The Zeta Function of a Cyclic Language with Connections to Elliptic Curves and Chip-Firing Games

Gregg Musiker

University of California, San Diego

March 14, 2007

OUTLINE

I. Introduction

II. Elliptic Curves

III. A Combinatorial Interpretation of N_k

IV. Determinantal Formula

V. Chip-Firing Games

VI. Critical Groups

VII. Connection to Cyclic Languages

I. INTRODUCTION

The **zeta function** of a Formal Language L is defined as [Berstel and Reutenauer, 1990]

$$\zeta(L) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)$$

where $a_n = |L \cap A^n|$ is the number of words of length n in L.

The **zeta function** of a Formal Language L is defined as [Berstel and Reutenauer, 1990]

$$\zeta(L) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)$$

where $a_n = |L \cap A^n|$ is the number of words of length n in L.

Furthermore, a Language is **cyclic** if it is closed under conjugation and powers (i.e. $uv \in L$ if and only if vu in L and w in L implies that $w^m \in L$ for all m.)

The **zeta function** of a Formal Language L is defined as [Berstel and Reutenauer, 1990]

$$\zeta(L) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)$$

where $a_n = |L \cap A^n|$ is the number of words of length n in L.

Furthermore, a Language is **cyclic** if it is closed under conjugation and powers (i.e. $uv \in L$ if and only if vu in L and w in L implies that $w^m \in L$ for all m.)

Theorem 1. *If L is a cyclic language which is recognizable by a finite automaton, then its zeta function is rational.*

The **zeta function** of a Formal Language L is defined as [Berstel and Reutenauer, 1990]

$$\zeta(L) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)$$

where $a_n = |L \cap A^n|$ is the number of words of length n in L.

Furthermore, a Language is **cyclic** if it is closed under conjugation and powers (i.e. $uv \in L$ if and only if vu in L and w in L implies that $w^m \in L$ for all m.)

Theorem 1. *If L is a cyclic language which is recognizable by a finite automaton, then its zeta function is rational.*

We compare with the theory of zeta functions for algebraic varieties.

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

We can also let K be a field extension of $\mathbb{F}_q$, such as $\mathbb{F}_{q^k}$, or even the algebraic closure $\overline{\mathbb{F}_q}$.

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

We can also let K be a field extension of $\mathbb{F}_q$, such as $\mathbb{F}_{q^k}$, or even the algebraic closure $\overline{\mathbb{F}_q}$.

A model for a non-singular projective curve (with a rational point) defined over K is the zero locus of an equation $f(x, y)$ with coefficients in K, plus a single point at infinity. We denote such a curve as C.

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

We can also let K be a field extension of $\mathbb{F}_q$, such as $\mathbb{F}_{q^k}$, or even the algebraic closure $\overline{\mathbb{F}_q}$.

A model for a non-singular projective curve (with a rational point) defined over K is the zero locus of an equation $f(x, y)$ with coefficients in K, plus a single point at infinity. We denote such a curve as C.

$C(\mathbb{F}_q)$, $C(\mathbb{F}_{q^k})$, or $C(\overline{\mathbb{F}_q})$ will denote the curve C over these fields, respectively. (This means that solutions (x, y) to equation f have coordinates in $\mathbb{F}_q$, $\mathbb{F}_{q^k}$ and $\overline{\mathbb{F}_q}$, respectively.)

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

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

Curve C over field K has defining equation $f(x, y) = 0$ with coefficients in K.

Such a curve consists of a single point at infinity, P_∞, and affine points expressed as a pair of coordinates over K.

The **Frobenius** map π 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 1. *For point* $P \in C(\overline{\mathbb{F}_q})$,

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

Fact 2. *For point* $P \in C(\mathbb{F}_{q^k})$,

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

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

Alternatively, N_m counts the number of points in $C(\overline{\mathbb{F}_q})$ which are fixed by the mth power of the Frobenius map, π^m.

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.

$$\begin{aligned} Z(C,T) &= \exp\left(\sum_{m=1}^{\infty} N_m \frac{T^m}{m}\right) \\ &= \prod_{\mathfrak{p}} \frac{1}{1 - T^{deg\ \mathfrak{p}}} \quad \text{where } \mathfrak{p} \text{ is a prime ideal} \end{aligned}$$

$$\zeta(s) = \prod_{p \text{ prime integer}} \frac{1}{1 - p^{-s}}$$

Theorem 2 (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 α_i's, where g is the genus of the curve C. Furthermore, the numerator of $Z(C,T)$, which we will denote as $L(C,T)$, has integer coefficients.

Theorem 3 (Functional Equation - Weil 1948).

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

Theorem 2 (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 α_i's, where g is the genus of the curve C. Furthermore, the numerator of $Z(C,T)$, which we will denote as $L(C,T)$, has integer coefficients.

Theorem 3 (Functional Equation - Weil 1948).

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

In particular, the zeta function for a cyclic language and the zeta function for an algebraic curve are both rational.

Theorem 2 (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 α_i's, where g is the genus of the curve C. Furthermore, the numerator of $Z(C,T)$, which we will denote as $L(C,T)$, has integer coefficients.

Theorem 3 (Functional Equation - Weil 1948).

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

In particular, the zeta function for a cyclic language and the zeta function for an algebraic curve are both rational.

Question: Is there a cyclic language whose zeta function agrees with the zeta function for an elliptic curve?

II. ELLIPTIC CURVES

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

Fact 3. *E can be represented as the zero locus in $\mathbb{P}^2$ of the equation*

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

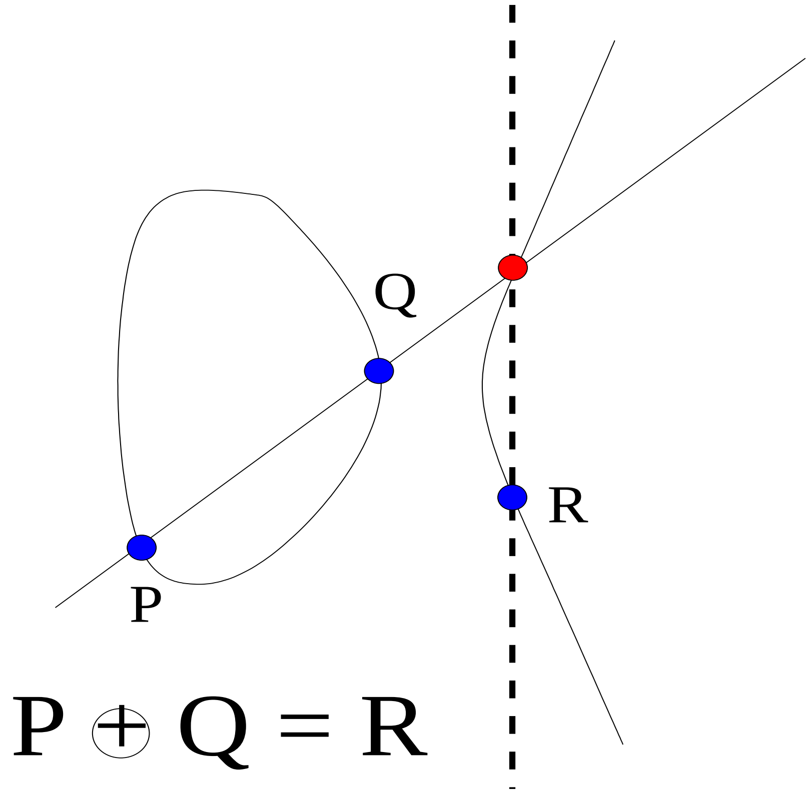
for $A, B \in \mathbb{F}_q$. (if $p \neq 2,\ 3$)

Fact 4. *E has a group structure where two points on E can be added to yield another point on the curve.*

Fact 5. *The Frobenius map is compatible with the group structure:*

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

Draw Chord/Tangent Line and then reflect about horizontal axis



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

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

1) If $x_1 \neq x_2$ then

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

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

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

4) P_∞ acts as the identity element in this addition.

Rationality (Weil 1948, 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 α_1 and α_2. (In fact $|\alpha_1| = |\alpha_2| = \sqrt{q}$.)

Functional Equation (Weil 1948)

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

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

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 4 (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 4 (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.

$$\begin{aligned}
N_2 &= (2+2q)N_1 - N_1^2 \\
N_3 &= (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
N_4 &= (4+4q+4q^2+4q^3)N_1 - (6+8q+6q^2)N_1^2 + (4+4q)N_1^3 - N_1^4 \\
N_5 &= (5+5q+5q^2+5q^3+5q^4)N_1 - (10+15q+15q^2+10q^3)N_1^2 \\
&+ (10+15q+10q^2)N_1^3 - (5+5q)N_1^4 + N_1^5
\end{aligned}$$

Question 1. *What is a combinatorial interpretation of these expressions, i.e. of the $P_{k,i}$'s?*

III. A COMBINATORIAL INTERPRETATION OF N_k.

Fibonacci Numbers

$$F_n = F_{n-1} + F_{n-2}$$

$$F_0 = 1, \quad F_1 = 1$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34 \ldots$$

Counts the number of subsets of $\{1, 2, \ldots, n-1\}$ with no two elements consecutive

e.g. $F_5 = 8: \quad \{\ \},\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,3\},\ \{1,4\},\ \{2,4\}$

Lucas Numbers

$$L_n = L_{n-1} + L_{n-2}$$

$$L_1 = 1, \quad L_2 = 3$$

$$1, 3, 4, 7, 11, 18, 29, 47, \ldots$$

Counts the number of subsets of $\{1, 2, \ldots, \mathbf{n}\}$ with no two elements **circularly** consecutive

e.g. $L_4 = 7 :$ $\{\ \}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1, 3\}$, $\{2, 4\}$

By Convention and Recurrence: $L_0 = 2$

Definition 1. *We define the* $(\mathbf{q}, \mathbf{t})-$**Lucas numbers** *to be a sequence of polynomials in variables* q *and* t *such that* $L_n(q,t)$ *is defined as*

$$L_n(q,t) = \sum_S q^{\#\text{ even elements in } S}\, t^{\lfloor \frac{n}{2} \rfloor - \#S}$$

where the sum is over subsets S *of* $\{1, 2, \ldots, n\}$ *such that no two numbers are circularly consecutive.*

Theorem 5.

$$L_{2k}(q,t) = 1 + q^k - N_k \Big|_{N_1 = -t}$$

The $L_{2k}(q,t)$'s satisfy recurrence relation

$$L_{2k+2}(q,t) = (1 + q + t)L_{2k}(q,t) - qL_{2k-2}(q,t).$$

Symmetric Function Aside: We can also think of this plethystically as

$$L_{2k}(q, -N_1) = 1 + q^k - p_k[1 + q - \alpha_1 - \alpha_2].$$

Symmetric Function Aside: We can also think of this plethystically as

$$L_{2k}(q, -N_1) = 1 + q^k - p_k[1 + q - \alpha_1 - \alpha_2].$$

Symmetric Functions give rise to other identities including:

$$\# \text{ Positive Divisors of degree k} \quad = \quad h_k[1 + q - \alpha_1 - \alpha_2] \quad \text{and}$$

$$(-1)^k F_{2k-1}(q, -N_1) \quad = \quad e_k[1 + q - \alpha_1 - \alpha_2]$$

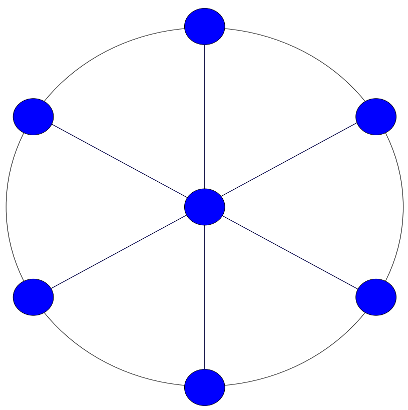
for suitably defined bivariate Fibonacci polynomials.

Question 2. *Is there a generating function equal to* N_k *directly?*

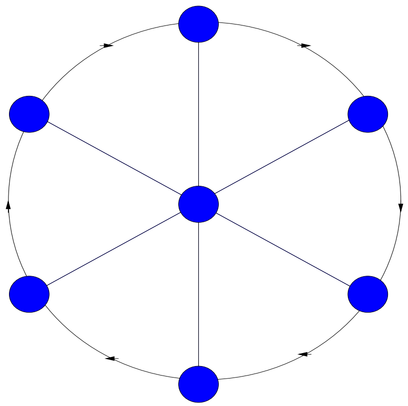
Question 2. *Is there a generating function equal to N_k directly?*

We can come close.

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



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



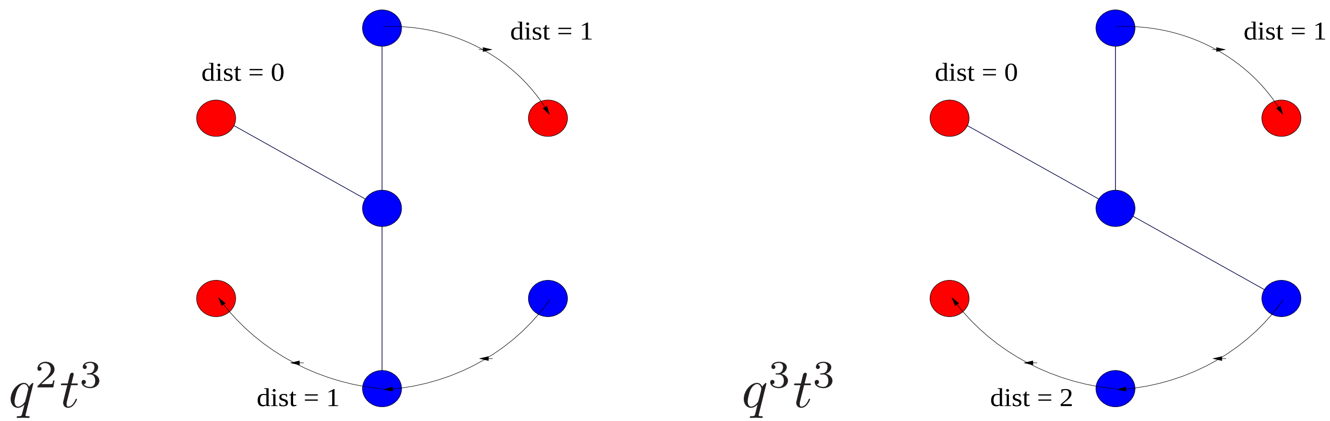
We note that a spanning tree will consist of arcs on the rim and spokes. We orient the arcs clockwise and designate the head of each arc.

Definition 2.

$$\mathcal{W}_k(q,t) = \sum_{\text{spanning trees of } W_k} q^{\text{total dist from spokes to tails}}\ t^{\#\text{ spokes}}.$$

Theorem 6.

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



The proof uses combinatorial facts from [Eğeciouğlu-Remmel 1990] and [Benjamin-Yerger 2004].

IV. A DETERMINANTAL FORMULA FOR N_k

Let $M_1 = [-N_1]$, $M_2 = \begin{bmatrix} 1+q-N_1 & -1-q \\ -1-q & 1+q-N_1 \end{bmatrix}$, and for $k \geq 3$,

let M_k be the k-by-k "three-line" circulant matrix

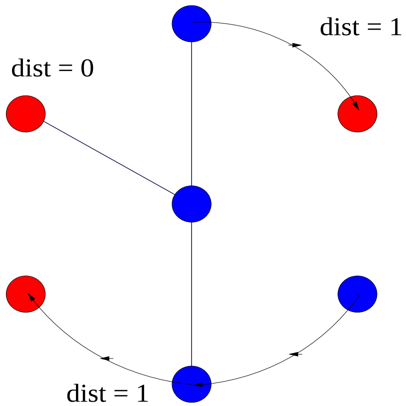
$$\begin{bmatrix} 1+q-N_1 & -1 & 0 & \dots & 0 & -q \\ -q & 1+q-N_1 & -1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & -q & 1+q-N_1 & -1 & 0 \\ 0 & \dots & 0 & -q & 1+q-N_1 & -1 \\ -1 & 0 & \dots & 0 & -q & 1+q-N_1 \end{bmatrix}.$$

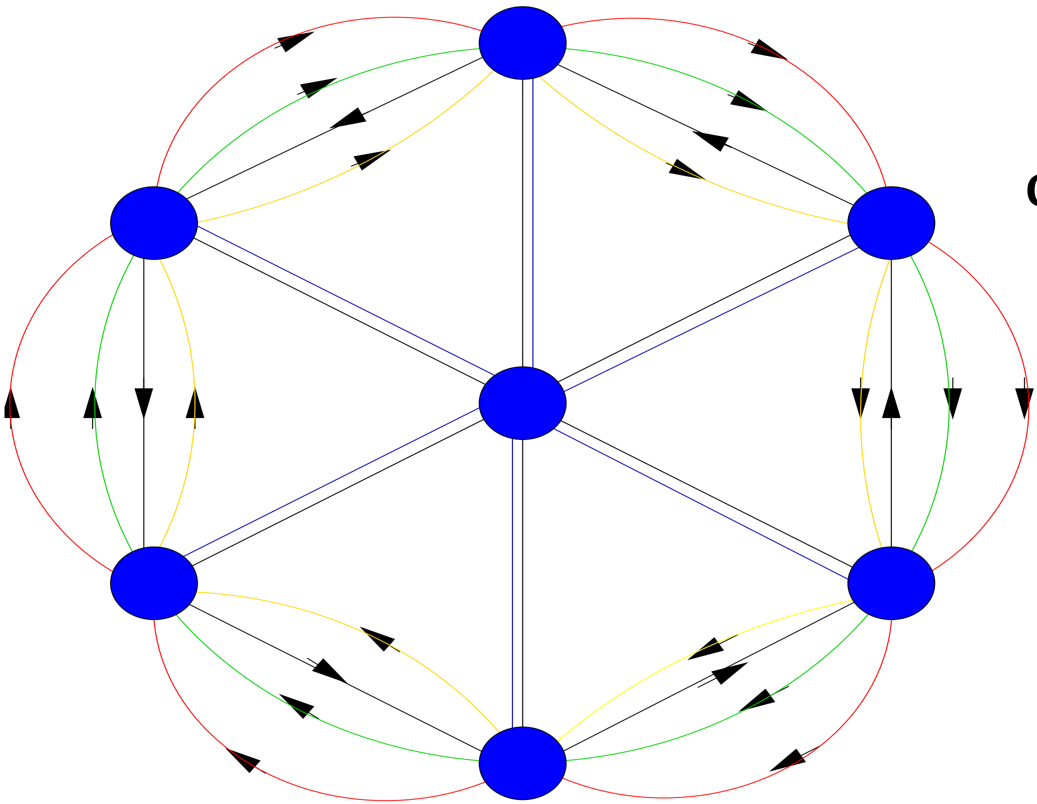
Theorem 7. *The sequence of integers $N_k = \#E(\mathbb{F}_{q^k})$ satisfies the relation*

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

Analogously, $\mathcal{W}_k(q,t) = \det M_k|_{N_1=-t}$.

$q^2 t^3$





q = 3
t = 2

Proof by the Matrix-Tree Theorem:

The Laplacian Matrix for $W_k(q,t)$ is

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

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

By the Matrix-Tree theorem, the number of directed rooted spanning trees is $\det L_0$ where L_0 is matrix L with the last row and last column deleted.

V. CHIP-FIRING GAMES

Let G be a finite loopless directed multi-graph.

That is $G = (V, E)$ where V is a finite set $\{v_1, v_2, \ldots, v_n\}$ and E is a multiset whose elements are pairs from $V \times V$.

For every vertex v_i let C_i be a nonnegative integer representing the number of chips on vertex v_i.

Let G be a finite loopless directed multi-graph.

That is $G = (V, E)$ where V is a finite set $\{v_1, v_2, \ldots, v_n\}$ and E is a multiset whose elements are pairs from $V \times V$.

For every vertex v_i let C_i be a nonnegative integer representing the number of chips on vertex v_i.

If there is an edge $e = (v_i, v_j)$ in E, we say that v_i and v_j are adjacent, and that edge e is directed from v_i to v_j.

The **outdegree** of a vertex v_i, d_i is the number of edges in E with first coordinate v_i.

We call vertex v_j a **neighbor** of v_i if edge $(v_i, v_j) \in E$.

Finally, we let d_{ij} be the number of edges (v_i, v_j) in E.

Chip-Firing: (Björner, Lovász, Shor)

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

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.

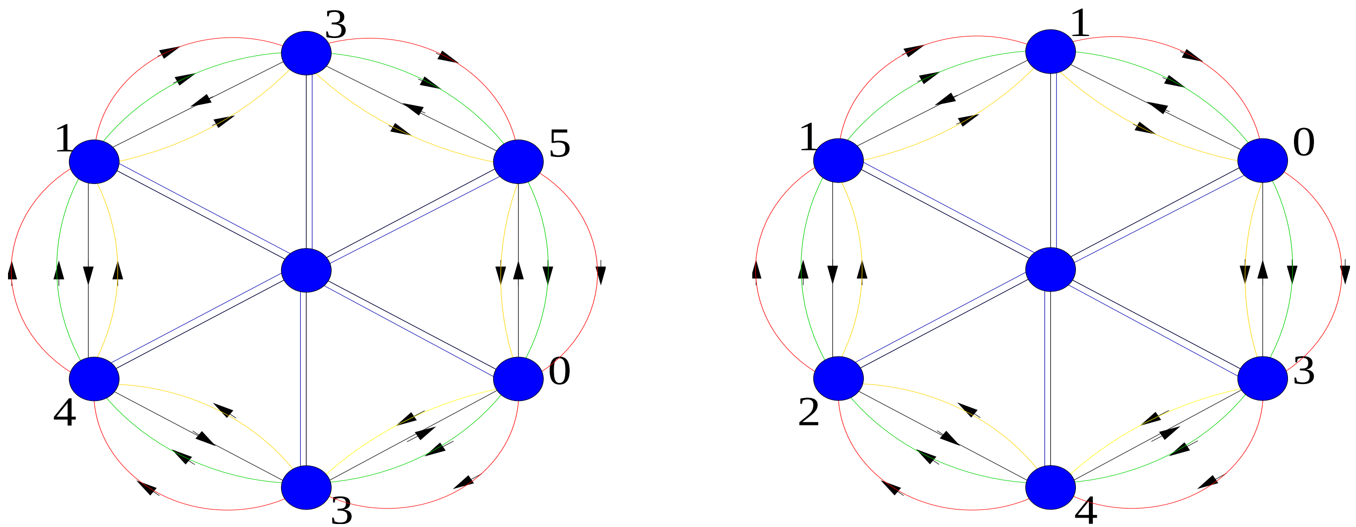
(Note that this will necessarily require the use of v_0 firing.)

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

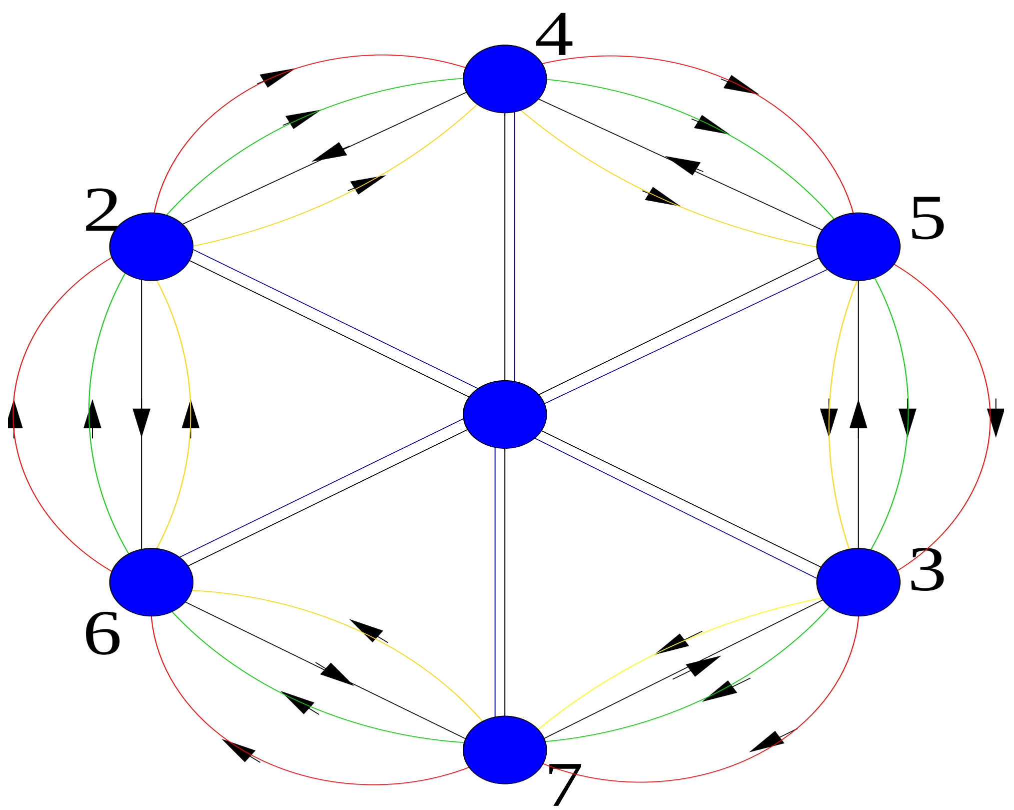
Theorem 8 (Biggs 1999). *For any initial configuration C with $\sum_{i=0}^{k} C_i = 0$ and $C_i \geq 0$ for all $1 \leq i \leq k$, there exists a* unique *critical configuration that can be reached by an allowable firing sequence.*

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

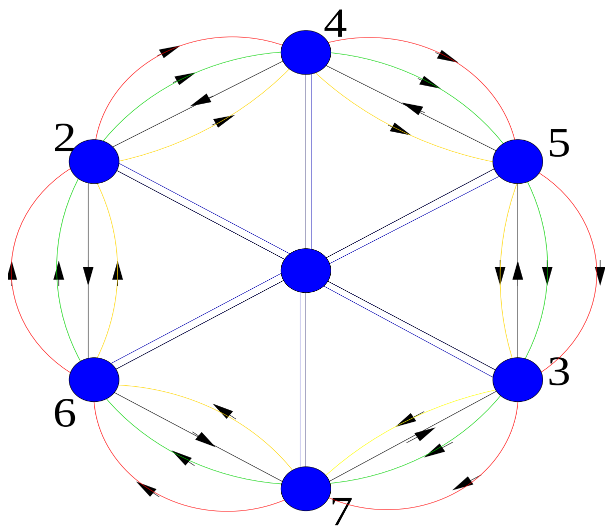
We do not label the number of chips on the hub vertex since forced.

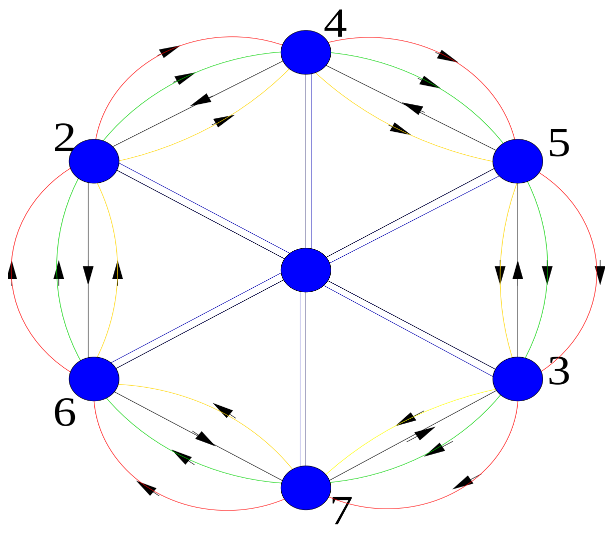


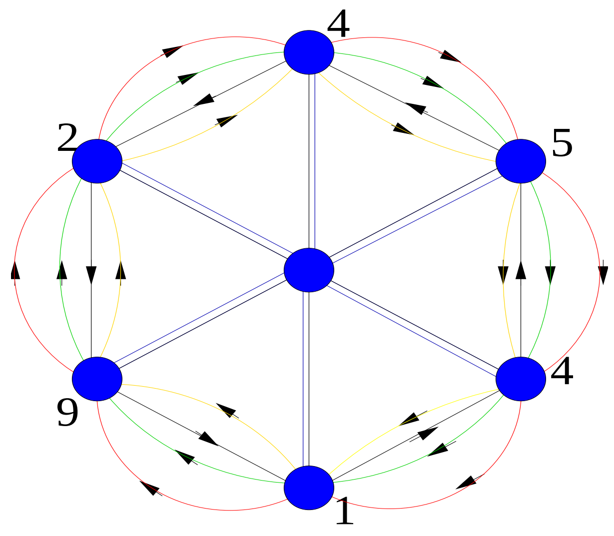
If we add these together pointwise we obtain

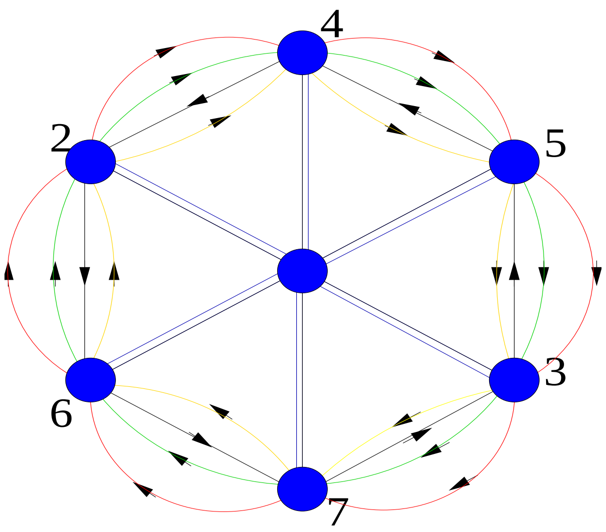


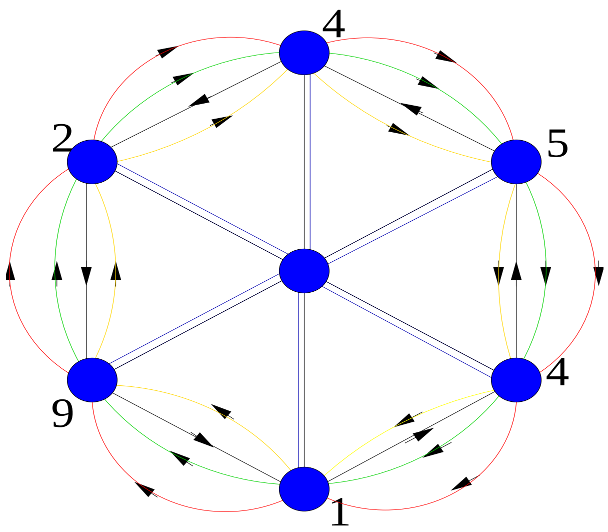
This is not a critical configuration, but by the theorem, reduces to a unqiue critical configuration.

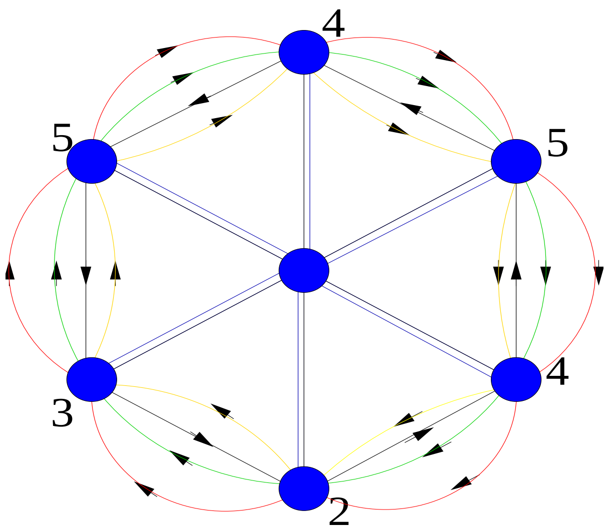

4
2
5
3
6
7


4
2
5
6
3
7


4
2
5
9
4
1







This last one is critical.

The **critical group of graph** G, with respect to vertex 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 reachable from C.

When v_0 is understood, we will abbreviate this group as the critical group of graph G, and denote it as $\mathcal{C}(G)$.

The **critical group of graph** G, with respect to vertex 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 reachable from C.

When v_0 is understood, we will abbreviate this group as the critical group of graph G, and denote it as $\mathcal{C}(G)$.

Theorem 9 (Biggs 1999). *$\mathcal{C}(G)$ is an abelian (associative) group.*

The **critical group of graph** G, with respect to vertex 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 reachable from C.

When v_0 is understood, we will abbreviate this group as the critical group of graph G, and denote it as $\mathcal{C}(G)$.

Theorem 9 (Biggs 1999). $\mathcal{C}(G)$ *is an abelian (associative) group.*

Alternative definition:

$$\mathcal{C}(G) \cong \mathbb{Z}^{|V(G)|-1} \Big/ Im\ \ L_0\, \mathbb{Z}^{|V(G)|-1}$$

where L_0 is the Laplacian matrix of graph G with the last row and last column deleted.

We get in particular that

$$|\mathcal{C}(G)| = \#\text{Spanning Trees in Graph } G$$

(using the Matrix-Tree Theorem again.)

We get in particular that

$$|\mathcal{C}(G)| = \#\text{Spanning Trees in Graph } G$$

(using the Matrix-Tree Theorem again.)

Proposition 1. *There exists a natural bijection between rooted spanning trees of the directed (q,t)-wheel multi-graph on k rim vertices, and critical configurations of the same graph. (Multi-graph analogue of Biggs-Winkler 1997 for this special case.)*

Note: We abbreviate the configuration vector as $[C_1, C_2, \ldots, C_{\#V(G)-1}]$, leaving off coefficient C_0, which is forced by the relation

$$\sum_{i=0}^{\#V(G)-1} C_i = 0.$$

VI. CRITICAL GROUPS OF (q, t)-WHEEL GRAPHS

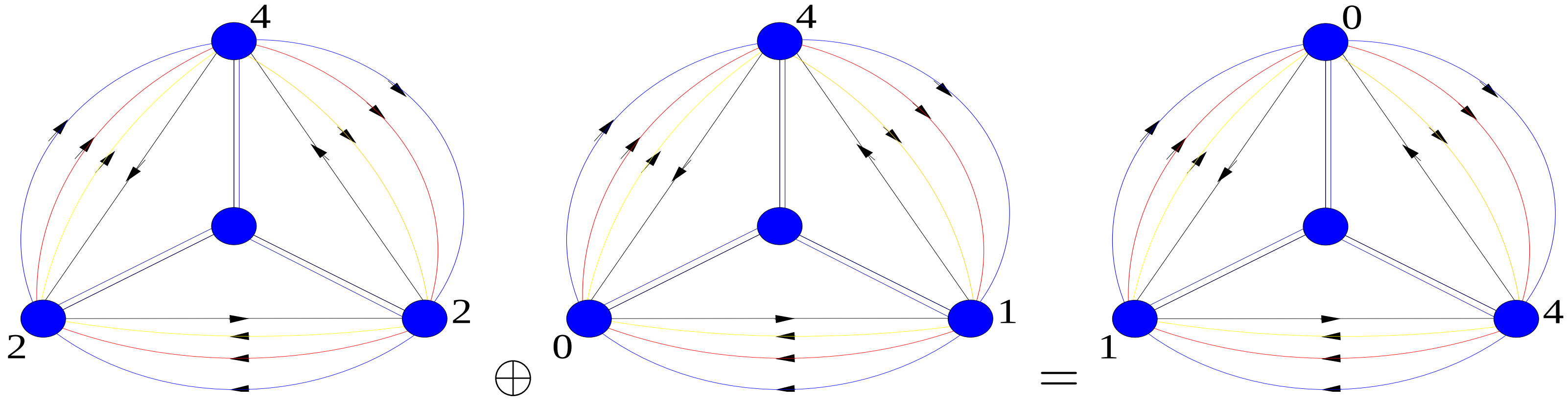
Understanding the sequence of Critical Groups:

$$\mathcal{C}(W_1(q,t)),\ \mathcal{C}(W_2(q,t)),\ \mathcal{C}(W_3(q,t)),\ \dots$$

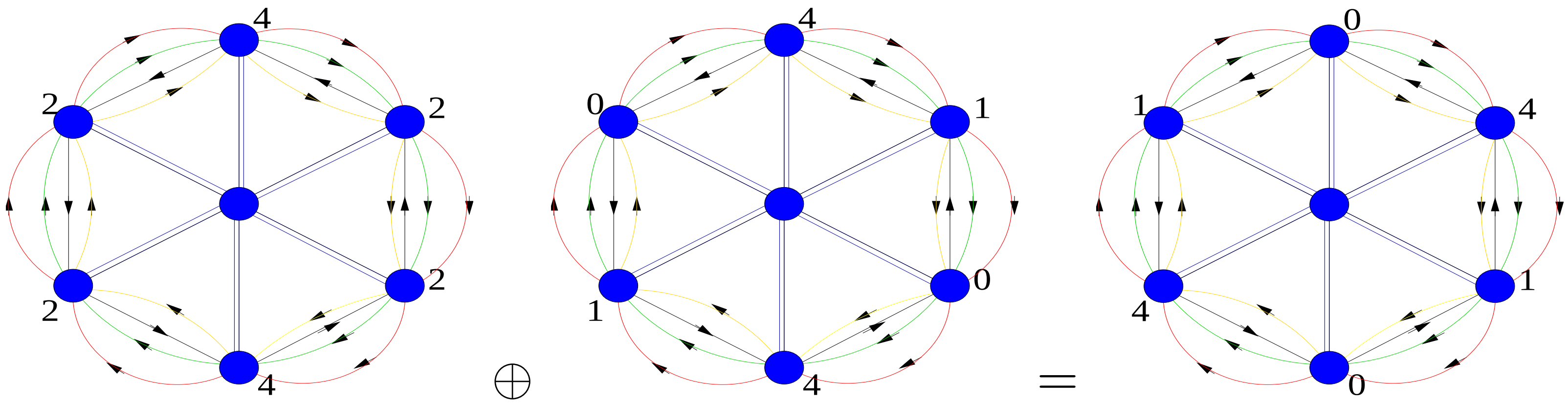
The set $\left\{\text{Elements of the critical group } \mathcal{C}(W_k(q,t))\right\}$ is a subset of the set of length k words in alphabet $\{0,1,2,\dots,q+t\}$.

Proposition 2. *The map $\psi : w \to www\dots w$ is an injective group homomorphism between $\mathcal{C}(W_{k_1}(q,t))$ and $\mathcal{C}(W_{k_2}(q,t))$ whenever $k_1|k_2$. Here map ψ replaces w with k_2/k_1 copies of w.*

Example: $[2,4,2] \oplus [0,4,1] \equiv [1,0,4]$ in $\mathcal{W}_3(q=3, t=2)$ versus



$[2,4,2,2,4,2] \oplus [0,4,1,0,4,1] \equiv [1,0,4,1,0,4]$ in $\mathcal{W}_6(q=3, t=2)$



Chip-firing is a local process.

Proposition 2. *The map* $\psi : w \rightarrow www\dots w$ *is an injective group homomorphism between* $\mathcal{C}(W_{k_1}(q,t))$ *and* $\mathcal{C}(W_{k_2}(q,t))$ *whenever* $k_1|k_2$*. Here map* ψ *replaces* w *with* k_2/k_1 *copies of* w*.*

Define ρ to be the rotation map on $\mathcal{C}(W_k(q,t))$.

If we consider elements of the critical group to be configuration vectors, then we mean clockwise rotation of elements to the right.

Equivalently, ρ acts by rotating the rim vertices of W_k clockwise if we view elements of $\mathcal{C}(W_k(q,t))$ as spanning trees.

Proposition 3. *The kernel of* $(1-\rho^{k_1})$ *acting on* $\mathcal{C}(W_{k_2}(q,t))$ *is isomorphic to the subgroup* $\mathcal{C}(W_{k_1}(q,t))$ *whenever* $k_1|k_2$*.*

Proposition 3. *The kernel of* $(1-\rho^{k_1})$ *acting on* $\mathcal{C}(W_{k_2}(q,t))$ *is isomorphic to the subgroup* $\mathcal{C}(W_{k_1}(q,t))$ *whenever* $k_1 | k_2$.

We therefore can define a direct limit

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

where ρ provides the transition maps.

Another view of $\mathcal{C}(\overline{W}(q,t))$:

The set of bi-infinite words which are (1) periodic, and (2) have fundamental subword, i.e. pattern, equal to a configuration vector in $\mathcal{C}(W_k(q,t))$ for some $k \geq 1$.

In this interpretation, map ρ acts on $\mathcal{C}(\overline{W}(q,t))$ as the shift map.

In particular we obtain

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

We now can describe a combinatorial interpretation for the factorizations of $\mathcal{W}_k(q,t) = |\mathcal{C}(W_k(q,t))|$ into irreducible integral polynomials.

In particular we obtain

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

We now can describe a combinatorial interpretation for the factorizations of $\mathcal{W}_k(q,t) = |\mathcal{C}(W_k(q,t))|$ into irreducible integral polynomials.

Let ρ denote the shift map, $Cyc_d(x)$ be the dth cyclotomic polynomial $\left(x^k - 1 = \prod_{d|k} Cyc_d(x)\right)$, and $\mathcal{C}(\overline{W}(q,t))$ be the direct limit of the sequence $\{\mathcal{C}(W_k(q,t))\}_{k=1}^{\infty}$.

Theorem 10.

$$\mathcal{W}_k(q,t) = \prod_{d|k} WCyc_d(q,t) \quad \text{and}$$

$$WCyc_d = \left| Ker\left(Cyc_d(\rho)\right) : \ \mathcal{C}(\overline{W}(q,t)) \rightarrow \mathcal{C}(\overline{W}(q,t))\right|.$$

Shift map ρ is the wheel graph-analogue of the Frobenius map π on elliptic curves.

1. We have an analogous family of bivariate integral polynomials and factorizations

$$\begin{aligned} N_k(q,t) &= \prod_{d|k} ECyc_d(q,t) \quad \text{and} \\ ECyc_d &= \left| Ker\Big(Cyc_d(\pi)\Big) :\ E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q}) \right| \end{aligned}$$

where for $d \geq 2$, $ECyc_d(q, N_1) = WCyc_d(q,t)|_{t=-N_1}$.

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

3. We get the equation $\rho^2 - (1+q+t)\rho + q = 0$ on $\mathcal{C}(\overline{W}(q,t))$. This can be read off from matrix

$$M_k = \begin{bmatrix} 1+q-N_1 & -1 & 0 & \ldots & 0 & -q \\ -q & 1+q-N_1 & -1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & -q & 1+q-N_1 & -1 & 0 \\ 0 & \ldots & 0 & -q & 1+q-N_1 & -1 \\ -1 & 0 & \ldots & 0 & -q & 1+q-N_1 \end{bmatrix}$$

and the configuration vectors' images under clockwise and counter-clockwise rotation. This is a direct analogue of the characteristic equation $\pi^2 - (1+q-N_1)\pi + q = 0$ on $E(\overline{\mathbb{F}_q})$.

VII. CONNECTION TO CYCLIC LANGUAGES.

Spanning trees of wheel graphs have cyclic symmetry, and

Consist of disconnected arcs on the rim

(one such piece for each spoke)

Spanning trees of wheel graphs have cyclic symmetry, and

Consist of disconnected arcs on the rim

(one such piece for each spoke).

We can characterize (conjugates of) critical configurations of the wheel graph (q,t)-W_k as a concatonation of blocks with form

$$B, M_1, \ldots, M_r$$

with the properties

1. $B \in \{q+1, \ldots, q+t\}$,
2. $M_i \in \{0, 1, \ldots, q\}$, and
3. if $M_j = 0$, then $M_{j+1} = \cdots = M_r = q$.

Spanning trees of wheel graphs have cyclic symmetry, and

Consist of disconnected arcs on the rim

(one such piece for each spoke).

We can characterize (conjugates of) critical configurations of the wheel graph (q,t)-W_k as a concatonation of blocks with form

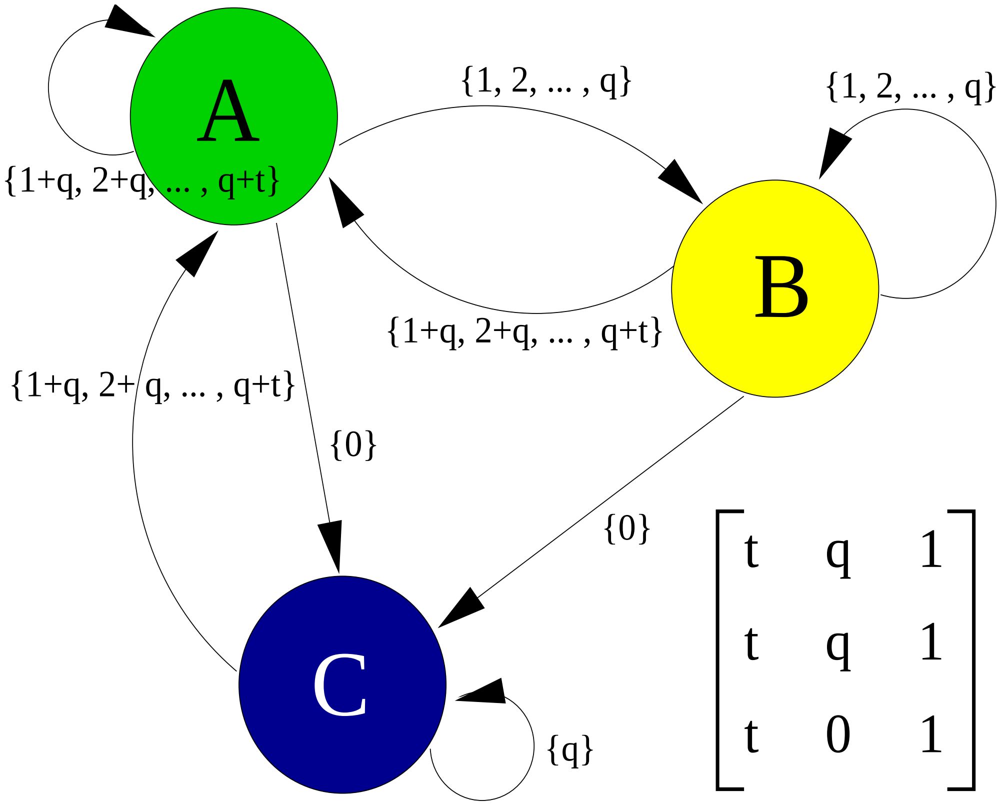
$$B, M_1, \dots, M_r$$

with the properties

1. $B \in \{q+1, \dots, q+t\}$, (Need at least one element $> q$
2. $M_i \in \{0, 1, \dots, q\}$ for config to be recurrent.)
3. if $M_j = 0$, then $M_{j+1} = \dots = M_r = q$. (Recurrent also forces.)

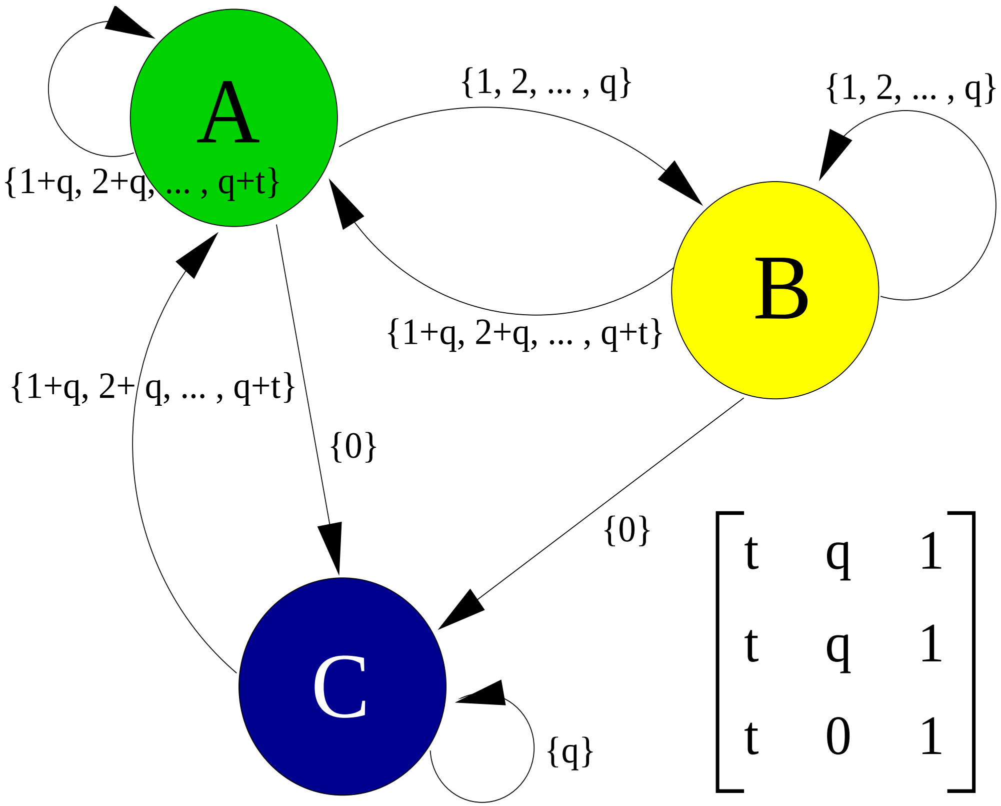
Considering these as elements of $\mathcal{C}(W_k(q,t)) \subset \mathcal{C}(\overline{W}(q,t))$, we identity $C_1, \dots, C_k$ with periodic string

$$\dots C_k, C_1, C_2, \dots C_{k-1}, C_k, C_1, \dots$$



$$\begin{bmatrix} t & q & 1 \\ t & q & 1 \\ t & 0 & 1 \end{bmatrix}$$

Critical Configurations correspond to Closed Paths in this DFA, $\mathcal{D}$, which go through state A.



$$\begin{bmatrix} t & q & 1 \\ t & q & 1 \\ t & 0 & 1 \end{bmatrix}$$

Critical Configurations correspond to Closed Paths in this DFA, $\mathcal{D}$, which go through state A.

Thus we disallow cycles containing only state B and cycles containing only state C.

Recall the zeta function of a Cyclic Language L is

$$\zeta(L,T) = \exp\left(\sum_{k=1}^{\infty} \mathcal{W}_k \frac{T^k}{k}\right)$$

where $\mathcal{W}_k$ is the number of words of length k.

Recall the zeta function of a Cyclic Language L is

$$\zeta(L,T) = \exp\left(\sum_{k=1}^{\infty} \mathcal{W}_k \frac{T^k}{k}\right)$$

where $\mathcal{W}_k$ is the number of words of length k.

Also can write

$$\zeta(L,T) \quad = \quad \exp\left(\sum_{\text{allowed closed paths } P} \#\text{ words admissible by path } P \;\; T^k\right).$$

Recall the zeta function of a Cyclic Language L is

$$\zeta(L,T) = \exp\left(\sum_{k=1}^{\infty} \mathcal{W}_k \frac{T^k}{k}\right)$$

where $\mathcal{W}_k$ is the number of words of length k.

Also can write

$$\zeta(L,T) \quad = \quad \exp\left(\sum_{\text{allowed closed paths } P} \# \text{ words admissible by path } P \;\; T^k\right).$$

The **trace** of an automaton $\mathcal{A}$ is the language of words generated by closed paths in $\mathcal{A}$, and satisfies

$$\zeta(trace(\mathcal{A})) = \frac{1}{\det(I - M \cdot T)},$$

where M encodes the number of directed edges between state i and state j in $\mathcal{A}$.

Let $L(W(q,t))$ be the language of patterns for set $\mathcal{C}((\overline{W})(q,t))$.

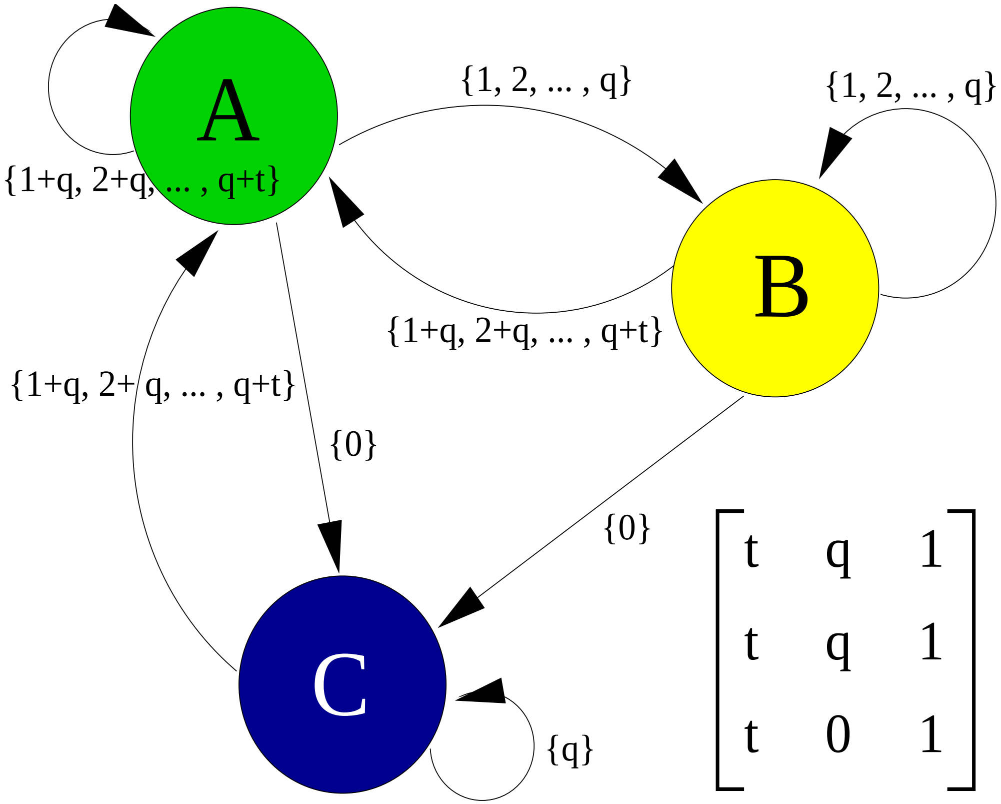
Language $L(W(q,t))$ also equals the set $\bigcup_{k=1}^{\infty} \mathcal{C}(W_k(q,t))$.

Let $L(W(q,t))$ be the language of patterns for set $\mathcal{C}((\overline{W})(q,t))$.

Language $L(W(q,t))$ also equals the set $\bigcup_{k=1}^{\infty} \mathcal{C}(W_k(q,t))$.

$$L(W(q,t)) = trace(\mathcal{D}) - trace(\mathcal{B}) - trace(\mathcal{C})$$

where we let $\mathcal{B}$ (resp. $\mathcal{C}$) signify the DFA we get by taking $\mathcal{D}$ and removing states A and C (resp. A and B).



Critical Configurations correspond to Closed Paths in this DFA, $\mathcal{D}$, which go through state A. Thus we disallow cycles containing only state B and cycles containing only state C.

$$\det(I - M \cdot T) = 1 - (1 + q + t)T - qT^2.$$

Let $L(W(q,t))$ be the language of patterns for set $\mathcal{C}((\overline{W})(q,t))$.

Language $L(W(q,t))$ also equals the set $\bigcup_{k=1}^{\infty} \mathcal{C}(W_k(q,t))$.

$$L(W(q,t)) = trace(\mathcal{D}) - trace(\mathcal{B}) - trace(\mathcal{C})$$

where we let $\mathcal{B}$ (resp. $\mathcal{C}$) signify the DFA we get by taking $\mathcal{D}$ and removing states A and C (resp. A and B).

Theorem 11.

$$\zeta(L(W(q,t))) = \frac{(1-T)(1-qT)}{1-(1+q+t)T-qT^2}.$$

Let $L(W(q,t))$ be the language of patterns for set $\mathcal{C}((\overline{W})(q,t))$.

Language $L(W(q,t))$ also equals the set $\bigcup_{k=1}^{\infty} \mathcal{C}(W_k(q,t))$.

$$L(W(q,t)) = trace(\mathcal{D}) - trace(\mathcal{B}) - trace(\mathcal{C})$$

where we let $\mathcal{B}$ (resp. $\mathcal{C}$) signify the DFA we get by taking $\mathcal{D}$ and removing states A and C (resp. A and B).

Theorem 11.

$$\zeta(L(W(q,t))) = \frac{(1-T)(1-qT)}{1-(1+q+t)T-qT^2}.$$

Compare with:

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