k_2$ .*

## Proposition

*The kernel of  $(1 - \rho^{k_1})$  acting on  $K(W_{k_2}(q, t))$  is isomorphic to the subgroup  $K(W_{k_1}(q, t))$  whenever  $k_1 | k_2$ .*

We therefore can define a direct limit

$$K(\overline{W}(q, t)) \cong \bigcup_{k=1}^{\infty} K(W_k(q, t))$$

where  $\rho$  provides the transition maps.

## Proposition

*The kernel of  $(1 - \rho^{k_1})$  acting on  $K(W_{k_2}(q, t))$  is isomorphic to the subgroup  $K(W_{k_1}(q, t))$  whenever  $k_1 | k_2$ .*

We therefore can define a direct limit

$$K(\overline{W}(q, t)) \cong \bigcup_{k=1}^{\infty} K(W_k(q, t))$$

where  $\rho$  provides the transition maps.

In particular we obtain

$$K(W_k(q, t)) \cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)).$$

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q}). \end{aligned}$$

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q}). \end{aligned}$$

2 There is a characteristic equation  $\pi^2 - (1 + q - N_1)\pi + q = 0$  on  $E(\overline{\mathbb{F}_q})$ , an elliptic curve over the algebraic closure.

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q). \end{aligned}$$

2 There is a characteristic equation  $\pi^2 - (1 + q - N_1)\pi + q = 0$  on  $E(\overline{\mathbb{F}}_q)$ , an elliptic curve over the algebraic closure.

We get an analogous equation  $\rho^2 - (1 + q + t)\rho + q = 0$  on  $K(\overline{W}(q, t))$ .

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q). \end{aligned}$$

2 There is a characteristic equation  $\pi^2 - (1 + q - N_1)\pi + q = 0$  on  $E(\overline{\mathbb{F}}_q)$ , an elliptic curve over the algebraic closure.

We get an analogous equation  $\rho^2 - (1 + q + t)\rho + q = 0$  on  $K(\overline{W}(q, t))$ . (Linear Algebraic Techniques suffice)

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q). \end{aligned}$$

2 There is a characteristic equation  $\pi^2 - (1 + q - N_1)\pi + q = 0$  on  $E(\overline{\mathbb{F}}_q)$ , an elliptic curve over the algebraic closure.

We get an analogous equation  $\rho^2 - (1 + q + t)\rho + q = 0$  on  $K(\overline{W}(q, t))$ . (Linear Algebraic Techniques suffice)

3 Both the collection of  $E(\mathbb{F}_{q^k})$ 's and  $K(W_k(q, t))$ 's are abelian groups which decompose into at most two cyclic subgroups.

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q}). \end{aligned}$$

2 There is a characteristic equation  $\pi^2 - (1 + q - N_1)\pi + q = 0$  on  $E(\overline{\mathbb{F}_q})$ , an elliptic curve over the algebraic closure.

We get an analogous equation  $\rho^2 - (1 + q + t)\rho + q = 0$  on  $K(\overline{W}(q, t))$ . (Linear Algebraic Techniques suffice)

3 Both the collection of  $E(\mathbb{F}_{q^k})$ 's and  $K(W_k(q, t))$ 's are abelian groups which decompose into at most two cyclic subgroups. (Proof via the Smith normal form of Laplacian matrix.)

Shift map  $\rho$  is the wheel graph-analogue of the Frobenius map  $\pi$  on elliptic curves.

1

$$\begin{aligned} K(W_k(q, t)) &\cong \text{Ker}(1 - \rho^k) : K(\overline{W}(q, t)) \rightarrow K(\overline{W}(q, t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= \text{Ker}(1 - \pi^k) : E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q). \end{aligned}$$

2 There is a characteristic equation  $\pi^2 - (1 + q - N_1)\pi + q = 0$  on  $E(\overline{\mathbb{F}}_q)$ , an elliptic curve over the algebraic closure.

We get an analogous equation  $\rho^2 - (1 + q + t)\rho + q = 0$  on  $K(\overline{W}(q, t))$ . (Linear Algebraic Techniques suffice)

3 Both the collection of  $E(\mathbb{F}_{q^k})$ 's and  $K(W_k(q, t))$ 's are abelian groups which decompose into at most two cyclic subgroups. (Proof via the Smith normal form of Laplacian matrix.)

4 One last surprising connection ...

# Behavior of Torsion Subgroups of $K(\overline{W}(q, t))$

- 4 The Group  $K(\overline{W}(q, t))$  (the direct limit of the  $K(W_k(q, t))$ 's) contains the subgroup  $\mathbb{Z}/n\mathbb{Z}$  for all  $n \geq 1$ , and  $K(\overline{W}(q, t))$  contains the subgroup  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  if and only if  $n$  and  $q$  are coprime.

# Behavior of Torsion Subgroups of $K(\overline{W}(q, t))$

4 The Group  $K(\overline{W}(q, t))$  (the direct limit of the  $K(W_k(q, t))$ 's) contains the subgroup  $\mathbb{Z}/n\mathbb{Z}$  for all  $n \geq 1$ , and

$K(\overline{W}(q, t))$  contains the subgroup  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  if and only if  $n$  and  $q$  are coprime.

(Analogous to  $E(\overline{\mathbb{F}}_q)$  when  $E$  is an ordinary elliptic curve.)

# Behavior of Torsion Subgroups of $K(\overline{W}(q, t))$

4 The Group  $K(\overline{W}(q, t))$  (the direct limit of the  $K(W_k(q, t))$ 's) contains the subgroup  $\mathbb{Z}/n\mathbb{Z}$  for all  $n \geq 1$ , and

$K(\overline{W}(q, t))$  contains the subgroup  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  if and only if  $n$  and  $q$  are coprime.

(Analogous to  $E(\overline{\mathbb{F}}_q)$  when  $E$  is an ordinary elliptic curve.)

What does the proof use? ....

# Behavior of Torsion Subgroups of $K(\overline{W}(q, t))$

4 The Group  $K(\overline{W}(q, t))$  (the direct limit of the  $K(W_k(q, t))$ 's) contains the subgroup  $\mathbb{Z}/n\mathbb{Z}$  for all  $n \geq 1$ , and

$K(\overline{W}(q, t))$  contains the subgroup  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  if and only if  $n$  and  $q$  are coprime.

(Analogous to  $E(\overline{\mathbb{F}}_q)$  when  $E$  is an ordinary elliptic curve.)

What does the proof use? ....

## Question

*Given an integer  $n \geq 1$ , does there exist a  $k \geq 1$  such that  $n$  divides the  $k$ th Fibonacci number?*

# Behavior of Torsion Subgroups of $K(\overline{W}(q, t))$

4 The Group  $K(\overline{W}(q, t))$  (the direct limit of the  $K(W_k(q, t))$ 's) contains the subgroup  $\mathbb{Z}/n\mathbb{Z}$  for all  $n \geq 1$ , and

$K(\overline{W}(q, t))$  contains the subgroup  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  if and only if  $n$  and  $q$  are coprime.

(Analogous to  $E(\overline{\mathbb{F}}_q)$  when  $E$  is an ordinary elliptic curve.)

What does the proof use? ....

## Question

*Given an integer  $n \geq 1$ , does there exist a  $k \geq 1$  such that  $n$  divides the  $k$ th Fibonacci number?*

Answer provided by a result of D.D Wall from 1960.

## Lemma (Wall 1960)

*The sequence  $\{F_k \pmod n : k \in \mathbb{Z}\}$  is periodic, and  $F_k \equiv 0 \pmod n$  for some  $k \geq 1$ .*

**Proof.** Finite number ( $n^2$ ) of possibilities for a window of length two, and an infinite number of  $k$ . Thus there will be two identical windows.

## Lemma (Wall 1960)

*The sequence  $\{F_k \bmod n : k \in \mathbb{Z}\}$  is periodic, and  $F_k \equiv 0 \bmod n$  for some  $k \geq 1$ .*

**Proof.** Finite number ( $n^2$ ) of possibilities for a window of length two, and an infinite number of  $k$ . Thus there will be two identical windows.

Using linear recurrence in both directions, we obtain periodicity.

## Lemma (Wall 1960)

*The sequence  $\{F_k \pmod n : k \in \mathbb{Z}\}$  is periodic, and  $F_k \equiv 0 \pmod n$  for some  $k \geq 1$ .*

**Proof.** Finite number ( $n^2$ ) of possibilities for a window of length two, and an infinite number of  $k$ . Thus there will be two identical windows.

Using linear recurrence in both directions, we obtain periodicity.

Letting  $F_1 = F_2 = 1$  and running recurrence backwards,  $F_0 = 0$ . Thus  $F_{k_0} \equiv 0 \pmod n$  for some  $k_0 \geq 1$  too.

# Application to Torison Groups

## Theorem (M- 2009)

For  $k \geq 3$ , the Smith normal form of  $(L_k)_0$  is equivalent to a direct sum of the identity matrix and

$$\begin{bmatrix} q\hat{F}_{2k-4} + 1 & q\hat{F}_{2k-2} \\ \hat{F}_{2k-2} & \hat{F}_{2k} - 1 \end{bmatrix} \equiv \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}, \quad d_1 | d_2$$

where  $\hat{F}_k$  denotes a bivariate analogue of the Fibonacci numbers:

We let  $S$  range over all subsets  $\{1, 2, \dots, 2k\}$  with no two consecutive elements, and define

$$\hat{F}_{2k}(q, t) = \sum_S q^{\#\text{ even elements in } S} t^{k-\#S}.$$

# Application to Torison Groups

## Theorem (M- 2009)

For  $k \geq 3$ , the Smith normal form of  $(L_k)_0$  is equivalent to a direct sum of the identity matrix and

$$\begin{bmatrix} q\hat{F}_{2k-4} + 1 & q\hat{F}_{2k-2} \\ \hat{F}_{2k-2} & \hat{F}_{2k} - 1 \end{bmatrix} \equiv \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}, \quad d_1 | d_2$$

where  $\hat{F}_k$  denotes a bivariate analogue of the Fibonacci numbers:

We let  $S$  range over all subsets  $\{1, 2, \dots, 2k\}$  with no two consecutive elements, and define

$$\hat{F}_{2k}(q, t) = \sum_S q^{\#\text{ even elements in } S} t^{k-\#S}.$$

The  $\hat{F}_k$ 's satisfy the recurrence  $\hat{F}_{2k+2} = (1 + q + t)\hat{F}_{2k} - q\hat{F}_{2k-2}$ .

# Factorizations of $N_k$ and Elliptic Cyclotomic Polynomials

$$\mathcal{W}_k(q, t) = -N_k|_{N_1=-t} = \sum_{i=1}^k P_{k,i}(q) t^i \text{ for all } k \geq 1.$$

$\overline{M}_k$  be the  $k$ -by- $k$  “three-line” circulant matrix

$$\begin{bmatrix} 1+q+t & -q & 0 & \dots & 0 & -1 \\ -1 & 1+q+t & -q & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & -1 & 1+q+t & -q & 0 \\ 0 & \dots & 0 & -1 & 1+q+t & -q \\ -q & 0 & \dots & 0 & -1 & 1+q+t \end{bmatrix}.$$

Let  $M_k = \overline{M}_k|_{t=-N_1}$ .

Corollary (M- 2007)

The sequence of integers  $N_k = \#E(\mathbb{F}_{q^k})$  satisfies the relation

$$N_k = -\det M_k \text{ for all } k \geq 1.$$

# Elliptic Cyclotomic Polynomials

We have a determinantal formula for  $N_k$ , and

Combinatorial interpretations for the summands when we write  $N_k$  as an alternating sum in powers of  $N_1$

# Elliptic Cyclotomic Polynomials

We have a determinantal formula for  $N_k$ , and

Combinatorial interpretations for the summands when we write  $N_k$  as an alternating sum in powers of  $N_1$

We now look at factorizations of  $N_k$  into  $\mathbb{Z}[q, N_1]$  polynomials.

$$\text{e.g. } N_2 = N_1 \left( 2 + 2q - N_1 \right)$$

Motivates a combinatorial interpretation of  $E(\mathbb{F}_{q^k})$  as Cartesian Product of smaller subsets.

$$N_2 = N_1 \left( 2 + 2q - N_1 \right)$$

$$N_3 = N_1 \left( (3 + 3q + 3q^2) - (3 + 3q)N_1 + N_1^2 \right)$$

$$N_4 = N_1 \left( 2 + 2q - N_1 \right) \left( (2q^2 + 2) - (2q + 2)N_1 + N_1^2 \right)$$

$$N_5 = N_1 \left( (5 + 5q + 5q^2 + 5q^3 + 5q^4) - (10 + 15q + 15q^2 + 10q^3)N_1 \right. \\ \left. + (10 + 15q + 10q^2)N_1^2 - (5 + 5q)N_1^3 + N_1^4 \right)$$

$$N_6 = N_1 \left( 2 + 2q - N_1 \right) \left( (3 + 3q + 3q^2) - (3 + 3q)N_1 + N_1^2 \right) \\ \times \left( (q^2 - q + 1) - (q + 1)N_1 + N_1^2 \right)$$

Factoring  $N_k$  in general:

### Theorem (M- 2007)

*There exists integral polynomials, which we will denote as  $ECyc_d$ , in  $N_1$  and  $q$ , only depending on  $d$  such that*

$$N_k(N_1, q) = \prod_{d|k} ECyc_d.$$

Compare with  $1 - x^k = \prod_{d|k} Cyc_d(x)$ .

Factoring  $N_k$  in general:

### Theorem (M- 2007)

*There exists integral polynomials, which we will denote as  $ECyc_d$ , in  $N_1$  and  $q$ , only depending on  $d$  such that*

$$N_k(N_1, q) = \prod_{d|k} ECyc_d.$$

Compare with  $1 - x^k = \prod_{d|k} Cyc_d(x)$ .

We call these **Elliptic Cyclotomic Polynomials**.

### Definition

$ECyc_d(q, N_1) = Cyc_d(\alpha_1)Cyc_d(\alpha_2)$  where  $\alpha_1$  and  $\alpha_2$  are the two complex roots of quadratic  $T^2 - (1 + q - N_1)T + q$ , and

$$Cyc_d(x) = \prod_{e|d} (1 - x^e)^{\mu(d/e)}.$$

$$ECyc_1 = N_1$$

$$ECyc_2 = 2 + 2q - N_1$$

$$ECyc_3 = (3 + 3q + 3q^2) - (3 + 3q)N_1 + N_1^2$$

$$ECyc_4 = (2q^2 + 2) - (2q + 2)N_1 + N_1^2$$

$$ECyc_5 = (5 + 5q + 5q^2 + 5q^3 + 5q^4) - (10 + 15q + 15q^2 + 10q^3)N_1 \\ + (10 + 15q + 10q^2)N_1^2 - (5 + 5q)N_1^3 + N_1^4$$

$$ECyc_6 = (q^2 - q + 1) - (q + 1)N_1 + N_1^2$$

### Proposition (M- 2007)

$$ECyc_d \Big|_{N_1=0} = Cyc_d(1) \cdot Cyc_d(q)$$

where  $Cyc_1(1) = 0$ ,  $Cyc_d(1) = p$  if  $d = p^k$  and  $Cyc_d(1)$  equals 1 otherwise.

## Conjecture

$$\text{For } d \geq 2, \text{ } ECyc_d(q, N_1) = Cyc_d(1) \cdot Cyc_d(q) + \sum_{i=1}^{\phi(d)} (-1)^i Q_{i,d}(q) N_1^i$$

where  $Q_{i,d}$  is a univariate polynomial with positive integer coefficients.

## Conjecture

$$\text{For } d \geq 2, \text{ } ECyc_d(q, N_1) = Cyc_d(1) \cdot Cyc_d(q) + \sum_{i=1}^{\phi(d)} (-1)^i Q_{i,d}(q) N_1^i$$

where  $Q_{i,d}$  is a univariate polynomial with positive integer coefficients.

True for  $2 \leq d \leq 104$ .

## Conjecture

$$\text{For } d \geq 2, \text{ } ECyc_d(q, N_1) = Cyc_d(1) \cdot Cyc_d(q) + \sum_{i=1}^{\phi(d)} (-1)^i Q_{i,d}(q) N_1^i$$

where  $Q_{i,d}$  is a univariate polynomial with positive integer coefficients.

True for  $2 \leq d \leq 104$ .

However, Conjecture fails for  $d = 105$ .

Nonetheless, we can give a geometric interpretation of the values  $ECyc_d(q, N_1)$  for a given  $q$  and  $N_1 = |E(\mathbb{F}_q)|$ .

Nonetheless, we can give a geometric interpretation of the values  $ECyc_d(q, N_1)$  for a given  $q$  and  $N_1 = |E(\mathbb{F}_q)|$ .

### Theorem (M- 2007)

$$ECyc_d(q, N_1) = \left| \text{Ker } Cyc_d(\pi) : E(\overline{\mathbb{F}}_q) \circlearrowleft \right|$$

where  $Cyc_d(\pi)$  denotes the isogeny obtained from the  $d$ th Cyclotomic polynomial of the Frobenius map.

$$\text{Ker } M = \{P \in E(\overline{\mathbb{F}}_q) : M(P) = P_\infty\}$$

# From Chip-Firing to Tropical Geometry

Variant of earlier discussion: Let  $G = (V, E)$  be any **undirected** graph.

A **chip configuration**  $C$  is an assignment of integers to each vertex.

# From Chip-Firing to Tropical Geometry

Variant of earlier discussion: Let  $G = (V, E)$  be any **undirected** graph.

A **chip configuration**  $C$  is an assignment of integers to each vertex.

A **chip-firing move** is a choice of a vertex  $v_i$ .  $v_i$  gives  $d_{ij}$  chips to each of its neighbors  $v_j$ . Such chip configurations are also called **divisors**.

(Like algebraic geometric definition where a divisor is a formal  $\mathbb{Z}$ -linear combination of points on a curve.)

# From Chip-Firing to Tropical Geometry

Variant of earlier discussion: Let  $G = (V, E)$  be any **undirected** graph.

A **chip configuration**  $C$  is an assignment of integers to each vertex.

A **chip-firing move** is a choice of a vertex  $v_i$ .  $v_i$  gives  $d_{ij}$  chips to each of its neighbors  $v_j$ . Such chip configurations are also called **divisors**.

(Like algebraic geometric definition where a divisor is a formal  $\mathbb{Z}$ -linear combination of points on a curve.)

## Definition

The **degree** of a divisor  $D = \sum_{i=1}^n C_i v_i$  is  $\sum_{i=1}^n C_i$ .

$D$  is **effective** if  $C_i \geq 0$  for all  $i$ .

# From Chip-Firing to Tropical Geometry

Variant of earlier discussion: Let  $G = (V, E)$  be any **undirected** graph.

A **chip configuration**  $C$  is an assignment of integers to each vertex.

A **chip-firing move** is a choice of a vertex  $v_i$ .  $v_i$  gives  $d_{ij}$  chips to each of its neighbors  $v_j$ . Such chip configurations are also called **divisors**.

(Like algebraic geometric definition where a divisor is a formal  $\mathbb{Z}$ -linear combination of points on a curve.)

## Definition

The **degree** of a divisor  $D = \sum_{i=1}^n C_i v_i$  is  $\sum_{i=1}^n C_i$ .

$D$  is **effective** if  $C_i \geq 0$  for all  $i$ .

Two divisors  $D_1$  and  $D_2$  are said to be **linearly equivalent** ( $D_1 \sim D_2$ ) if  $D_2$  can be reached from  $D_1$  by a sequence of chip-firing moves.

# From Chip-Firing to Tropical Geometry

Variant of earlier discussion: Let  $G = (V, E)$  be any **undirected** graph.

A **chip configuration**  $C$  is an assignment of integers to each vertex.

A **chip-firing move** is a choice of a vertex  $v_i$ .  $v_i$  gives  $d_{ij}$  chips to each of its neighbors  $v_j$ . Such chip configurations are also called **divisors**.

(Like algebraic geometric definition where a divisor is a formal  $\mathbb{Z}$ -linear combination of points on a curve.)

## Definition

The **degree** of a divisor  $D = \sum_{i=1}^n C_i v_i$  is  $\sum_{i=1}^n C_i$ .

$D$  is **effective** if  $C_i \geq 0$  for all  $i$ .

Two divisors  $D_1$  and  $D_2$  are said to be **linearly equivalent** ( $D_1 \sim D_2$ ) if  $D_2$  can be reached from  $D_1$  by a sequence of chip-firing moves.

Equivalently,  $D_1 - D_2$  is a  $\mathbb{Z}$ -sum of columns of the Laplacian matrix  $L(G)$ .

## Definition

The **Linear System of  $D$** , denoted as  $|D|$ , is the set  $\{D' : D' \sim D \text{ and } D' \text{ is effective.}\}$ .

The following definitions are from Baker-Norine.

- 1 Let  $K(G) = [(deg v_1) - 2, (deg v_2) - 2, \dots, (deg v_n) - 2]$ , the **canonical divisor** of  $G$ .

## Definition

The **Linear System of  $D$** , denoted as  $|D|$ , is the set  $\{D' : D' \sim D \text{ and } D' \text{ is effective.}\}$ .

The following definitions are from Baker-Norine.

- 1 Let  $K(G) = [(deg v_1) - 2, (deg v_2) - 2, \dots, (deg v_n) - 2]$ , the **canonical divisor** of  $G$ .
- 2  $g(G) = |E| - |V| + 1$ , the **genus** of  $G$ . Also the 1st Betti number of the graph as a 1-complex.

## Definition

The **Linear System of  $D$** , denoted as  $|D|$ , is the set  $\{D' : D' \sim D \text{ and } D' \text{ is effective.}\}$ .

The following definitions are from Baker-Norine.

- 1 Let  $K(G) = [(deg v_1) - 2, (deg v_2) - 2, \dots, (deg v_n) - 2]$ , the **canonical divisor** of  $G$ .
- 2  $g(G) = |E| - |V| + 1$ , the **genus** of  $G$ . Also the 1st Betti number of the graph as a 1-complex.
- 3 The **rank** of  $D$ ,  $r(D)$ , is the biggest  $k \geq 0$  such that for all effective  $E$  of degree  $k$ ,  $|D - E| \neq \emptyset$  if such a  $k$  exists.  
(By convention  $r(D) = -1$  if  $|D| = \emptyset$ .)

# From Chip-Firing to Tropical Geometry

## Definition

The **Linear System of  $D$** , denoted as  $|D|$ , is the set  $\{D' : D' \sim D \text{ and } D' \text{ is effective.}\}$ .

The following definitions are from Baker-Norine.

- 1 Let  $K(G) = [(deg v_1) - 2, (deg v_2) - 2, \dots, (deg v_n) - 2]$ , the **canonical divisor** of  $G$ .
- 2  $g(G) = |E| - |V| + 1$ , the **genus** of  $G$ . Also the 1st Betti number of the graph as a 1-complex.
- 3 The **rank** of  $D$ ,  $r(D)$ , is the biggest  $k \geq 0$  such that for all effective  $E$  of degree  $k$ ,  $|D - E| \neq \emptyset$  if such a  $k$  exists.  
(By convention  $r(D) = -1$  if  $|D| = \emptyset$ .)

Theorem (Baker-Norine 2006 - Riemann-Roch Theorem for Graphs)

$$r(D) - r(K - D) = \deg D - g + 1.$$

# From Chip-Firing to Tropical Geometry

This has motivated search for further analogies between algebraic curve theory and graph theory.

# From Chip-Firing to Tropical Geometry

This has motivated search for further analogies between algebraic curve theory and graph theory.

Gathmann-Kerber and Mikhalkin-Zharkov showed

## Corollary

*Riemann-Roch Theorem for Tropical Curves (Metric graphs satisfying certain balancing conditions)*

# From Chip-Firing to Tropical Geometry

This has motivated search for further analogies between algebraic curve theory and graph theory.

Gathmann-Kerber and Mikhalkin-Zharkov showed

## Corollary

*Riemann-Roch Theorem for Tropical Curves (Metric graphs satisfying certain balancing conditions)*

With Christian Haase and Josephine Yu:

- 1 We explicitly describe cell structures of  $|D|$  as a polyhedral cell complex
- 2 Show how to embed  $|D|$  into tropical projective space.
- 3 Also get generalization of chip-firing to metric graphs, called weighted chip-firing games.

<http://arxiv.org/pdf/0909.3685.pdf>

THANKS FOR COMING

<http://math.mit.edu/~musiker/CGs.pdf>

G. Musiker, *Combinatorial aspects of elliptic curves*, Seminaire Lotharingien de Combinatoire 56 (2007), Article B56f, 1-31

G. Musiker, *The critical groups of a family of graphs and elliptic curves over finite fields*, Journal of Algebraic Combinatorics: Vol. 30, Issue 2 (2009), 255–276

C. Haase, G. Musiker, and J. Yu, *Linear systems on tropical curves*, <http://arxiv.org/pdf/0909.3685.pdf>