SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Cyclic sieving on closed walks in abelian Cayley graphs

av

Benjamin Khademi

2020 - No K23

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Cyclic sieving on closed walks in abelian Cayley graphs

Benjamin Khademi

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Per Alexandersson

2020

CYCLIC SIEVING ON CLOSED WALKS IN ABELIAN CAYLEY GRAPHS

BENJAMIN KHADEMI

Abstract. In this paper we study cyclic sieving on the set of closed walks of a particular length in abelian Cayley graphs. We interpret these walks as words in the alphabet of the generating set. We enumerate the number of such walks and their fixed point sets under the action of a cyclic group acting on the walks by way of cyclically shifting the letters of their corresponding words. We then show that this constitutes an instance of the cyclic sieving phenomenon. We show this first for cyclic graphs, then for circulant graphs before turning to the case of infinite rectangular grids. Finally, we also show it for Cayley graphs that are direct products of a finite number of circulant graphs.

Contents

1. Introduction

It is quite common for sets of combinatorial objects to exhibit some kind of cyclic symmetry. More surprisingly, it turns out that generating functions enumerating such sets, when evaluated at roots of unity, often count the fixed point sets under the action of some cyclic group on the set. This is called the cyclic sieving phenomenon. Since first introduced by Reiner, Stanton and White in 2004 [RSW04] many instances of cyclic sieving have been described.

In this paper we study the cyclic sieving phenomenon on closed walks in finite abelian Cayley graphs. That is, given a graph which is the Cayley graph of some finite abelian group we enumerate the number of walks of length m as a function of m, then construct a polynomial which is a generating polynomial of this enumeration and show that at roots of unity this polynomial counts the fixed point sets of a particular cyclic action on the set of walks.

The restriction of our study to Cayley graphs is fundamental. Walks in Cayley graphs can be naturally described as words in a generating set of the corresponding group. This allows us both to define a natural cyclic action on the set of walks and to employ combinatorial methods pertaining to words to understand these walks. Furthermore, many instances of cyclic sieving on sets of words are already known, so that the analogy with words allows our present study to build on those. The restriction to abelian groups on the other hand is done out of sheer necessity. We have simply made no progress with Cayley graphs of non-abelian groups. The restriction to finite graphs, finally, is somewhat arbitrary and we do briefly consider a family of infinite graphs. In the concluding remarks we state a few conjectures concerning cyclic sieving on closed walks in infinite Cayley graphs.

This paper is divided into two main parts.

In section 2 we cover some preliminaries. In section 2.1 we review some basic definitions from graph theory and discuss the relation between the number of closed walks in a graph and powers of its adjacency matrix. In section 2.2 we review some definitions from combinatorics, in particular the combinatorics of words. Section 2.3 covers algebra, in particular the construction of Cayley graphs from groups and we demonstrate some basic properties of such graphs. Section 2.4 introduces q-analogues and shows some properties of a few of the classic combinatorial q-analogues. All generating functions used to prove cyclic sieving in this paper are such q-analogues. Section 2.5 finally, gives a brief overview of the cyclic sieving phenomenon and a first basic example.

Section 3 contains our main results, where we find some new instances of cyclic sieving. Section 3.1 starts out softly by considering a small and simple family of graphs, the cycle graphs. We prove cyclic sieving on closed walks in cycle graph and find a combinatorial statistic for the generating polynomial. Section 3.2 largely mirrors 3.1 but for a more general family of graphs: the circulant graphs, which contains all Cayley graphs of finite cyclic groups. We prove cyclic sieving on closed walks in circulant graphs and again find a combinatorial statistic for the generating polynomial. Section 3.3 takes a slight detour into the subject of infinite graphs.

We prove cyclic sieving on closed walks in infinite rectangular grids by way of an "approximative" method, where we show that there is a circulant graph that has as many closed walks of a particular length as the infinite grid. In section 3.4 we show cyclic sieving on closed walks in Cayley graphs that are direct products of circulant graphs. This family of graphs contains Cayley graphs of any finite, abelian group but not every Cayley graph of a finite, abelian group.

2. Preliminaries

2.1. Basic graph theory.

We begin by establishing some basic facts of algebraic graph theory.

Definition 1. A graph is an ordered pair of sets $G = (V, E)$ such that $E \subseteq V^2$, that is the elements of E are two-element subsets of V. The elements of V are called vertices and the elements of E edges.

Remark. A graph as defined above is sometimes called a simple, undirected graph. This is to distinguish it from a multigraph or a directed graph. In a multigraph the set E is a multiset and so may include multiple instances of the same two-element set. Such graphs are often also allowed to include edges of the form $\{v, v\}, v \in V$, so called loops. In a directed graph, the edge-set E is taken to consist of ordered 2 -tuples $(v_i, v_j) \neq (v_j, v_i)$ In the context of this paper, however, an unqualified reference to a graph will always refer to an undirected, loop-free, simple graph.

Definition 2. If $u, v \in V$ and $\{u, v\} \in E$ then u and v are said to be adjacent or, informally, to be neighbours. The number of vertices adjacent to particular vertex v is the degree of v. If every vertex $v \in V$ has the same degree, the graph G is said to be a regular graph.

Definition 3. The adjacency matrix A of a graph $G = (V, E)$ on the vertex set $V = \{v_1, \ldots, v_n\}$ is the $n \times n$ matrix whose entries are given by

$$a_{ij} = \begin{cases} 1 & \{v_i, v_j\} \in E \\ 0 & \{v_i, v_j\} \notin E \end{cases}$$

Example 1. Figure 1 shows the graph $G = (V, E)$ with $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and $E = \{\{8, 1\}, \{8, 4\}, \{8, 7\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 6\}, \{3, 4\}, \{4, 5\}, \{5, 6\}, \{5, 7\}, \{6, 7\}\}$.The adjacency matrix A of G is given below.

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Notice how A is symmetric, has zeroes on the main diagonal and has every entry in $\{0, 1\}$. These properties of A reflect that G is an undirected, loop-free, simple graph.

Definition 4. A walk of length m in a graph G is a sequence of not necessarily distinct vertices of G $v_0, v_1, \ldots, v_{m+1}$ such that $\{v_i, v_{i+1}\} \in E$ for $0 \leq i \leq m$. More

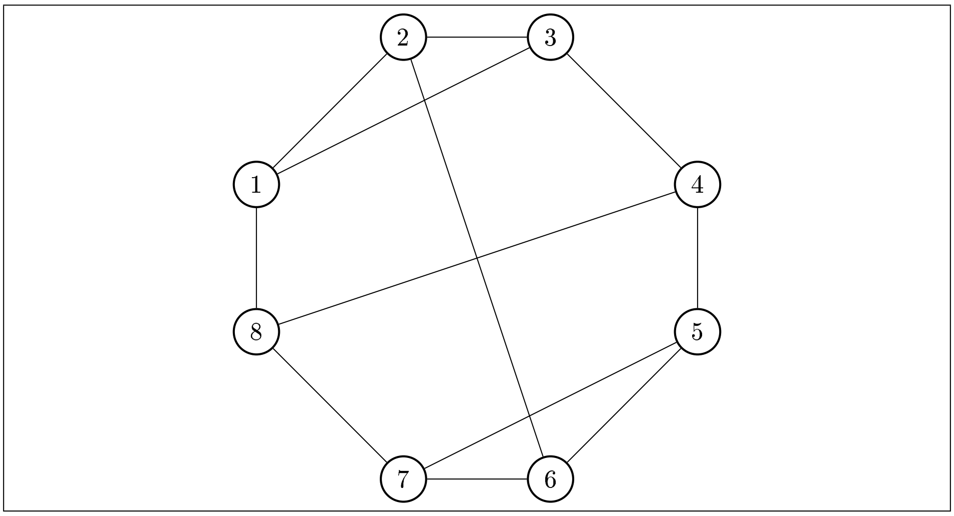

Figure 1: An example of a graph

specifically, this is said to be a walk from v_0 to v_{m+1}. If $v_0 = v_{m+1}$ it is said to be a closed walk.

Definition 5. A graph $G = (V, E)$ is said to be connected, if for every pair of distinct vertices $v_i, v_j \in V$ there is a walk beginning in v_i and ending in v_j.

Example 2. The graph G in Figure 1 is a connected graph. For such a small graph, this can be verified simply by looking at Figure 1. An example of a walk in G is $v = 8, 1, 2, 3, 1, 8, 7, 6, 2, 3, 4, 8, 7, 5$. The existence of v also proves connectivity, because it travels past every vertex in V.

We now prove our first important theorem, which will be critical in the following.

Theorem 1. *The number of walks of length m in a graph G from v_i to v_j, is the entry in position (i, j) of the matrix A^m, where A is the adjacency matrix of G. [Big74]*

Proof. The result is true for $m = 0$ since then $A^0 = I$ and for $m = 1$ since then A^1 is simply the adjacency matrix. Now suppose that the theorem is true for some $m = n$. By the definition av matrix multiplication we then have:

$$\left(A^{n+1}\right)_{ij} = \sum_{k=1}^{n} \left(A^n\right)_{ik} a_{kj} = \sum_{k:(v_k, v_j) \in E} \left(A^n\right)_{ik},$$

so that the (i, j)-th entry of A^{n+1} is the sum of those entries (i, k) in the i :th row of A^n for which v_k is a neighbour of v_j. By the induction hypothesis, this means that the (i, j)-th entry of A^{n+1} is the number of walks of length n from v_i to any neighbour of v_j, that is precisely the number of walks of length $n+1$ from v_i to v_j. So the theorem follows by induction. □

Example 3. For the adjacency matrix A of the graph G in Figure 1, we have:

$$A^3 = \begin{pmatrix} 2 & 5 & 6 & 1 & 4 & 2 & 1 & 6 \\ 5 & 2 & 5 & 3 & 2 & 5 & 2 & 3 \\ 6 & 5 & 2 & 6 & 1 & 2 & 4 & 1 \\ 1 & 3 & 6 & 0 & 6 & 3 & 1 & 7 \\ 4 & 2 & 1 & 6 & 2 & 5 & 6 & 1 \\ 2 & 5 & 2 & 3 & 5 & 2 & 5 & 3 \\ 1 & 2 & 4 & 1 & 6 & 5 & 2 & 6 \\ 6 & 3 & 1 & 7 & 1 & 3 & 6 & 0 \end{pmatrix}.$$

The ij-th entry of this matrix gives the number of walks of length 3 in G beginning in i and ending in j. For instance, $A^3_{11} = 2$ counts the walks $1,2,3,1$ and $1,3,2,1$.

Definition 6. By the trace of a $n \times n$ matrix A we mean the sum of its diagonal elements, that is

$$\operatorname{tr}(A) = \sum_{k=1}^{n} (A)_{kk}.$$

This definition allows us to formulate an important corollary to Theorem 2.1.

Corollary 1.1. *The number of closed walks of length m in a graph G equals* $\operatorname{tr}(A^m)$.

Corollary 1.1 will be crucial in enumerating the number of closed walks in different kinds of graphs, but the trace of a matrix can be expressed in another form as well, namely through its eigenvalues. We now state without proof a few well-known properties of eigenvectors and eigenvalues. For proof, consult probably any book on linear algebra, for instance [HU14]

Theorem 2. *Suppose that $v \in \mathbb{C}^n$ is a $n \times 1$ vector and that A and B are $n \times n$ matrices such that $Av = \lambda v$ and $Bv = \mu v$ for some scalars λ, μ. Then:*

- *The matrices $A + B, AB, cA, A^k$, where c is a scalar and $k \in \mathbf{N}$, also have v as an eigenvector with eigenvalues $\lambda + \mu, \lambda\mu, c\lambda$ and λ^k.*
- *If A is invertible then v is an eigenvector of A^{-1} with eigenvalue λ^{-1}.*
- *If $p(x)$ is a polynomial then the matrix $p(A)$ has v as an eigenvector with eigenvalue $p(\lambda)$.*
- *Furthermore, the number λ is an eigenvalue of A if and only if it is a root of the characteristic polynomial $p(\lambda) = |\lambda I - A|$.*

With these preliminaries, we are now ready to express the relation between the eigenvalues of a matrix and its trace.

Theorem 3. *If A is an $n \times n$ matrix and $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the roots of the characteristic polynomial $p(\lambda) = |\lambda I - A|$, then $\operatorname{tr}(A) = \sum_{k=1}^{n} \lambda_k$, that is: the trace of a matrix equals the sum of its eigenvalues, if we account for the multiplicity of eigenvalues. [RB00]*

Proof. The characteristic polynomial of A can be factorized $p(\lambda) = \prod_{k=1}^{n} (\lambda - \lambda_k)$ so the λ^{n-1}-coefficient is $-\sum_{k=1}^{n} \lambda_k$. On the other hand in the expansion of

$$|\lambda I - A| = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & \lambda - a_{nn} \end{vmatrix}$$

the only term containing λ^{n-1} is the product of entries along the main diagonal $\prod_{k=1}^{n}(\lambda - a_{kk})$, so that the λ^{n-1} -coefficient is $-\sum_{k=1}^{n}(A)_{kk}$. □

The following corollary brings out what in Theorem 3 is essential in the study of closed walks.

Corollary 3.1. *If G is a graph with adjacency matrix A with eigenvalues $\lambda_1, \dots, \lambda_n$ then the number of closed walks of length m in G is equal to*

$$\mathrm{tr}\,(A^m) = \sum_{k=1}^{n} \lambda_k^m.$$

Corollary 3.1, while important, suffers from the fact that it is not always possible to find the eigenvalues of a matrix. Also it gives us very little combinatorial information on the closed walks of a graph, except for enumerating them. However, it should be noted that it can be used in the other direction. That is, since the spectrum of a graph is in some way related to virtually every graph invariant and since the eigenvalues are often difficult to find or even approximate algebraically, combinatorial methods counting closed walks can in fact be used to obtain knowledge of the spectral properties of the graph. In fact much research on closed walks in graphs is motivated by its value in approximating eigenvalues. For an article developing this point of view, see for instance [DK13].

2.2. **Basic combinatorics.** The reader is assumed to be familiar with permutations, the binomial and mulinomial coefficients and their most common combinatorial interpretations. All these concepts are covered in depth in chapter one of [Sta12]. There are many textbooks giving a lot more gentle introductions than Stanley, for instance [Big02].

Definition 7. A word w of length m in the alphabet S is a sequence $a_1, a_2, \dots, a_m$ with elements $a_i \in S$, where S is some set. The set of all such words of length m is S_m. The elements of such a sequence are called letters. A subword of a word $w = a_1, a_2, \dots, a_m$ is a word $a_k, a_{k+1}, \dots, a_{k+n}$ with $1 \leq k \leq k+n \leq m$. Two words $w_a = a_1, a_2, \dots, a_m$ and $w_b = b_1, b_2, \dots, b_n$ in the same alphabet can be concatenated into a new word $w_a w_b = a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n$. If $w_a = w_b$ then this concatenation can be written w_a^2 and so on, if there are more than two words concatenated.

A word w of length m in alphabet $S = \{s_1, s_2, \dots, s_n\}$ is said to have the content $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ if the letter s_i occurs α_i times in w. The vector α is obviously a weak composition of m into n non-negative components. In this paper a composition will always refer to a weak composition. If α is some composition of m, or some set of compositions of m, then S_α denotes the set of all words in S_m with content α, or content in α. The set of all compositions of m into n components is denoted $\alpha_{m,n}$. Finally, given two alphabet of the same size $S = \{s_1, s_2, \dots, s_n\}$

and $T = \{t_1, t_2, \ldots, t_n\}$, a translation is a function taking a word w in S into a word w' in T by exchanging the i:th symbol of A with the i:th symbol of B, so that both words have the same content in their respective alphabets.

Example 4. Example: The word *ababab* can be written $(ab)^3$. It has content $\alpha = (3,3)$ in the alphabet $S = \{a,b\}$ but content $\beta = (3,3,0)$ in the alphabet $S' = \{a,b,c\}$. The set S_α consists of all words composed out of 3 a:s and 3 b:s. If we translate the word *ababab* into the alphabet $\{c,d\}$ we obtain a new word $(cd)^3$.

Of course, the number of words of length m from a particular alphabet S with content $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is simply

$$\binom{m}{\alpha_1, \alpha_2, \ldots, \alpha_n}.$$

This follows immediately from the fact that the multinomial coefficients counts the number of permutations of a multi-set, since a word with content α can be seen precisely as a permutation of the multi-set containing s_i α_i times. In this manner a word $w = a_1, a_2, \ldots, a_m$ can be seen as a function ϕ defined by $\phi(i) = a_i$. The word is then the word form of the function. Understood in this way, the one-line form of a permutation can be seen as its word form. For a given composition α, we will write the multinomial coefficient simply as

$$\binom{m}{\alpha}.$$

Definition 8. Given a set X of combinatorial objects a combinatorial statistic is a function $\sigma : X \to \mathbb{N}$. The generating polynomial F of σ is defined by

$$F(q) = \sum_{s \in X} q^{\sigma(s)}.$$

Observe in particular that $F(1) = |X|$ so that knowing the generating function for a statistic on some set immediately gives an enumeration of that set. If the statistic in question is combinatorially interesting, then the generating function of that statistic can be seen as a refinement of the enumeration: not only do we know how many elements there are in X but also how many such that $\sigma(x) = 0$, how many such that $\sigma(x) = 1$ and so on. To illustrate these ideas we might consider one specific statistic although we must postpone for a little while the question of its generating polynomial.

Definition 9. Let ϕ be a function from $M = \{1, 2, \ldots, m\}$ to some set of integers S. For $i \in M$ define the number of inversions of i to be the number of elements of M such that $i > j$ and $\phi(i) < \phi(j)$. Hence, the number of inversions of i is the number of letters larger than $\phi(i)$ among the first $i-1$ letters of the word form of ϕ. Let k_i be the number of inversions of i. The sum

$$\sum_{i=1}^{m} k_i$$

then defines a combinatorial statistic on the set of functions of $M \to S$, and by extension on S_m, the inversion statistic. For a word $w \in S_m$ we denote this $\mathrm{inv}(w)$. The vector $(k_1, k_2, \ldots, k_m)$ is called the inversion table of the function.

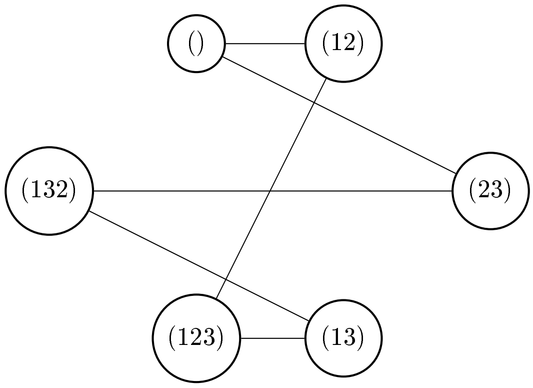

Figure 2: A Cayley graph of S_3

Example 5. The word $w = 150721$ is the word form of the function defined by $\phi(1) = 1, \phi(2) = 5, \phi(3) = 0, \phi(4) = 7, \phi(5) = 2, \phi(6) = 1$. Its inversion table is $(0, 0, 2, 0, 2, 3)$ and $\mathrm{inv}(w) = 7$.

Of course a word whose letters form a non-decreasing series has inversion statistic 0, so that the inversion statistic can be understood as how far the letters of a word are from being ordered according to, increasing, size.

2.3. **Basic algebra.** It is assumed that the reader knows the basics of finite group theory, at least to the extent of being familiar with groups, generating sets of a group, some properties of cyclic groups and direct products of groups, otherwise chapter one and two of [DF04] covers this.

We begin by defining and describing some of the basic properties of Cayley graphs.

Definition 10. Let G be a finite group with identity 1 and let S be a set generating G such that $x \in S \implies x^{-1} \in S$ and such that $1 \notin S$. Then the graph $\Gamma = (V, E)$ with $V = G$ and E defined by $\{g, h\} \in E \iff g^{-1}h \in S$ is called the Cayley graph of G with respect to S.

Example 6. Let $G = S_3$ and $S = \{(12), (23)\}$. Then the Cayley graph Γ of G with respect to S is presented in Figure 2.

Theorem 4. *A Cayley graph $\Gamma = (G, S)$ is a loop-free, undirected, connected and regular graph. [Löh17]*

Proof. Suppose $\{g, g\} \in E$. Then it would follow that $g^{-1}g = 1 \in S$, which is false by the definition of S. So Γ is loop-free. Now suppose $g^{-1}h \in S$. Then $\left(g^{-1}h\right)^{-1} = h^{-1}g \in S$. So there is an edge from vertex g to vertex h if and only if there is an edge from h to g. So Γ is undirected. Furthermore, since S generates G, given $g, h \in G$, $g^{-1}h$ can be written as the product of elements of S, as $s_1 s_2 \dots s_k$ for $s_i \in S$. Then starting at vertex g there is an edge to gs_1 and then from gs_1 to $gs_1 s_2$ and so on, all the way to $gs_1 s_2 \dots s_k = gg^{-1}h = h$. So, there is a walk between arbitrary nodes g, h, so Γ is connected. Finally, for any $g \in G$, the equation $g^{-1}x = s$ has precisely one solution, $x = gs$, for every $s \in S$, so every vertex in Γ has as many edges as there are elements in S. Thus, Γ is regular. $\square$

Observe that the finiteness of the group G is not really necessary to ensure that the Cayley graph has the desirable properties expressed in the theorem, however an infinite group will obviously occasion an infinite graph. The following simple observation will be quite useful in the following.

Theorem 5. *The adjacency matrix of a Cayley graph can be expressed as the sum of a number of permutation matrices.*

Proof. Given a Cayley graph $\Gamma = (G,S)$ with $G = \{g_1, g_2, \dots, g_n\}$ and $S = \{s_1, s_2, \dots, s_k\}$ we define k permutations $\pi_i : G \to G$ by $\pi_i(g_j) = g_j s_i$. Now let P_i be the permutation matrix corresponding to π_i, that is, let P_i be the matrix defined by:

$$(P_i)_{jk} = \begin{cases} 1 & \pi(g_j) = g_j s_i = g_k \\ 0 & \text{otherwise} \end{cases}.$$

Now consider the matrix

$$A = \sum_{i=1}^{k} P_i.$$

The j,k-th entry of A is then $|s_i \in S : g_j s_i = g_k|$. But this is 1 if $g_j^{-1} g_k \in S$ and 0 if not, so A is in fact the adjacency matrix of Γ. □

Example 7. Consider again the graph in Example 6. Its adjacency matrix, with rows and columns 1 to 6 corresponding to $(), (12), (23), (13), (123), (132)$, can be written

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

where the two matrices on the right hand side are the permutation matrices corresponding to the permutations $G \to G$ given by $\pi_1(g) = g \circ (12)$ and $\pi_2(g) = g \circ (23)$.

As the proof of connectivity in Theorem 4 suggests there is a natural bijection between walks starting in a particular vertex of a Cayley graph and words in the alphabet $\{s_1, s_2, \dots, s_k\}$.

Theorem 6. *There are as many walks in the Cayley graph $\Gamma = (G,S)$ of length m beginning in a particular vertex $g_0 \in G$ as there are words of length m in the alphabet $S = \{s_1, s_2, \dots, s_k\}$. [Cio06]*

Proof. Given a walk $g_0, g_1, \dots, g_{m+1}$ in Γ, it follows that $g_i^{-1} g_{i+1} \in S$ for $0 \le i \le m$, so the sequence $g_0^{-1} g_1, g_1^{-1} g_2, \dots, g_m^{-1} g_{m+1} \in S_m$. Now suppose $g_0, h_1, \dots, h_{m+1}$ is another walk inducing a word $w' = g_0^{-1} h_1, h_1^{-1} h_2, \dots, h_m^{-1} h_{m+1}$. Then $w = w'$ if and only if $g_i = h_i$ for every $i, 1 \le i \le m+1$. On the other hand, given a word $a_1, a_2, \dots, a_m \in S_m$ we can define a corresponding walk in Γ by $g_0, g_0 a_1, g_0 a_1 a_2, \dots, g_0 a_1 a_2 \dots a_m$. Now, a second such word $b_1, b_2, \dots, b_m$ would induce a walk $g_0, g_0 b_1, g_0 b_1 b_2, \dots, g_0 b_1 b_2 \dots b_m$ and these walks would be identical if and only if if $a_i = b_i$ for every $i, 1 \le i \le m$. So such a mapping from words to walks is a bijection. □

Example 8. Consider again the graph Γ in Figure 2. There are four words of length two in the alphabet $\{(12),(23)\}$, namely $(12)(12),(12)(23),(23)(12),(23)(23)$. These four words correspond to four walks beginning in $()$, namely the walks $(),(12),()$ and $(),(12),(123)$ and $(),(23),(132)$ and $(),(23),()$ respectively.

The following corollary summarizes some properties of walks in Cayley graphs that became evident in the proof of the Theorem 6.

Corollary 6.1. *Given a Cayley graph $\Gamma = (G,S)$ the number of closed walks of length m beginning and ending in a particular vertex $g_0 \in G$ is equal to the number of words in S_m such that the product of letters is the identity in G. From this, it in turn follows that the number of closed walks of length m in Γ beginning and ending in a particular vertex is the same for all vertices. Because of this second fact, we will always restrict our attention to closed walks beginning and ending in the identity element of G. Crucially, it also follows that if G is abelian, content alone determines closedness, so that the order of letters in a word is irrelevant for determining whether the corresponding walk is closed. The set of such closed walks of length m is denoted $C_{\Gamma,m}$. The corresponding set of words is denoted S^c_m. Since if G is abelian, the product of the letters in a word w in the alphabet S is the same for all words with the same content α, we refer to this product as $S\alpha$.*

Finally we review the concept of a group action.

Definition 11. If G is a group and X is a set, a group action of G on X is a function $G \times X \to X$ such that:

- $1 \times x = x$ for all $x \in X$,
- $g \times (h \times x) = (gh) \times x$ for all $g, h \in G$ and all $x \in X$.

For every element $x \in X$ we define the stabilizer of x as the subgroup $G_x \leq G$ such that $g \in G_x \iff g \times x = x$. If we define a relation R on $X \times X$ by xRy if $g \times x = y$ for some $g \in G$, then the equivalence classes of R are said to be the orbits of the group action, and the orbit of an element $x \in X$ is the equivalence class to which it belongs under R and is denoted O_x. The fixed point set of an element of $g \in G$ is the subset X_g of X such that $x \in X_g \iff g \times x = x$.

In this paper the group G acting on X will always be a cyclic group. In fact mostly one particular group action will be studied.

Definition 12. Given a word $w \in S_m$, we define a cyclic shift of w by k steps, where $0 \leq k < m$, in the following manner. If the letters of w are $w = a_1, a_2, \ldots, a_m$, then define the subword $w_1 = a_1, a_2, \ldots, a_{m-k}$ and $w_2 = a_{m-k+1}, a_{m-k+2}, \ldots, a_m$, so that $w = w_1 w_2$. The cyclic shift of w by k steps is then $w_2 w_1$. Alternatively, we can define the cyclic shift of a word by k steps as a function taking a word w of length m in the alphabet A to another word w' of length m in the same alphabet A, such that the letter in position i in w is in position $i + k \mod m$ in w'. This second definition is preferable, since it makes unnecessary the restriction that $0 \leq k < m$. Also, the second definition makes it quite obvious that cyclic shift defines a group action by $\mathbb{Z}_m$ on the set A_m.

It should be noted, that by the bijection between walks in the Cayley graph $\Gamma = (G,S)$ and words in the alphabet S, the cyclic shift action can be viewed as an action on the set of walks in Γ as well as on words in S.

Example 9. Consider words of length 4 in the alphabet $\{0,1\}$. Under the action of $\mathbb{Z}_4$ the 16 such words are divided into the following orbits $\{0000\}, \{1111\}, \{1010, 0101\}$, $\{0011, 1001, 1100, 0110\}, \{1110, 0111, 1011, 1101\}, \{0001, 1000, 0100, 0010\}$. The words in the one-element orbits have all of $\mathbb{Z}_4$ as stabilizer, the words in the two-element orbit have $\{0,2\}$ as stabilizer and the words in the four-element orbits have $\{0\}$ as stabilizer. Conversely, the fixed point set of 0 contains all 16 words, the fixed point set of 1 and 3 contain only the two mono-syllabic words $\{0000, 1111\}$ and the fixed point set of 2 contains the four words $\{0000, 1111, 1010, 0101\}$. Observe how the fixed point set of $g \in \mathbb{Z}_4$ contain all the words of length $\gcd(g,4)$ in the alphabet $\{0,1\}$, repeated $4/\gcd(g,4)$ times.

2.4. **q-Analogues.** A q-analogue is a mathematical theorem, identity or expression parametrized by a quantity q that generalizes a known expression and reduces to the known expression in the limit $q \to 1$. Given an enumeration of a set of combinatorial objects, a q -analogue of this enumeration evaluates to the cardinality of the set as $q \to 1$, so that the q-analogue is sometimes a generating function of some statistic on the set. Later on, we will see that q-analogues play an essential role in the cyclic sieving phenomenon. We define some classic q-analogues that will serve as generating polynomials in this paper.

Definition 13. We define the following polynomials:

- If $n \in \mathbb{N}$, the q-analogue of n is defined by $[0]_q = 0$ and $[n]_q = 1 + q + q^2 + \ldots + q^{n-1}$ for $n > 0$.
- If $n \in \mathbb{N}$, the q-analogue of $n!$ is defined by $[0]!_q = 1$ and $[n]!_q = \prod_{k=1}^{n} [k]_q$.
- If $n, k \in \mathbb{N}$ and $k \leq n$ then the q-analogue of $\binom{n}{k}$ is
$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]!_q}{[n-k]!_q [k]!_q}$$
.
- If $n \in \mathbb{N}$ and $\alpha \in \alpha_{n,m}$ then the q-analogue of $\binom{n}{\alpha}$ is
$$\begin{bmatrix} n \\ \alpha \end{bmatrix}_q = \frac{[n]!_q}{\prod_{i=1}^{m} [\alpha_i]!_q}.$$

Example 10. We have $[1]_q = 1, [2]_q = 1+q, [3]_q = 1+q+q^2, [4]_q = 1+q+q^2+q^3$. It then follows $[1]!_q = 1, [2]!_q = 1(1+q), [3]!_q = 1(1+q)(1+q+q^2), [4]!_q = 1(1+q)(1+q+q^2)(1+q+q^2+q^3)$. In turn we then get for instance
$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{[4]!_q}{[2]!_q [2]!_q} = \frac{[1]_q [2]_q [3]_q [4]_q}{[1]_q [2]_q [1]_q [2]_q} = \frac{[3]_q [4]_q}{[1]_q [2]_q} =$$
$$\frac{(1+q+q^2)(1+q+q^2+q^3)}{1+q} = (1+q+q^2)(1+q^2).$$

Now we have the means necessary for a discussion of the generating polynomial for the inversion statistic on the set of n-element permutations.

Theorem 7. *The q-factorial $[n]!_q$ is a generating polynomial for the inversion statistic on the set of permutation $S_n : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. [Sta12]*

Proof. We show this by induction over n. For $n = 1$ there is only one element in S_1, the function taking 1 to itself, and it has inversion statistic 0, so the generating polynomial for the inversion statistic on S_1 is $1 = [1]!_q$. Suppose that the generating polynomial for the inversion statistic on S_N is $[N]!_q$. Now define the $N+1$ sets

$S_{N+1,i} = \{\pi \in S_{N+1} : \pi(N+1) = i\}$. Obviously, each $S_{N+1,i}$ has $N!$ elements and we define a bijection $\pi \in S_{N+1,i} \to \psi \in S_N$ in the following manner: $\psi(j) = \pi(j)$ if $\pi(j) < i$ and $\psi(j) = \pi(j) - 1$ if $\pi(j) > i$.

How does the inversion statistic of π, $\mathrm{inv}(\pi)$, relate to that of ψ, $\mathrm{inv}(\psi)$? Suppose that $j \neq N+1$ and that k is an inversion of j in π, that is: suppose that $j > k$, which implies $k \neq N+1$, and that $\pi(j) < \pi(k)$. Then it follows that $\psi(j) < \psi(k)$ as well, so that k is an inversion of j in ψ as well. Obviously the same is true in the other direction. Thus, if the inversion table of π is $(k_1, k_2, \dots, k_N, k_{N+1})$, then the inversion table of ψ is $(k_1, k_2, \dots, k_N)$. It follows that $\mathrm{inv}(\psi) + k_{N+1} = \mathrm{inv}(\pi)$. But k_{N+1} is the number of elements $k \in \{1, 2, \dots, N\}$ such that $N+1 > k$ and $\pi(N+1) < \pi(k)$. But $N+1 > k$ is true for all $k \in \{1, 2, \dots, N\}$, so k_{N+1} is just the number of elements $k \in \{1, 2, \dots, N\}$ such that $i = \pi(N+1) < \pi(k)$, which is $N+1-i$. Now, we consider the generating polynomial of the inversion statistic on S_{N+1} :

$$F(q) = \sum_{\pi \in S_{N+1}} q^{\mathrm{inv}(\pi)} = \sum_{i=1}^{N+1} \sum_{\pi \in S_{N+1,i}} q^{\mathrm{inv}(\pi)} =$$
$$\sum_{i=1}^{N+1} \sum_{\psi \in S_N} q^{\mathrm{inv}(\psi)+N+1-i} = \sum_{i=1}^{N+1} q^{N+1-i} \sum_{\psi \in S_N} q^{\mathrm{inv}(\psi)} =$$
$$\sum_{i=1}^{N+1} q^{N+1-i} [N]!_q = [N]!_q \sum_{i=1}^{N+1} q^{N+1-i} = [N]!_q [N+1]_q = [N+1]!_q,$$

which finishes the proof by induction. □

Example 11. Consider $[3]!_q = 1(1+q)(1+q+q^2) = 1 + 2q + 2q^2 + q^3$. On the other hand consider the 6 permutation $\{1,2,3\} \to \{1,2,3\}$. For these we have $\mathrm{inv}(123) = 0, \mathrm{inv}(132) = 1, \mathrm{inv}(213) = 1, \mathrm{inv}(231) = 2, \mathrm{inv}(312) = 2$ and $\mathrm{inv}(321) = 3$. From this we see that, indeed, $[3]!_q$ is the generating polynomial for the inversion statistic on S_3.

It's not immediately evident that the q-binomial and q-multinomial coefficients have natural coefficients, in fact it is not even obvious that they are polynomials. The following recurrence relations, q-analogues of Pascals identity, will help establish that they really are polynomials with natural coefficients, and so are suitable candidates for generating polynomials of combinatorial statistics.

Theorem 8 (q-Pascal identities)**.** *The q-binomial coefficients, with $k > 0$ satisfy the two following recursions:*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q, \tag{1}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q, \tag{2}$$

[Sta12]

Proof. This is purely algebraic manipulation:

$$q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q = q^k \frac{[n-1]!_q}{[k]!_q[n-k-1]!_q} + \frac{[n-1]!_q}{[k-1]!_q[n-k]!_q} =$$
$$\frac{[n-1]!_q}{[k-1]!_q[n-k-1]!_q}\left(\frac{q^k}{[k]_q} + \frac{1}{[n-k]_q}\right) = \frac{[n-1]!_q}{[k-1]!_q[n-k-1]!_q}\left(\frac{q^k[n-k]_q + [k]_q}{[n-k]_q[k]_q}\right) =$$
$$\frac{[n-1]!_q}{[k]!_q[n-k]!_q}\left(q^k[n-k]_q + [k]_q\right) = \frac{[n-1]!_q}{[k]!_q[n-k]!_q}[n]_q = \frac{[n]!_q}{[k]!_q[n-k]!_q} = \begin{bmatrix} n \\ k \end{bmatrix}_q,$$

which proves (1) . (2) is similar:

$$\begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q = \frac{[n-1]!_q}{[k]!_q[n-k-1]!_q} + q^{n-k}\frac{[n-1]!_q}{[k-1]!_q[n-k]!_q} =$$
$$\frac{[n-1]!_q}{[k-1]!_q[n-k-1]!_q}\left(\frac{1}{[k]_q} + \frac{q^{n-k}}{[n-k]_q}\right) = \frac{[n-1]!_q}{[k-1]!_q[n-k-1]!_q}\left(\frac{[n-k]_q + q^{n-k}[k]_q}{[n-k]_q[k]_q}\right) =$$
$$\frac{[n-1]!_q}{[k]!_q[n-k]!_q}\left([n-k]_q + q^{n-k}[k]_q\right) = \frac{[n-1]!_q}{[k]!_q[n-k]!_q}[n]_q = \frac{[n]!_q}{[k]!_q[n-k]!_q} = \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

□

With the help of these recursions, we can now prove the following.

Theorem 9. *The q-binomial and q-multinomial coefficients are polynomials in* $\mathbb{N}[q]$*. [Sta12]*

Proof. We first prove by induction over n that the q-binomial coefficient is a polynomial in $\mathbb{N}[q]$. As induction base we have $\begin{bmatrix} 0 \\ 0 \end{bmatrix}_q = 1$, $\begin{bmatrix} 1 \\ 0 \end{bmatrix}_q = 1$, $\begin{bmatrix} 1 \\ 1 \end{bmatrix}_q = 1$. Now as induction hypothesis, suppose that for $n = N$, all q-binomial coefficients $\begin{bmatrix} N \\ k \end{bmatrix}_q$ are polynomials in $\mathbb{N}[q]$. Then for the q-binomial coefficients $\begin{bmatrix} N+1 \\ k \end{bmatrix}_q$ we have two cases. If $k = 0$, then $\begin{bmatrix} N+1 \\ k \end{bmatrix}_q = 1$. If $k > 0$ then by either of the Pascal-analogue recursions together with the induction hypothesis, it follows that $\begin{bmatrix} N+1 \\ k \end{bmatrix}_q$ is a sum of two polynomials in $\mathbb{N}[q]$, so is a polynomial in $\mathbb{N}[q]$. Thus, it follows by induction that the q-binomial coefficients are polynomials in $\mathbb{N}[q]$.

Now, for the q-multinomial coefficient $\begin{bmatrix} n \\ k_1, k_2, \ldots, k_m \end{bmatrix}_q$ we use induction over m. For $m = 1$ we have $\begin{bmatrix} n \\ k_1 \end{bmatrix}_q = 1$ and for $m = 2$ the q-multinomial coefficient is just a q-binomial coefficient. Now suppose that for $m = M$ every q-multinomial coefficient $\begin{bmatrix} n \\ k_1, k_2, \ldots, k_M \end{bmatrix}_q$ is a polynomial in $\mathbb{N}[q]$. Now for a q-multinomial coefficient with $m = M + 1$ we consider the following factorization:

$$\begin{bmatrix} n \\ k_1, k_2, \ldots, k_{M+1} \end{bmatrix}_q = \frac{[n]!_q}{\prod_{i=1}^{M+1}[k_i]!_q} =$$
$$\frac{[n-k_{M+1}]!_q}{\prod_{i=1}^{M}[k_i]!_q}\frac{[n]!_q}{[n-k_{M+1}]!_q[k_{M+1}]!_q} =$$
$$\begin{bmatrix} n-k_{M+1} \\ k_1, k_2, \ldots, k_M \end{bmatrix}_q \begin{bmatrix} n \\ k_{M+1} \end{bmatrix}_q.$$

From this factorization we see that a q-multinomial coefficient with $m = M + 1$ is the product of a q-multinomial coefficient with $m = M$, which by the induction hypothesis is a polynomial in $\mathbb{N}[q]$ and a q-binomial coefficient, which by what was proven above is a polynomial in $\mathbb{N}[q]$, so it is a polynomial in $\mathbb{N}[q]$. This completes the proof. □

The following theorem is the most important in this paper, to a certain extent all the results of this paper can be seen as applications of this theorem.

Theorem 10 (q-Lucas)**.** *Let $n = n_1 d + n_0$ and $k = k_1 d + k_0$, where $0 \le n_0, k_0 < d$, where n, k are natural numbers and d is a positive integer. Furthermore, let $\xi = e^{2\pi i \frac{c}{d}}$ be a primitive d-th root of unity. Then*

$$\begin{bmatrix} n \\ k \end{bmatrix}_\xi = \binom{n_1}{k_1} \begin{bmatrix} n_0 \\ k_0 \end{bmatrix}_\xi ,$$

where the (q-)binomial coefficients are interpreted as 0 if the denominator is larger than the numerator.

We give no proof of this theorem here. Originally this was proven in [Oli65]. A nice proof based on cyclic sieving like methods was given in [Sag92]. These proofs demonstrate a somewhat more general statement and would be a distraction if given here. The weaker statement, which provides all that is needed in this paper, can in fact be proven with elementary methods, using induction and the q-Pascal analogues in a style similar to the previous proofs of this section but such a proof would be quite long and very tedious and so is omitted.

Example 12. We consider again the q-binomial coefficient

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$$

First let $d = 3$. Then $n_1 = 1, n_0 = 1$ and $k_1 = 0, k_0 = 2$.For $\xi = e^{c\frac{2\pi i}{3}}$ with $\gcd(c, 3) = 1$, q-Lucas gives us:

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_\xi = \binom{1}{0} \begin{bmatrix} 0 \\ 2 \end{bmatrix}_\xi = 0,$$

and indeed, $\left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right]_q = (1 + q + q^2)(1 + q^2)$ has $\xi = e^{c\frac{2\pi i}{3}}$ with $\gcd(c, 3) = 1$ for roots, since for $q \neq 1$ we have $(1 + q + q^2) = \frac{q^3-1}{q-1}$.

Now, let $d = 2$. Then $n_1 = 2, n_0 = 0$ and $k_1 = 1, k_0 = 0$.For odd integers c, we then have $\xi = e^{c\frac{2\pi i}{2}} = -1$, and q-Lucas gives us:

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_\xi = \binom{2}{1} \begin{bmatrix} 0 \\ 0 \end{bmatrix}_\xi = 2,$$

and again, $\left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right]_q = (1 + q + q^2)(1 + q^2)$ evaluates to 2 when $q = -1$.

2.5. **Cyclic sieving.** Reiner, Stanton and White first introduced the cyclic sieving phenomenon in their 2004 paper [RSW04]. It defines a relation between three mathematical objects. The first of these is a finite set, X. The second is a finite cyclic group, $C = \langle g \rangle$, which acts on X. The third is a polynomial in $\mathbb{N}[q]$, which will often be a generating polynomial of X. We now state the formal definition.

Definition 14. Let X be a set of combinatorial objects, $C = \langle g \rangle$ be a finite cyclic group of size n acting on X, and $f(q) \in \mathbb{N}[q]$. Then the triple $(X, C, f(q))$ is said to exhibit the cyclic sieving phenomenon if for all $d \in \mathbb{N}$, we have

$$\left|\{x \in X : g^d x = x\}\right| = f\left(e^{\left(2\pi i \frac{d}{n}\right)}\right)$$

In words, $f(q)$ evaluated at certain roots of unity gives the number of elements in X fixed by powers of g. Note that $f(1) = |X|$, so in many instances, $f(q)$ is a q-analogue of the set X.

At first sight this definition might seem quite strange. Why would one expect such triples to appear "naturally" except in trivial cases? Of course, given X and G, one could always find a polynomial satisfying the conditions of the definition, but it doesn't seem obvious that this polynomial should have natural numbers for coefficients. And it seems even less obvious that the polynomial would have some intuitive relation to X. Yet the growing literature on the cyclic sieving phenomenon indicates that there a great many such triples. For an overview of many results see [Ale20]. This might seem slightly less surprising if one considers that the roots of unity form a cyclic group themselves, and that g^d and $e^{2\pi i \frac{d}{n}}$ are elements of the same order in their respective groups, so that the cyclic sieving phenomenon expresses a relation between two isomorphic groups. Of course nothing better encourages understanding than an example.

Example 13. Let $N = \{1, 2, ..., n\}$ and let K be the set of k-element subsets of N. It is one of the most basic results of combinatorics that $|K| = \binom{n}{k}$, a natural q-analogue for which is $\begin{bmatrix} n \\ k \end{bmatrix}_q$. Now we consider the following action of $\mathbb{Z}_n$ on K. For any $g \in \mathbb{Z}_n$ and any $M = \{a_1, a_2, \ldots, a_k\} \in K$, we define

$$g + M = \{a_1 + g \mod n, a_2 + g \mod n, \ldots, a_k + g \mod n\}.$$

Now suppose that $M \in K$ is fixed under the action of $g \in G$ and that $a \in M$. Then M must also contain $a + g, a + 2g, \ldots$, so it follows that is must contain the entire congruence class of a modulo $d = \gcd(n, g)$. From this it in turn follows that if M is fixed by the action of g then M must be the union of congruence classes modulo d. Since every such class is of size $\frac{n}{d}$ and M is a k-element set it follows that $\frac{n}{d} | k$. So if, $\frac{n}{d} \not| k$, no elements in K are fixed by the action of g. On the other hand, if $\frac{n}{d} | k$, M will be fixed by the action of g if and only if it is a union of congruence classes modulo d. Since there are d such classes, the number of elements in K fixed by the action g is equal to the number of ways of constructing a k-element set as a union of kd/n congruence classes out of d different choices, so we have

$$\binom{d}{kd/n} = |K_g|.$$

Now, to show cycling sieving, we need to evaluate the polynomial $\begin{bmatrix} n \\ k \end{bmatrix}_q$ at roots of unity. Thus, we let $\xi = e^{\left(2\pi i \frac{g}{n}\right)}$ and consider $\begin{bmatrix} n \\ k \end{bmatrix}_\xi$. We have that $\xi = e^{\left(2\pi i \frac{g/d}{n/d}\right)}$ where $\gcd(g/d, n/d) = 1$ so ξ is a primitive n/d-th root of unity. Setting $n = d\frac{n}{d} + 0$ and $k = k_1 \frac{n}{d} + k_0$ we get from q-Lucas theorem that

$$\begin{bmatrix} n \\ k \end{bmatrix}_\xi = \binom{d}{k_1} \begin{bmatrix} 0 \\ k_0 \end{bmatrix}_\xi.$$

Now unless $k_0 = 0$, that is : unless $\frac{n}{d}|k$, this evaluates to zero. On the other hand, if $k_0 = 0$ then it evaluates to

$$\binom{d}{k_1}$$

where $k_1 = kd/n$. In fact then, the cardinality of the fixed point set under the action of g is equal to the value of q-analogue of the enumeration at $\xi = e^{\left(2\pi i \frac{g}{n}\right)}$. This proves that the triple $(K, \mathbb{Z}_n, \begin{bmatrix} n \\ k \end{bmatrix}_q)$ is an instance of the cyclic sieving phenomenon.

The method used in Example 13 is typical of how cyclic sieving will be proved in this paper. First, through some combinatorial argument determine the size of the fixed point sets. Then through algebraic argument evaluate the q-analogue. In this paper, the algebraic argument always involves q-Lucas theorem, although there are many similar identities that can be exploited, see for instance [FH11]. In more advanced research, cyclic sieving is sometimes shown with the methods of representation theory. For an introduction to this paradigm of proving cyclic sieving, see [Sag11]. The reasons that such avenues are not explored in this paper lie entirely in the ignorance of its author.

Finally, we state one particular instance of cyclic sieving, which was shown, in a somewhat different form, already in [RSW04].

Theorem 11. *Let W_α be all words of length m with content α in some alphabet. Suppose $\mathbb{Z}_m$ act on W_α by cyclic shift. Then the triple*

$$\left(W_\alpha, \mathbb{Z}_m, \begin{bmatrix} m \\ \alpha \end{bmatrix}_q\right)$$

exhibit the cyclic sieving phenomenon and the polynomial $\begin{bmatrix} m \\ \alpha \end{bmatrix}_q$ is the generating polynomial of the inversion statistic on W_α.

We do not prove this theorem here, nor will we ever immediately apply it, because all of section 3.1 and section 3.2 can be seen as

- a proof of Theorem 11,
- a slight generalization of it to sets of compositions of m,
- most importantly, an application of it to walks in Cayley graphs interpreted as words.

One could say that Theorem 11 is the key to why the interpretation of walks as words is so fruitful for proving cyclic sieving on closed walks in abelian Cayley graphs.

3. Results

3.1. Closed walks in cycle graphs.

In this subsection we will be studying closed walks in cycle graphs. We will show that they are a certain kind of Cayley graphs, enumerate the number of closed walks of length m, describe and determine the size of the fixed point sets under the cyclic shift action, prove cyclic sieving and show that the q-analogue of the enumeration is the generating polynomial of the inversion statistic.

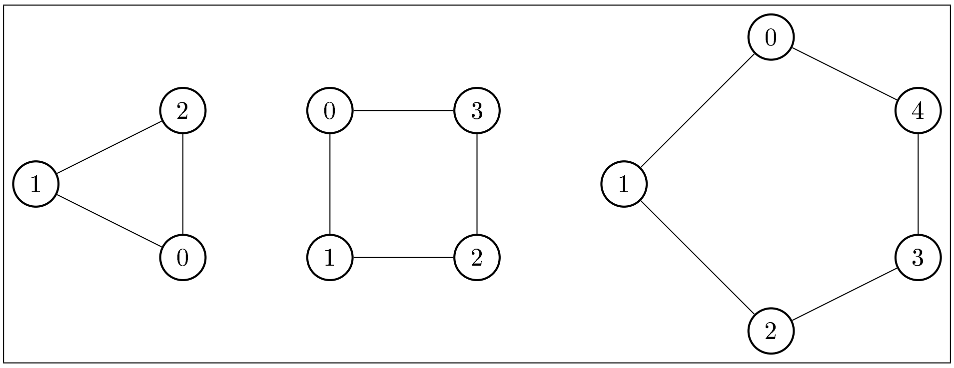

Figure 3: The cycle graphs C_3, C_4 and C_5.

Definition 15. The cycle graph of order n, C_n, is the graph $G = (V, E)$ with $V = \{0, 1, \ldots, n-1\}$ and with edges $\{(0,1), (1,2), (2,3), \ldots (n-2, n-1), (n-1, 0)\}$, that is: $\{i, j\} \in E$ if and only if $i - j \equiv \pm 1 \mod n$.

Example 14. Figure 3 shows a few example of cycle graphs.

We show that cycle graphs are Cayley graphs.

Proposition 12. *C_n is the Cayley graph $\Gamma_n = (\mathbb{Z}_n, S = \{1, -1\})$ and its adjacency matrix can be written $A = P + P^{-1}$ where P is the permutation matrix of the cyclic permutation $(12 \ldots n)$.*

Proof. Obviously C_n and Γ_n have the same number of vertices, namely n. Furthermore ij is an edge in Γ_n if and only if $j - i \in \{1, -1\}$ which is exactly when ij is an edge in C_n. Now that we have established that C_n is a Cayley graph it follows from Theorem 5 that its adjacency matrix A can be expressed as the sum $P_1 + P_2$ where P_1, P_2 are the permutation matrices corresponding to the permutations $\pi_1(i) = i + 1 \mod n$ and $\pi_2(i) = i - 1 \mod n$ but these are precisely the permutation $(123 \ldots n)$ and its inverse. □

Proposition 13. *The number of closed walks of length m in $\Gamma = (\mathbb{Z}_n, \{1, -1\})$ beginning and ending in vertex 0 is*

$$|C_{\Gamma,m}| = \sum_{\substack{\alpha \in \alpha_{m,2}: \\ n | S\alpha}} \binom{m}{\alpha}.$$

[DK13]

Proof. We prove this in two different ways. First, we have $|C_{\Gamma,m}| = (A^m)_{1,1}$ by Theorem 1. Now, since the matrices P, P^{-1} commute we have

$$A^m = (P + P^{-1})^m = \sum_{k=0}^{m} \binom{m}{k} P^{-k} P^{m-k} = \sum_{k=0}^{m} \binom{m}{k} P^{m-2k}.$$

Now $\left(P^i\right)_{11} = 0$ except if $n|i$ when $P^{nk} = I$ and $I_{11} = 1$. So we have

$$(A^m)_{11} = \left(\sum_{k=0}^{m} \binom{m}{k} P^{m-2k} \right)_{11} = \sum_{\substack{0 \le k \le m: \\ n | m-2k}} \binom{m}{m-k, k},$$

and the proposition follows.

Now consider again $C_{\Gamma,m}$. Let S_m^c be the set of corresponding words in the alphabet $S = \{1, -1\}$. Geometrically a 1 can be interpreted as a step in clockwise direction, while a -1 can be interpreted as a step in anti-clockwise direction. If a word $w \in S_m^c$ has content $\alpha = (m-k, k)$ then the condition that w corresponds to a closed walk is equivalent to $n|S\alpha$ and for each such k there are precisely $\binom{m}{k}$ words with content $(m-k, k)$ in S_m. □

Example 15. Consider closed walks of length 8 in C_3. From Proposition 13 we get that the number of such walks is

$$\sum_{\substack{0 \le k \le 8:\\ 3|8-2k}} \binom{8}{k}.$$

The k-values satisfying these conditions are $k \in \{1, 4, 7\}$, corresponding to walks that take one step in clockwise direction and seven in anti-clockwise, walks that take four of each and walks that take seven steps in clockwise direction and one in anti-clockwise. The total number of closed walks is thus

$$\binom{8}{1} + \binom{8}{4} + \binom{8}{7} = 8 + 70 + 8 = 86.$$

Now, let us describe the fixed point sets of the cyclic shift action on the set $C_{\Gamma,m}$.

Proposition 14. *For clarity, let $W = S_m^c$ and let $V = C_{\Gamma,m}$. Suppose that $\mathbb{Z}_m$ acts by cyclic shift on W, and thus by extension on V. Furthermore, for $g \in \mathbb{Z}_m$ let $d = \gcd(g, m)$. Then the cardinality of the fixed point set V_g is given by*

$$|V_g| = \sum_{\substack{\alpha \in \alpha_{d,2}:\\ n|\frac{m}{d}S\alpha}} \binom{d}{\alpha}.$$

Proof. A word $w \in W$ can be subdivided into m/d subwords each of length d, as $w = w_1 w_2 \dots w_{m/d}$. Now the action of g takes the letter of w in position i to position $i+g \bmod m$, so a subword w_j is taken to a subword w_k where $k = i + g/d \bmod m/d$. Suppose w_1 is mapped onto w_{i_1} which in turn is mapped onto w_{i_2} and so on. Because $\gcd(g/d, m/d) = 1$, such a series doesn't return to w_1 before having traversed all other subwords. So if w is fixed under the action of g then all subwords w_i must be identical, that is $w = w_1^{m/d}$. Now suppose w_1 has content α. Then w has content $\frac{m}{d}\alpha$ and, since $w \in W$, it follows that $n|\frac{m}{d}S\alpha$. On the other hand these criteria are sufficient, that is if w_1 is a word of length d with content α such that $n|\frac{m}{d}S\alpha$, then the word $w = w_1^{m/d}$ is fixed by the action of g and belongs to W. But for a particular α the number of such words is $\binom{d}{\alpha}$ so we have

$$|V_g| = |W_g| = \sum_{\substack{\alpha \in \alpha_{d,2}:\\ n|\frac{m}{d}S\alpha}} \binom{d}{\alpha}.$$

□

Example 16. We consider again the closed walks of length 8 in C_3, this time as words and under the action of Z_8 by cyclic shift. Every such word is obviously fixed by the action of 0 so the fixed point set of 0 contains all 86 closed walks. Words that are fixed by the action of 4 consist of two identical sub-words of length 4, and so must contain an even number of 1:s and an even number of -1:s. Hence, among words representing closed walks, only those with content $(4,4)$ could be fixed. Each subword would then have content $(2,2)$ and there are $\binom{4}{2}=6$ such words, namely $(1,1,-1,-1)^2,(1,-1,1,-1)^2,(-1,1,1,-1)^2,(1,-1,-1,1)^2,(-1,1,-1,1)^2$ and $(-1,-1,1,1)^2$. Words that are fixed by the action of 2 and 6 consist of four identical sub-words of length 2, and so the number of 1:s and -1:s must be divisible by four. Again, among words representing closed walks, only those with content $(4,4)$ could be fixed by the action of 2 or 6. Each subword would then have content $(1,1)$ and there are $\binom{2}{1}=2$ such words, namely $(1,-1)^4,(-1,1)^4$. Finally words that are fixed by the action of $1,3,5,7$ consist of 8 identical subwords each of length 1, that is: they are monosyllabic. However no such word represents a closed walk in C_3 so the fixed point sets of $1,3,5,7$ are empty.

Now, we return to the enumeration of $C_{\Gamma,m}$,

$$\sum_{\substack{\alpha\in\alpha_{m,2}:\\ n|S\alpha}}\binom{m}{\alpha}.$$

A natural q-analogue for this is

$$f_{n,m}(q)=\sum_{\substack{\alpha\in\alpha_{m,2}:\\ n|S\alpha}}\begin{bmatrix}m\\ \alpha\end{bmatrix}_q.$$

We are now ready to prove our first instance of the cyclic sieving phenomenon.

Theorem 15. *The triple $(C_{\Gamma,m},\mathbb{Z}_m,f_{n,m})$ exhibits the cyclic sieving phenomenon.*

Proof. To see this we need to evaluate

$$f_{n,m}\left(e^{2\pi i\frac{g}{m}}\right)$$

for $g\in\mathbb{Z}_m$. Now let $d=\gcd(g,m)$. Then $\xi=e^{2\pi i\frac{g}{m}}=e^{2\pi i\frac{g/d}{m/d}}$ with $\gcd(g/d,m/d)=1$, so ξ is a primitive m/d-th root of unity. We have $m=d\frac{m}{d}$ and for each $\alpha\in\alpha_{m,2}$ such that $\alpha=(\alpha_1,m-\alpha_1)$ we let $\alpha_1=k_1\frac{m}{d}+k_0, 0\le k_0<m/d$. Now we get from q-Lucas that:

$$f_{n,m}(\xi)=\sum_{\substack{\alpha\in\alpha_{m,2}:\\ n|S\alpha}}\begin{bmatrix}m\\ \alpha\end{bmatrix}_q=\sum_{\substack{0\le\alpha_1\le m:\\ n|2k_1\frac{m}{d}+2k_0-m}}\binom{d}{k_1}\times\begin{bmatrix}0\\ k_0\end{bmatrix}_\xi=\sum_{\substack{0\le\alpha_1\le m:\\ n|2k_1\frac{m}{d}-m}}\binom{d}{k_1}$$

where the last equality uses the fact that

$$\begin{bmatrix}0\\ k_0\end{bmatrix}_\xi=0$$

unless $k_0=0$, when it is 1. So in fact we have that the only relevant compositions α are those such that $\alpha_1=k_1\frac{m}{d}$, and there is precisely one such α for each $0\le k_1\le d$, so we can sum over compositions of d instead of over compositions of m:

$$f_{n,m}(\xi)=\sum_{\substack{0\le\alpha_1\le m:\\ n|2k_1\frac{m}{d}-m}}\binom{d}{k_1}=\sum_{\substack{\alpha\in\alpha_{d,2}:\\ n|\frac{m}{d}S\alpha}}\binom{d}{\alpha}$$

That is, the q-analogue

$$f_{n,m}(q) = \sum_{\substack{\alpha \in \alpha_{m,2}: \\ n \mid S\alpha}} \begin{bmatrix} m \\ \alpha \end{bmatrix}_q,$$

evaluated at $\xi = e^{\frac{2\pi i}{m} g}$ is equal to the cardinality of the fixed point set of g when Z_m acts on $C_{\Gamma,m}$ by cyclic shift, so that we here have an instance of the cyclic sieving phenomenon. □

Example 17. We consider again the closed walks of length 8 on C_3. We have already in Example 16 calculated the size of the fixed point sets and in Example 15 we found the enumeration

$$\binom{8}{1} + \binom{8}{4} + \binom{8}{7},$$

so our q-analogue is

$$f_{3,8}(q) = \begin{bmatrix} 8 \\ 1 \end{bmatrix}_q + \begin{bmatrix} 8 \\ 4 \end{bmatrix}_q + \begin{bmatrix} 8 \\ 7 \end{bmatrix}_q =$$

$$2\frac{q^8-1}{q-1} + \frac{q^7-1}{q-1}\frac{q^5-1}{q-1}(1-q+q^2)(1+q^4).$$

Evaluating this at $\xi = e^{2\pi i \frac{g}{m}}$ we get the following results. For $g = 0$ we of course have $f_{3,8}(1) = 86$. For odd g, $\xi^4 = -1$ and $f_{3,8}(\xi) = 0$. For $g = 2$ we have $\xi = i$ and $f_{3,8}(i) = 2$ and for $g = 6$ we have $\xi = -i$ and $f_{3,8}(-i) = 2$. Finally for $g = 4$ we have $\xi = -1$ and $f_{3,8}(-1) = 6$. This agrees with our conclusions in Example 16.

Now, it would be interesting if the polynomial

$$f_{n,m}(q) = \sum_{\substack{\alpha \in \alpha_{m,2}: \\ n \mid S\alpha}} \begin{bmatrix} m \\ \alpha \end{bmatrix}_q$$

turned out to be the generating polynomial of some statistic on the set $C_{\Gamma,m}$ or its associated set of words A_m^c. In fact, the inversion statistic works again. We first prove the following lemma.

Lemma 16. *Let $S = \{1, -1\}$ and $\alpha \in \alpha_{m,2}$. Then the generating polynomial of the inversion statistic on S_α is $\begin{bmatrix} m \\ \alpha \end{bmatrix}_q$. [Sta12]*

Proof. We prove this with induction over m. If $m = 1$ then for each α there is only one word in S_α, the words 1 and -1 respectively, each having inversion statistic 0, so in both cases the generating polynomial of the inversion statistic is $F(q) = 1 = \begin{bmatrix} 1 \\ \alpha \end{bmatrix}_q$. Now suppose that for $m = M$ the generating polynomial of the inversion statistic on S_α is $\begin{bmatrix} M \\ \alpha \end{bmatrix}_q$ for every α. Consider now S_α for $\alpha \in \alpha_{M+1,2}$ If $\alpha = (0, M+1)$ or $\alpha = (M+1, 0)$ we again have that S_α consists of only one monosyllabic word with inversions statistic 0 and so $F(q) = 1 = \begin{bmatrix} M+1 \\ \alpha \end{bmatrix}_q$. Now, for any other α we divide S_α into two subsets S_1 and S_{-1} where S_i consists of those words in S_α whose last letter is i. Given such a division, we have

$$F(q) = \sum_{w \in S_\alpha} q^{\mathrm{inv}(w)} = \sum_{w \in S_1} q^{\mathrm{inv}(w)} + \sum_{w \in S_{-1}} q^{\mathrm{inv}(w)}.$$

Now, consider an operation on the word w of length at least 2 and content $\alpha = (k, M+1-k)$ whereby we obtain a new word w' by deleting the last letter of w. Suppose that $i \neq M+1$ and that j is an inversion of i in w, that is, suppose that $i > j$, which implies $j \neq M+1$, and that $\phi(i) < \phi(j)$. Then j is an inversion of i in w' as well. Obviously the same is true in the other direction too. So if the inversion table of w is $(k_1, k_2, \dots, k_M, k_{M+1})$, then the inversion table of w' is $(k_1, k_2, \dots, k_M)$. So we have $\mathrm{inv}(w') + k_{M+1} = \mathrm{inv}(w)$. Now for words in S_1 the function $w \to w'$ defines a bijection from S_1 to $S_{(k-1,M+1-k)}$. Furthermore for words in S_1, $k_{M+1} = 0$ since $\phi(M+1) = 1$, and so $\mathrm{inv}(w') = \mathrm{inv}(w)$. On the other hand, for words in S_{-1} the function $w \to w'$ defines a bijection from S_{-1} to $S_{(k,M-k)}$. Finally, for words in S_{-1}, $k_{M+1} = k$ since $\phi(M+1) = -1$ and there are k ones in w, and so $\mathrm{inv}(w') + k = \mathrm{inv}(w)$. So we have

$$F(q) = \sum_{w \in S_{(k,M+1-k)}} q^{\mathrm{inv}(w)} = \sum_{w \in S_1} q^{\mathrm{inv}(w)} + \sum_{w \in S_{-1}} q^{\mathrm{inv}(w)} =$$
$$\sum_{w' \in S_{(k-1,M+1-k)}} q^{\mathrm{inv}(w')} + \sum_{w' \in S_{(k,M-k)}} q^{\mathrm{inv}(w')+k} =$$
$$\sum_{w' \in S_{(k-1,M+1-k)}} q^{\mathrm{inv}(w')} + q^k \sum_{w' \in S_{(k,M-k)}} q^{\mathrm{inv}(w')} =$$
$$\begin{bmatrix} M \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} M \\ k \end{bmatrix}_q = \begin{bmatrix} M+1 \\ k \end{bmatrix}_q = \begin{bmatrix} M+1 \\ \alpha \end{bmatrix}_q$$

which concludes the proof. Observe that we could just as well have made the division of S_α based on the first letter. Then the proof would instead have followed from the second q-Pascal recursion. □

With the help of this lemma it is quite straightforward to prove the following proposition.

Proposition 17. *The function*

$$f_{n,m}(q) = \sum_{\substack{\alpha \in \alpha_{m,2}: \\ n \mid S\alpha}} \begin{bmatrix} m \\ \alpha \end{bmatrix}_q$$

is the generating polynomial of the inversion statistic on the set $C_{\Gamma,m}$ in the sense that it is the generating polynomial of the inversion statistic on the corresponding set of words S^c_m.

Proof. This follows immediately from Lemma 16 by simply adding the generating polynomials for the inversion statistic on S_α for every composition α in the index set. □

3.2. **Closed walks in circulant graphs.** This subsection largely mirrors the last. We prove the very same propositions but for a more general family of graphs. We first define a certain kind of matrix.

Definition 16. A $n \times n$ matrix M is said to be a circulant matrix if its entries satisfy

$$m_{i,j} = m_{1,j-i+1}$$

where the subscripts are reduced modulo n. In other words row i of M is obtained from the first row of M by cyclic shift of $i-1$ steps and so any circulant matrix is determined by its first row. Observe that the circulant matrix whose first row is $[0,1,0,\dots,0]$ is the permutation matrix P generating a n-element cyclic sub-group of S_n.

Now we use circulant matrices to define a family of graphs.

Definition 17. A graph G is said to be a circulant graph if its adjacency matrix A is circulant. Important sub-classes of circulant graphs include cycle graphs, complete graphs and the cocktail party graphs $K_{2,2,\dots,2}$. More generally, it follows from the fact that the adjacency matrix is a symmetric matrix with zeroes on the main diagonal that the adjacency matrix of a circulant graph has a first row $[0,a_2,\dots,a_n]$ where $a_i = a_{n-i+2}$ since $a_{1,i} = a_{i,1} = a_{1,2-i} = a_{1,n-2+i}$. In a simple graph we will also have $a_i \in \{0,1\}$. Such a graph can be described in the following manner: we take $k \le n-1$ indices such that $0 < s_1 < s_2 < ..s_k \le n-1$ and $a_i = 1$ iff $i \in \{s_1+1, s_2+1, \dots, s_k+1\}$. The set $\{s_1, s_2, \dots, s_k\}$ is called the index set of the circulant graph.

We prove that circulant matrices are Cayley graphs of cyclic groups.

Proposition 18. *The circulant graph G with n vertices and index set $\{s_1, s_2, \dots, s_k\}$ is the Cayley graph $\Gamma = (\mathbb{Z}_n, \{s_1, s_2, \dots, s_k\})$ and for its adjacency matrix A the following identity holds*

$$A = \sum_{i=1}^{k} P^{s_i}$$

Proof. Obviously both graphs have the same number of vertices. Given two vertices u, v in Γ we have that uv is an edge of Γ if and only if $u - v = s_i \mod n$ for some i. On the other hand, uv is an edge in G if and only if the $(v+1, u+1)$-th entry of its adjacency matrix A is 1. But since A is a circulant matrix, we have $a_{v+1,u+1} = a_{1,v-u+1}$ which is 1 if and only $v - u = s_i$ for some i. Now that we have established that G is a Cayley graph it follows from Theorem 5, that its adjacency matrix A can be expressed as a sum $P_1 + P_2 + \dots P_k$ where $P_1, P_2, \dots, P_k$ are the permutation matrices corresponding to the permutations $\pi_i(a) = a + s_i \mod n$. But then π_i is just p^{s_i} where p is the permutation defined by $p(a) = a + 1 \mod n$. So the permutation matrix corresponding to π_i is P^{s_i} which proves the second part of the theorem. □

Example 18. Figure 4 shows the circulant graph $\Gamma = (\mathbb{Z}_6, \{1,3,5\})$. Its adjacency matrix is given by $A = P + P^3 + P^5$.

We now enumerate $C_{\Gamma,m}$.

Proposition 19. *For a circulant Cayley graph $\Gamma = (\mathbb{Z}_n, S)$ with $|S| = k$, we have*

$$|C_{\Gamma,m}| = \sum_{\substack{\alpha \in \alpha_{m,k}: \\ n \mid S\alpha}} \binom{m}{\alpha}.$$

Proof. Again we prove this in two different ways. First, we have $C_{\Gamma,m} = (A^m)_{11}$ by Theorem 1. Now, all the matrices P^{s_i} commute, so the multinomial theorem

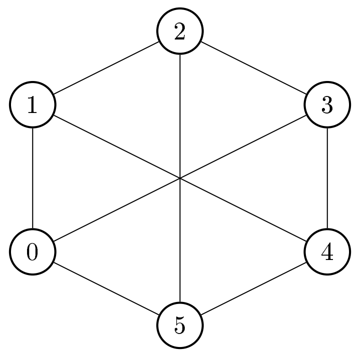

Figure 4: The circulant graph $\Gamma = (\mathbb{Z}_6, \{1, 3, 5\})$

applies and we have

$$(A^m)_{11} = ((\sum_{i=1}^{k} P_1^{j_i})^m)_{11} = \sum_{\alpha \in \alpha_{m,k}} \binom{m}{\alpha} (P^{S\alpha})_{11}.$$

Now since

$$(P^{S\alpha})_{11} = 0$$

unless $n|S\alpha$, in which case it is 1, we get

$$(A^m)_{11} = \sum_{\substack{\alpha \in \alpha_{m,k}: \\ n|S\alpha}} \binom{m}{\alpha},$$

as desired. For the second proof, we consider instead the corresponding set of words S_m^c in the alphabet $S = \{s_1, s_2, \ldots, s_k\}$. A word $w \in S_m$ with content α corresponds to a closed walk if and only if $n|S\alpha$, and for each such composition α there are precisely $\binom{m}{\alpha}$ words with content α in S_m, which proves the result. □

Example 19. We consider a walk of length 4 in $\Gamma = (\mathbb{Z}_6, \{1, 3, 5\})$. Suppose the corresponding word w has content α. Then w is closed if and only if $6|\alpha_1 + 3\alpha_2 + 5\alpha_3$, which is satisfied by the compositions $(3, 1, 0), (0, 1, 3), (1, 2, 1), (0, 4, 0), (2, 0, 2)$. So the number of closed walks of length 4 is

$$\binom{4}{3,1,0} + \binom{4}{0,1,3} + \binom{4}{1,2,1} + \binom{4}{0,4,0} + \binom{4}{2,0,2} = 4 + 4 + 12 + 1 + 6 = 27.$$

Now we describe and enumerate the fixed point-sets when $\mathbb{Z}_m$ acts on $C_{\Gamma,m}$.

Proposition 20. *Let $\Gamma = (\mathbb{Z}_n, S = \{s_1, s_2, \ldots, s_k\})$ and for clarity let $V = C_{\Gamma,m}$ and let $W = S_m^c$ be the corresponding set of words. Suppose now that $g \in \mathbb{Z}_m$ acts by cyclic shift on W and thus by extension on V. Then the cardinality of the fixed point set V_g is given by*

$$|V_g| = \sum_{\substack{\alpha \in \alpha_{d,k}: \\ n|\frac{m}{d}S\alpha}} \binom{d}{\alpha}$$

where $d = \gcd(m, g)$.

Proof. A word $w \in W$ can be subdivided into m/d subwords each of length d, as $w = w_1w_2 \dots w_{m/d}$. In the exact same way as was argued in Theorem 14 it follows that if w is fixed under the action of g, then all subwords w_i must be identical, that is $w = w_1^{m/d}$. Now suppose w_1 has content α. Then w has content $(m/d)\alpha$ and it follows that w corresponds to a closed walk if and only if $n|\frac{m}{d}S\alpha$. On the other hand these criteria are sufficient, that is: if w_1 is a word in the alphabet S with content α such that $n|\frac{m}{d}S\alpha$, then the word $w = w_1^{m/d}$ is fixed by the action of g and corresponds to a closed walk. But for a particular composition $\alpha \in \alpha_{d,k}$ the number of such words is $\binom{d}{\alpha}$, so we have

$$|V_g| = |W_g| = \sum_{\substack{\alpha \in \alpha_{d,k}: \\ n|\frac{m}{d}S\alpha}} \binom{d}{\alpha}.$$

□

Example 20. We consider again the closed walks of length 4 in $\Gamma = (\mathbb{Z}_6, \{1, 3, 5\})$, this time under the action of $\mathbb{Z}_4$. We consider them again as words. Any such word is fixed under the action of 0, so $V_0 = 27$. Now, if such a word is fixed under the action of 2 then it is composed of two identical sub-words, so if it has content α then all α_i are even. By Example 19 it follows then that α is either $(0, 4, 0)$ or $(2, 0, 2)$ and so the two-letter subword has either content $(0, 2, 0)$ or $(1, 0, 1)$. The number of possible subwords is then

$$\binom{2}{0,2,0} + \binom{2}{1,0,1} = 1 + 2 = 3,$$

namely the words 33, 15 and 51, giving the four-letter words $3333, 1515, 5151$. Finally, words that are fixed by the action of 1 or 3 are composed of 4 identical sub-words of length 1 so among closed walks, only those with content $(0, 4, 0)$ apply and there is only 1 such word, namely 3333.

To prove that we here have another instance of the cyclic sieving phenomenon we need the following lemma.

Lemma 21. *Suppose that* $\xi = e^{\frac{2\pi i}{m}g}$*, that* $d = \gcd(m, g)$*, that* $\alpha \in \alpha_{m,k}$ *and let* $m = d\frac{m}{d}$*,* $\alpha_i = \beta_i\frac{m}{d} + \rho_i$*. The multinomial coefficient*

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_q$$

evaluated at ξ *is* 0 *unless* $(m/d)|\alpha_i$ *for every* i*, in which case it is*

$$\binom{d}{\beta}.$$

Proof. We prove this by induction over k. First, for $k = 1$ this is trivial. Suppose $k = 2$. Then the multinomial coefficient is really a binomial coefficient and we have:

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_q = \begin{bmatrix} m \\ \alpha_1 \end{bmatrix}_q.$$

Now $\xi = e^{2\pi i \frac{g}{m}} = e^{2\pi i \frac{g/d}{m/d}}$ with $\gcd(g/d, m/d) = 1$, so ξ is a primitive m/d-th root of unity. We get from q-Lucas that

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_\xi = \begin{bmatrix} m \\ \alpha_1 \end{bmatrix}_\xi = \binom{d}{\beta_1} \times \begin{bmatrix} 0 \\ \rho_1 \end{bmatrix}_\xi .$$

Now, if α_1 is not divisible by m/d then $\rho_1 > 0$ and so this is 0. On the other hand if α_1 is divisible by m/d then $\rho_1 = 0$ so then this is

$$\binom{d}{\beta_1} \times 1 = \binom{d}{\beta}.$$

Now as induction hypothesis, we assume that for $k = K$ the statement is true for every multinomial coefficient. Now, assuming $k = K + 1$, we factorize

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_q = \begin{bmatrix} m - \alpha_{K+1} \\ \alpha_1, \dots, \alpha_K \end{bmatrix}_q \begin{bmatrix} m \\ \alpha_{K+1} \end{bmatrix}_q$$

so that for $\xi = e^{\frac{2\pi i}{m} g}$ q-Lucas gives

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_\xi = \begin{bmatrix} m - \alpha_{K+1} \\ \alpha_1, \dots, \alpha_K \end{bmatrix}_\xi \binom{d}{\beta_{K+1}} \begin{bmatrix} 0 \\ \rho_{K+1} \end{bmatrix}_\xi .$$

Now if α_{K+1} is not divisible by m/d then this is 0 because of the last factor. But α_{K+1} is just an arbitrary part of the composition, so by symmetry $\rho_i = 0$ for all i or else the multinomial coefficient is zero. But if they all are divisible by m/d then $\beta \in \alpha_{d,K+1}$ and the induction hypothesis gives

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_\xi = \begin{bmatrix} m - \alpha_{K+1} \\ \alpha_1, \dots, \alpha_K \end{bmatrix}_\xi \begin{bmatrix} m \\ \alpha_{K+1} \end{bmatrix}_\xi = \binom{d - \beta_{K+1}}{\beta_1, \dots, \beta_K} \binom{d}{\beta_{K+1}} = \binom{d}{\beta},$$

and we are done. □

Now we return to the enumeration of $C_{\Gamma,m}$

$$|C_{\Gamma,m}| = \sum_{\substack{\alpha \in \alpha_{m,k}: \\ n | S\alpha}} \binom{m}{\alpha}.$$

A natural q-analogue for this enumeration is given by

$$f_{\Gamma,m}(q) = \sum_{\substack{\alpha \in \alpha_{m,k}: \\ n | S\alpha}} \begin{bmatrix} m \\ \alpha \end{bmatrix}_q .$$

With the help of the previous lemma it is now simple to prove our second, more general instance of the cyclic sieving phenomenon.

Theorem 22. *The triple $(C_{\Gamma,m}, \mathbb{Z}_m, f_{\Gamma,m})$, where $\mathbb{Z}_m$ acts on $C_{\Gamma,m}$ by cyclic shift, exhibit the cyclic sieving phenomenon.*

Proof. For $\xi = e^{\frac{2\pi i}{m} g}$ with $d = \gcd(g, m)$ it follows immediately from the previous lemma that

$$f_{\Gamma,m}(\xi) = \sum_{\substack{\alpha \in \alpha_{m,k}: \\ n | S\alpha}} \begin{bmatrix} m \\ \alpha \end{bmatrix}_\xi = \sum_{\substack{\beta \in \alpha_{d,k}: \\ n | \frac{m}{d} S\beta}} \binom{d}{\beta},$$

since a composition $\alpha \in \alpha_{m,k}$ where all α_i are divisible by m/d uniquely determines a composition $\beta \in \alpha_{d,k}$ and vice versa. But from the Proposition 20, we know that this is precisely the number of elements that are fixed by the action of g when $\mathbb{Z}_m$ acts on $C_{\Gamma,m}$ by cyclic shift, so that we here have an instance of the cyclic sieving phenomenon. □

Example 21. We return once again to closed walks of length 4 in $\Gamma = (\mathbb{Z}_6, \{1,3,5\})$. In Example 19 we found the enumeration

$$\binom{4}{3,1,0} + \binom{4}{0,1,3} + \binom{4}{1,2,1} + \binom{4}{0,4,0} + \binom{4}{2,0,2},$$

with q-analogue

$$f_{\Gamma,4}(q) = \begin{bmatrix}4\\3,1,0\end{bmatrix}_q + \begin{bmatrix}4\\0,1,3\end{bmatrix}_q + \begin{bmatrix}4\\1,2,1\end{bmatrix}_q + \begin{bmatrix}4\\0,4,0\end{bmatrix}_q + \begin{bmatrix}4\\2,0,2\end{bmatrix}_q =$$
$$2(1+q+q^2+q^3) + (1+q+q^2+q^3)(1+q+q^2) + 1 + (1+q^2)(1+q+q^2).$$

Evaluating this at $\xi = e^{\frac{2\pi i}{4} g}$, we get the following results. When $g = 0$ we have $\xi = 1$ and $f_{\Gamma,4}(1) = 27$. When $g = 1$ we have $\xi = i$ and $f_{\Gamma,4}(i) = 1$. When $g = 3$ we have $\xi = -i$ and $f_{\Gamma,4}(-i) = 1$ again. Finally, when $g = 2$ we have $\xi = -1$ and $f_{\Gamma,4}(-1) = 3$. This agrees with our enumeration of the fixed point sets in Example 20.

Finally, we in this case too show that the q-analogue

$$f_{\Gamma,m}(q) = \sum_{\substack{\alpha \in \alpha_{m,k}:\\ n \mid S\alpha}} \begin{bmatrix}m\\\alpha\end{bmatrix}_q.$$

is in fact the generating polynomial of the inversion statistic on the set $C_{\Gamma,m}$. To do this, we first need a lemma.

Lemma 23. *For every composition $\alpha \in \alpha_{m,k}$ the generating polynomial of the inversion statistic on S_α is $\begin{bmatrix}m\\\alpha\end{bmatrix}_q$ [Sta12].*

Proof. For the sake of clarity we think of S_α as words in the alphabet $\{1,2,\ldots,k\}$ instead of the alphabet $\{s_1, s_2, \ldots, s_k\}$. We now prove the lemma by induction over k. If $k = 1$ this is trivial, there is only one word in S_α and it has no inversions, so the generating polynomial is 1, which is equal to the multinomial coefficient. For $k = 2$ this is equivalent to Lemma 16. Now, suppose that for $k = N$ we have that, for every composition α the generating polynomial of the inversion statistic on S_α is $\begin{bmatrix}m\\\alpha\end{bmatrix}_q$.

Now consider a composition $\alpha \in \alpha_{m,N+1}$. For a word w with content α, we define two operations. The first takes w to a word w', obtained by removing all the 1:s in w, so that w' has content $\alpha' = (\alpha_2, \ldots, \alpha_{N+1})$ in the alphabet $\{2, \ldots, N, N+1\}$. The second takes w to a word w'' obtained by changing every letter except 1 into the letter 2, so that w'' has content $\alpha'' = (\alpha_1, m - \alpha_1)$ in the alphabet $\{1, 2\}$. Recall that an inversion in w is a pair i, j with $i > j$ but $\phi(i) < \phi(j)$, that is the i:th letter of w is smaller than the j:th letter. Since every inversion of w can be of two kinds, those were $\phi(i) = 1$ and those were $\phi(i) \neq 1$, every inversion in w corresponds to an inversion in exactly one of w' and w'', so that $\text{inv}(w) = \text{inv}(w') + \text{inv}(w'')$.

Furthermore, the function taking w to the pair (w', w'') is clearly a bijection $S_\alpha \to S_{\alpha'} \times S_{\alpha''}$. So we have for the generating function of the inversion statistic on S_α

$$F(q) = \sum_{w \in S_\alpha} q^{\mathrm{inv}(w)} = \sum_{(w',w'') \in S_{\alpha'} \times S_{\alpha''}} q^{\mathrm{inv}(w') + \mathrm{inv}(w'')} =$$

$$\sum_{w' \in S_{\alpha'}} q^{\mathrm{inv}(w')} \times \sum_{w'' \in S_{\alpha''}} q^{\mathrm{inv}(w'')} = \begin{bmatrix} m - \alpha_1 \\ \alpha' \end{bmatrix}_q \times \begin{bmatrix} m \\ \alpha_1 \end{bmatrix}_q = \begin{bmatrix} m \\ \alpha \end{bmatrix}_q,$$

which proves the lemma by induction. □

Example 22. Once again, we consider closed walks in $\Gamma = (\mathbb{Z}_6, \{1, 3, 5\})$, this time focusing on those with content $(2, 0, 2)$. There are six such walks, corresponding to the words $1155, 1515, 5115, 1551, 5151, 5511$ with inversion statistics $0, 1, 2, 2, 3, 4$. On the other hand we have

$$\begin{bmatrix} 4 \\ 2, 0, 2 \end{bmatrix} = (1 + q^2)(1 + q + q^2) = 1 + q + 2q^2 + q^3 + q^4,$$

verifying Lemma 23.

The following proposition now comes easy.

Proposition 24. *The function*

$$f_{\Gamma,m}(q) = \sum_{\substack{\alpha \in \alpha_{m,k}: \\ n \mid S\alpha}} \begin{bmatrix} m \\ \alpha \end{bmatrix}_q.$$

is the generating polynomial of the inversion statistic on the set $C_{\Gamma,m}$ in the sense that it is the generating polynomial of the inversion statistic on the corresponding set of words S_m^c.

Proof. As in Proposition 17, this follows immediately from Lemma 23 by simply adding the generating polynomials for the inversion statistic on S_α for every composition α in the index set. □

3.3. **Closed walks in n-dimensional infinite grids.** We now make a slight digression and consider a family of infinite Cayley graphs, the infinite rectangular grids. As before, we start by enumerating closed walks of length m but then take a quite different approach.

Definition 18. Let e_i be the i :th unit vector. The Cayley graph $\Gamma = (\mathbb{Z}^n, \{e_1, -e_1, e_2, -e_2 \ldots e_n, -e_n\})$ is then the n-dimensional infinite rectangular grid or just the n-grid for short.

We will show another instance of the cyclic sieving phenomenon on $C_{\Gamma,m}$. Because the graph is infinite, our method of considering the adjacency matrix as a sum of permutation matrices will not work, so enumeration has to be done with a combinatoric argument.

Proposition 25. *The number of closed walks of length m beginning and ending in the origin of Γ is*

$$|C_{\Gamma,m}| = \sum_{\alpha \in \alpha_{m/2,n}} \binom{m}{\alpha_1, \alpha_1, \alpha_2, \alpha_2, \ldots, \alpha_n, \alpha_n}.$$

Proof. Consider a walk in Γ of length m beginning at the origin and let w be the corresponding word in the alphabet S. Suppose w has content α. Then at the end of our walk we will find ourselves at point $(\alpha_1 - \alpha_2, \alpha_3 - \alpha_4, \dots, \alpha_{2n-1} - \alpha_{2n})$. It follows that w is closed if and only if $\alpha_1 = \alpha_2, \alpha_3 = \alpha_4, \dots \alpha_{2n-1} = \alpha_{2n}$. Hence, if w is closed then m is even, that is: Γ is bipartite. On the other hand, if n is even then the number of words with content $(\alpha_1, \alpha_1, \alpha_3, \alpha_3 \dots, \alpha_{2n-1}, \alpha_{2n-1})$ where $\alpha_1 + \alpha_3 + \dots \alpha_{2k-1} = n$ is

$$\binom{m}{\alpha_1, \alpha_1, \alpha_3, \alpha_3, \dots, \alpha_{2n-1}, \alpha_{2n-1}},$$

so the total number of closed walks is

$$|C_{\Gamma,m}| = \sum_{\alpha \in \alpha_{m/2,n}} \binom{m}{\alpha_1, \alpha_1, \alpha_2, \alpha_2, \dots, \alpha_n, \alpha_n}.$$

Observe that this is 0 when m is odd because then the index set is empty. □

Example 23. Consider walks of length 6 in the 3-grid. Such a walk is closed if and only if there as many moves up as down, as many left as right and as many forward as backward. So we can think of a closed walk of length 6 as consisting of 3 pairs of the form up-down, left-right, forward-backward. So a closed walk induces a composition of 3 into 3 components, signifying how many instances of each pair occur in the walk. There are 10 different compositions of 3 into 3 components, ordered by type there are 3 of the type $(3, 0, 0)$, 6 of the type $(2, 1, 0)$ and one of the type $(1, 1, 1)$. To each composition of 3 there is then a corresponding composition of 6, signifying how many steps are taken in each of the six directions, so for instance $(0, 3, 0)$ corresponds to $(0, 0, 3, 3, 0, 0)$. Finally for each such composition of 6 the multinomial coefficient counts the number of walks with this composition as content. So the total number of closed walks of length 6 is

$$3\binom{6}{3,3,0,0,0,0}+6\binom{6}{2,2,1,1,0,0}+1\binom{6}{1,1,1,1,1,1} = 3\cdot 20+6\cdot 180+1\cdot 720 = 1860.$$

Given this enumeration, a natural q-analogue presents itself immediately

$$f_{n,m}(q) = \sum_{\alpha \in \alpha_{m/2,n}} \begin{bmatrix} m \\ \alpha_1, \alpha_1, \alpha_2, \alpha_2, \dots, \alpha_n, \alpha_n \end{bmatrix}_q.$$

Of course we could again show cyclic sieving by enumerating the fixed point sets and then evaluating $f(n, m)(q)$ at roots of unity, as we have done before. However this time we will take another approach, namely constructing a circulant graph G_m and present a bijection between $C_{\Gamma,m}$ and $C_{G_m,m}$. Essentially this graph approximates the behaviour of walks in Γ starting at a particular point by exploiting the fact that for the purpose of studying walks of length at most m we might as well regard Γ as a finite graph, since only finitely many of its vertices can be reached in m steps. We first define G_m.

Definition 19. A m-th circulant approximation of the n-grid Γ is a circulant Cayley graph $G = (\mathbb{Z}_N, T = \{s_1, s_2 \dots, s_{2n}\}$ where N should be thought of as some very large number, $N = (m+1)^n$ is sufficient, and $s_{2i+1} = (m+1)^i$ for odd indices and $s_{2i+2} = -(m+1)^i$ for even indices.

Observe that there as many elements in the generating set of Γ as there are in the generating set of G_m. This immediately gives a bijection between walks of length m in Γ and walks of length m in G_m, by way of their words, by translating the word form of a walk in Γ into the word form of a walk in G_m. Also, this translation preserves the fixed point sets under the action of $\mathbb{Z}_m$ by cyclic shift. More formally stated, the translation function commutes with the cyclic shift action. However, it might not be immediately obvious that this translation preserves closedness.

Proposition 26. *The translation of walks in Γ into walks in G_m preserves closedness, that is, a walk in Γ is closed if and only the corresponding walk in G_m is closed. From this it also follows that $C_{\Gamma,m} = C_{G_m,m}$.*

Proof. Consider a word w of length m corresponding to a closed walk in G_m and suppose it has content α. $N|T\alpha$. For sufficiently large N this implies that $T\alpha = \alpha_1 s_1 + \ldots + \alpha_{2n} s_{2n} = 0$. Essentially, for sufficiently large N no closed walk can travel around the entire graph, so that we always return to 0 from the same direction as we last left it. Hence, for sufficiently large N we have, when considering s_i explicitly, that

$$(\alpha_1 - \alpha_2) + (\alpha_3 - \alpha_4)(m+1) + (\alpha_5 - \alpha_6)(m+1)^2 + \ldots + (\alpha_{2n-1} - \alpha_{2n})(m+1)^{n-1} = 0.$$

Since the left hand side of this equation is divisible by $m+1$ and since $-m \leq \alpha_i - \alpha_{i+1} \leq m$, we must have $\alpha_1 = \alpha_2$. The condition now becomes

$$(\alpha_3 - \alpha_4)(m+1) + (\alpha_5 - \alpha_6)(m+1)^2 + \ldots + (\alpha_{2n-1} - \alpha_{2n})(m+1)^{n-1} = 0,$$

and then it follows that since the left hand side is also divisible by $(m+1)^2$, we must have $\alpha_3 = \alpha_4$. Continuing in this manner, it becomes evident that $\alpha_1 = \alpha_2, \alpha_3 = \alpha_4, \ldots, \alpha_{2n-1} = \alpha_{2n}$. But translation preserves content, so it preserves closedness, so a word in T_m corresponds to a closed walk if and only if its translation to S_m does. This gives us

$$|C_{G_m,m}| = |C_{\Gamma,m}| = \sum_{\alpha \in \alpha_{m/2,n}} \binom{m}{\alpha_1, \alpha_1, \alpha_2, \alpha_2 \ldots, \alpha_n, \alpha_n}.$$

□

Example 24. A sixth circulant approximation of the 3-grid is given by $G = (\mathbb{Z}_{1000}, \{1, -1, 7, -7, 49, -49\})$. For $m \in \{1, 2, 3, 4, 5, 6\}$ there are as many closed walks of length m in G beginning and ending in some particular vertex as there are in the 3-grid.

Now cyclic sieving follows.

Theorem 27. *The triple $(C_{\Gamma,m}, \mathbb{Z}_m, f_{n,m}(q))$, where $\mathbb{Z}_m$ acts on $C_{\Gamma,m}$ by cyclic shift, exhibit the cyclic sieving phenomenon.*

Proof. This follows immediately from cyclic sieving on closed walks in circulant graphs. The translation function from Γ to G_m preserves the fixed point sets under the action of $\mathbb{Z}_m$ by cyclic shift and the polynomial $f_{n,m}(q)$ is the q-analogue of the enumeration of the circulant graph G_m. □

3.4. **Closed walks in general Cayley graphs.** Since everything has been going quite well so far, one might consider how far our results may be generalized. Perhaps we could show cyclic sieving on closed walks in a general Cayley graph? Unfortunately, this turns out to decidedly more difficult than anything we have dared so far. To realize why, we might stop to reflect on our methods so far. First, we have enumerated our sets. This we have done in two different ways, on the one hand by expressing the adjacency matrix A as a sum of permutation matrices and using the bi-/multi-nomial theorem to evaluate the diagonal elements of A^m. On the other hand we have used combinatorial arguments, based on an interpretation of walks as words. These two approaches largely mirror each other, the symmetries used in the combinatorial arguments are the same symmetries that allow easy evaluation of the multinomial expression of A^m. However, in the absence of such symmetries our methods fail. If the group on which the Cayley graph is built is non-abelian, the permutation matrices do not commute and the multinomial theorem is not even applicable. In this case too, two words abc and bca might represent walks with different destinations, one being closed the other not, so that content does not determine closedness. Even when G is abelian we will encounter difficulties. In the cases we have considered the adjacency matrix A could be expressed as a sum of permutation matrices that were all part of the same cyclic subgroup of the symmetric group. Absent this we cannot easily evaluate the expression of A^m even though the multinomial theorem is applicable.

In fact, no enumeration for the number of closed walks in a general Cayley graph is known, not even in a general finite abelian Cayley graph, so any hope of generalizing our results that far stumbles at the first step. More than a little research on the subject has been published. As a single example [Cio06] proves the following lower bound for the number of closed walks of length $2r$, W_{2r}, in an abelian Cayley graph with k vertices:

$$W_{2r} > \frac{k^{2r}}{2^k(2r+1)\binom{k+r-1}{k-1}}.$$

Bounds unfortunately do not suffice for our aims, so we must renounce any ambition to prove cyclic sieving on general Cayley graphs, even on general finite abelian Cayley graphs. But what if we were to restrict not G but S, the generating set? So far we have only restricted S to guarantee that the resulting Cayley graph is indeed a simple, undirected, loop free graph. It turns out that we can significantly generalize our results with regard to G by restricting them in regard to S. So far, we have considered Cayley graphs where the underlying group is cyclic, that is circulant graphs and in fact any Cayley graph of a finite cyclic group is circulant. But any non-cyclic finite abelian group is isomorphic to a direct product of cyclic groups. Choosing S in a particular manner allows us to use our already established results concerning circulant graphs on the Cayley graphs of such direct products.

Definition 20. Given a number of Cayley graphs $\Gamma_i = (G_i, S_i), 1 \leq i \leq n$, the direct product $\prod_{i=1}^{n} \Gamma_i$ is defined as the Cayley graph $\Gamma = (G, S)$, where $G = G_1 \times G_2 \cdots \times G_n$ and S is determined by the following criteria:

- for every $s \in S_i$ for every i, the vector se_i, with s in position i and zero in every other position, is in S,

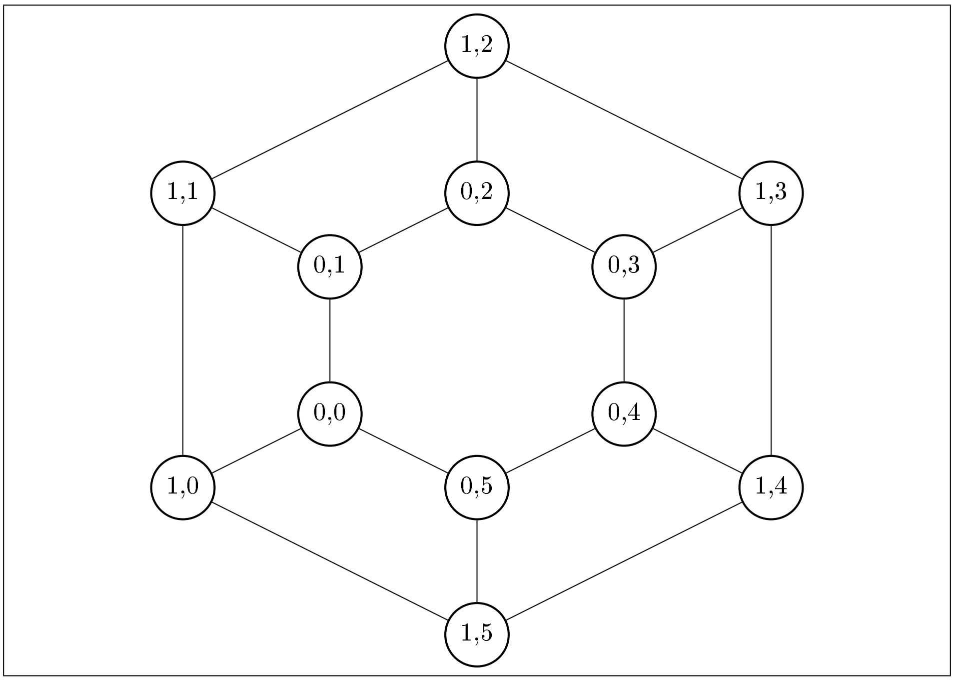

Figure 5: The graph $\Gamma = (\mathbb{Z}_2 \times \mathbb{Z}_6, \{(1,0),(0,1),(0,5)\})$

- every $s \in S$ has zero in every position except for one, say the i:th, and the i:th entry is a letter in S_i.

Furthermore, for $s_j \in S_i$ we say that the letter $s_j e_i \in S$ projects onto s_j. A word w in S projects onto $(w_1, w_2, \ldots, w_n)$, where w_i is a word in the alphabet S_i consisting of the projection of the letters in w that project onto letters in S_i and the letters in w_i appear in the same order as their preimages in w.

Example 25. Figure 5 shows the Cayley graph $\Gamma = (\mathbb{Z}_2 \times \mathbb{Z}_6, \{(1,0),(0,1),(0,5)\})$ with $\Gamma_1 = (\mathbb{Z}_2, \{1\})$ and $\Gamma_2 = (\mathbb{Z}_2, \{1,5\})$. The walk represented by the word $(1,0)(0,1)(1,0)(0,5)$ is closed. It projects onto the pair of words $11 \in \mathbb{Z}_2$ and $15 \in \mathbb{Z}_6$, both of which represent closed walks.

The point here is that a word w in S describes a closed walk in the direct product Γ if and only if for each i, the letters in w that project onto S_i describe a closed walk in Γ_i. This allows us to calculate the number of closed walks in Γ in terms of the number of closed walks in Γ_i. If all Γ_i are circulant we can then calculate the number of closed walks in Γ, based on our results on circulant graphs.

Proposition 28. *Suppose that $\Gamma = (G,S)$ is the direct product product $\prod_{i=1}^{n} \Gamma_i$, where each $\Gamma_i = (Z_{n_i}, S_i)$ is circulant. Then the number of closed walks of length m beginning and ending in $\mathbf{0}$ of Γ is given by*

$$|C_{\Gamma,m}| = \sum_{\alpha \in \alpha_{m,n}} \left(\binom{m}{\alpha} \prod_{i=1}^{n} |C_{\Gamma_i,\alpha_i}| \right).$$

Proof. For a word $w \in S_m$ the projection onto $(w_1, \ldots w_n)$ induces a composition $\alpha \in \alpha_{m,n}$ in the sense that each w_i has length α_i. For each such α we have $w \in S_m^c$

if and only if $w_i \in S^c_{i,\alpha_i}$ for every i. The number of ways to choose such words w_i is $\prod_{i=1}^n |C_{\Gamma_i,\alpha_i}|$ and the number of ways of arranging the letters se_i into a word in S while preserving the order of letters derived from each word w_i is

$$\binom{m}{\alpha}.$$

The proposition follows by summing over all the possible compositions of m and then considering the bijection between words and walks. □

Example 26. Let us look at closed walks of length 4 in $\Gamma = (\mathbb{Z}_2 \times \mathbb{Z}_6, \{(1,0),(0,1),(0,5)\})$. There are 5 possibilities as to how many letters project onto $\mathbb{Z}_2$ and how many onto $\mathbb{Z}_6$. For $\alpha = (4,0)$ we have 1 word in $C_{\Gamma_1,4}$ and 1 "word" in $C_{\Gamma_2,0}$, the words 1111 and the empty "word". For $\alpha = (3,1)$ there are no words in $C_{\Gamma_1,4}$ and also none in $C_{\Gamma_2,0}$, they are both bipartite. For $\alpha = (2,2)$ we have 1 word in $C_{\Gamma_1,2}$, 11, and 2 words in $C_{\Gamma_2,2}$, the words 15 and 51. The case $\alpha = (1,3)$ is just like the case $\alpha = (3,1)$. Finally, for $\alpha = (0,4)$ we have 1 word in $C_{\Gamma_1,0}$, the empty word, and 6 words in $C_{\Gamma_2,4}$, the words $1155, 1515, 5115, 1551, 5151, 5511$. The total number of closed walks in Γ is then given by

$$\binom{4}{4,0}1 \times 1 + \binom{4}{3,1}0 \times 0 + \binom{4}{2,2}1 \times 2 + \binom{4}{1,3}0 \times 0 + \binom{4}{0,4}1 \times 6 = \\ 1 + 0 + 12 + 0 + 6 = 19.$$

Now, let us determine the size of the fixed point sets when $\mathbb{Z}_m$ acts on S^c_m, and thus by extension on $C_{\Gamma,m}$.

Proposition 29. *Let $\Gamma = (G,S)$ be the direct product $\prod_{i=1}^n \Gamma_i$, where each $\Gamma_i = (Z_{n_i}, S_i)$ is circulant. Then the size of the fixed point set under the action of $g \in \mathbb{Z}_m$ on $C_{\Gamma,m}$ is given by*

$$\sum_{\alpha \in \alpha_{d,n}} \left(\binom{d}{\alpha} \prod_{i=1}^n W_{i,\alpha_i} \right).$$

where $d = \gcd(g,m)$ and W_{i,α_i} is the number of words in $S^c_{i,\alpha_i \frac{m}{d}}$ which are fixed by the action of $\alpha_i \frac{g}{d} \in \mathbb{Z}_{\alpha_i \frac{m}{d}}$.

Proof. A word w in S_m is fixed under the action of g if and only if, just as in the proofs of Proposition 14 and Proposition 20, it is a concatenation of m/d identical subwords, that is $w = w_0^{m/d}$ for some word w_0 of length d. As in Proposition 28, the projection of w_0 onto $(w_1, \ldots, w_n)$ induces a composition $\alpha \in \alpha_{d,n}$, such that w_i has length α_i. Then $w \in S^c_m$ if and only if each $w_i^{m/d} \in S^c_{i,\alpha_i \frac{m}{d}}$. Observe now how in w the action of g maps the first copy of w_0 onto the $\frac{g}{d} + 1$:th and how in $w_i^{m/d}$ it is the action of $\alpha_i \frac{g}{d}$ which maps the first copy of w_i onto the $\frac{g}{d} + 1$:th, so that w being fixed by the action of $g \in \mathbb{Z}_m$ is equivalent to w_i being fixed by the action of $\alpha_i \frac{g}{d} \in \mathbb{Z}_{\alpha_i \frac{m}{d}}$, for each i. Thus, the number of ways in which w_0 can be constructed so that $w = w_0^{m/d}$ represents a closed walk in Γ can be calculated as follows. First we choose a composition $\alpha \in \alpha_{d,n}$ representing how many of the letters in w_0 project onto each S_i. Then for each i, we pick a word w_i of length α_i in S_i such that $w_i^{m/d} \in S^c_{i,\alpha_i \frac{m}{d}}$ and this can be done in as many ways as there are words in $S^c_{i,\alpha_i \frac{m}{d}}$ which are fixed by the action of $\alpha_i \frac{g}{d}$. Finally we pick which of the

d letters in w_0 project onto which S_i. This we can do in $\binom{d}{\alpha}$ ways. In total then, the number of ways in which w_0 can be constructed is given by summing over all compositions α:

$$\sum_{\alpha \in \alpha_{d,n}} \left(\binom{d}{\alpha} \prod_{i=1}^{n} W_{i,\alpha_i} \right),$$

and the result follows as usual from the bijection between words and walks. □

Example 27. We consider again closed walks of length 4 in $\Gamma = (\mathbb{Z}_2 \times \mathbb{Z}_6, \{(1,0), (0,1), (0,5)\})$ now under the action of $\mathbb{Z}_4$. Of course all 19 words are closed under the action of 0. Words that are fixed under the action of 1 and 3 are those that consist of four identical one-letter words. The number of letters in such a word that project onto each S_i is then of the form 4α where α is a composition of 1 into two components. If $\alpha = (1,0)$ we then need to pick a word in $S^c_{1,4}$ that is fixed by the action of 1 and 3 respectively. In both cases, there is only one such word, namely 1111. Finally, we need to pick a word in $S^c_{2,0}$ that is fixed by the action of 0 and there is only one such word, the empty word. Hence the fixed point sets of 1 and 3 contain only one word $(1,0)(1,0)(1,0)(1,0)$. Words that are fixed by the action of 2 consist of 2 identical two-letter words and the number of letters in such a word that project onto each S_i is then of the form 2α where α is a composition of 2 into two components. For $\alpha = (2,0)$ we then need to pick two words, one in $S^c_{1,4}$ that is fixed by the action of 2 and one in $S^c_{2,0}$ that is fixed by the action of 0. There is only one such pair: 1111 and the empty word. For $\alpha = (1,1)$ we again need to pick two words, one in $S^c_{1,2}$ that is fixed by the action of 1 and one in $S^c_{2,2}$ that is fixed by the action of 1. There is no such word in $S^c_{2,2}$, so there is no such pair of words. Finally, for $\alpha = (0,2)$ we need to pick two words, one in $S^c_{1,0}$ that is fixed by the action of 0 and one in $S^c_{2,4}$ that is fixed by the action of 2. There is only one such word in $S^c_{1,0}$, the empty word, but there are two in $S^c_{2,4}$: 1515 and 5151. In total then there are three words that are fixed by the action of 2, namely $(1,0)(1,0),(1,0),(1,0)$ and $(0,1)(0,5)(0,1)(0,5)$ and $(0,5)(0,1)(0,5)(0,1)$.

Now given our enumeration of $|C_{\Gamma,m}|$ in Proposition 28 a natural q-analogue is given by using the q-analogue for $|C_{\Gamma_i,m_i}|$ as defined in Theorem 19. Hence we define for the direct product $\Gamma = \prod_{i=1}^{n} \Gamma_i$, where each $\Gamma_i = (Z_{n_i}, S_i)$ is circulant

$$f_{\Gamma,m}(q) = \sum_{\alpha \in \alpha_{m,n}} \left(\begin{bmatrix} m \\ \alpha \end{bmatrix}_q \prod_{i=1}^{n} f_{\Gamma_i,m_i}(q) \right).$$

Now cycling sieving follows from Theorem 22 and Lemma 21.

Theorem 30. *For the direct product $\Gamma = \prod_{i=1}^{n} \Gamma_i$, where each $\Gamma_i = (Z_{n_i}, S_i)$ is circulant, the triple $(C_{\Gamma,m}, \mathbb{Z}_m, f_{\Gamma,m})$ is an instance of the cyclic sieving phenomenon.*

Proof. Since $\xi = e^{\frac{2\pi i}{m} g}$ is a primitive m/d:th root of unity with $d = \gcd(g,m)$ it follows from Lemma 21 that

$$\begin{bmatrix} m \\ \alpha \end{bmatrix}_\xi = \binom{d}{\frac{d}{m}\alpha}$$

if all α_i are divisible by m/d and zero otherwise. But there is a bijection between compositions $\alpha \in \alpha_{m,n}$ such that $m/d|\alpha_i$for all i and compositions $\beta \in \alpha_{d,n}$, given by $\alpha_i = \frac{m}{d}\beta_i$, so we get

$$f_{\Gamma,m}(\xi) = \sum_{\beta\in\alpha_{d,n}} \left(\binom{d}{\beta} \prod_{i=1}^{n} f_{\Gamma_i,\frac{m}{d}\beta_i}(\xi) \right).$$

But because $\xi = e^{\frac{2\pi i}{m}g} = e^{2\pi i \frac{d}{m}\frac{g}{d}} = e^{2\pi i \frac{g\beta_i}{d}\frac{1}{\beta_i \frac{m}{d}}}$ it follows from Theorem 22, that $f_{\Gamma_i,\beta_i\frac{m}{d}}(\xi)$ is precisely the number of elements that are fixed by the action of $\frac{g\beta_i}{d}$ when $\mathbb{Z}_{\beta_i\frac{m}{d}}$ acts on $C_{\Gamma_i,\beta_i\frac{m}{d}}$ by cyclic shift, which is equal to the number of words in $S^c_{i,\beta_i\frac{m}{d}}$ which are fixed by the action of $\beta_i\frac{g}{d}$, that is

$$f_{\Gamma_i,\beta_i\frac{m}{d}}(\xi) = W_{i,\beta_i},$$

so that

$$f_{\Gamma,m}(\xi) = \sum_{\beta\in\alpha_{d,n}} \left(\binom{d}{\beta} \prod_{i=1}^{n} f_{\Gamma_i,\beta_i\frac{m}{d}}(\xi) \right) = \sum_{\beta\in\alpha_{d,n}} \left(\binom{d}{\beta} \prod_{i=1}^{n} W_{i,\beta_i} \right).$$

Hence by Proposition 29, $f_{\Gamma,m}(q)$ evaluated at $\xi = e^{\frac{2\pi i}{m}g}$ is equal to the size of the fixed point set of $C_{\Gamma,m}$ under the action of $g \in \mathbb{Z}_m$, so that we here have our final instance of the cyclic sieving phenomenon □

Example 28. We consider again walks of length 4 in $\Gamma = (\mathbb{Z}_2 \times \mathbb{Z}_6, \{(1,0),(0,1),(0,5)\})$. We then have

$$f_{\Gamma,m}(q) = \begin{bmatrix} 4 \\ 4,0 \end{bmatrix}_q f_{\Gamma_1,4}(q) f_{\Gamma_2,0}(q) + \begin{bmatrix} 4 \\ 3,1 \end{bmatrix}_q f_{\Gamma_1,3}(q) f_{\Gamma_2,1}(q) + \begin{bmatrix} 4 \\ 2,2 \end{bmatrix}_q f_{\Gamma_1,2}(q) f_{\Gamma_2,2}(q) + \begin{bmatrix} 4 \\ 1,3 \end{bmatrix}_q f_{\Gamma_1,1}(q) f_{\Gamma_2,3}(q) + \begin{bmatrix} 4 \\ 0,4 \end{bmatrix}_q f_{\Gamma_1,0}(q) f_{\Gamma_2,4}(q).$$

Explicating each term we get

$$f_{\Gamma,m}(q) = 1 + 0 + (1+q^2)(1+q+q^2)(1+q) + 0 + (1+q^2)(1+q+q^2) = 1 + (1+q^2)(1+q+q^2)(1+q) + (1+q^2)(1+q+q^2).$$

Evaluating this at $\xi = e^{\frac{2\pi i}{4}g}$, we get the following results. For $g = 0$ we have $\xi = 1$ and $f_{\Gamma,m}(1) = 19$. For $g = 1$ we have $\xi = i$ and $f_{\Gamma,m}(i) = 1$. For $g = 3$ we have $\xi = -i$ and $f_{\Gamma,m}(-i) = 1$. For $g = 2$ we have $\xi = -1$ and $f_{\Gamma,m}(-1) = 3$. So we see that this agrees with the size of the fixed point sets as calculated in Example 27.

4. Concluding remarks

In the end then, we have proved cyclic sieving on closed walks in a quite large family of Cayley graphs. We set out with the trivial case of cycle graphs. The methods used there to prove cyclic sieving could straightforwardly be generalized to prove cyclic sieving on circulant graphs, that is all the Cayley graphs of cyclic groups. A small detour allowed us to consider a kind of approximative approach to infinte graphs and we proved cyclic sieving on infinite rectangular grids. Finally we proved cyclic sieving on direct products of circulant graphs.

We mentioned in the introduction, that the restriction to finite graphs is rather arbitrary. In fact, if it were not for lack of time we might have been able to generalize some of our results to include infinite cyclic graphs. It seems quite evident that on any Cayley graph $\Gamma = (\mathbb{Z}, S)$, we could have used the same approximative method as in section 3.3. A very large circle locally looks like a line, after all. We state this as a conjecture.

Conjecture 1. *For any positive integer m and any Cayley graph $\Gamma = (\mathbb{Z}, S)$, there is some circulant graph G such that there are as many closed walks of length $k < m$ in Γ as in G.*

It would then seem quite straightforward to generalize Theorem 30 to include direct products including infinite cyclic graphs as factors, since for any m we could substitute such a factor with a circulant graph. We state this too as a conjecture.

Conjecture 2. *For the direct product $\Gamma = \prod_{i=1}^{n} \Gamma_i$, where each $\Gamma_i = (Z_{n_i}, S_i)$ is circulant or of the form $\Gamma_i = (\mathbb{Z}, S_i)$, the triple $(C_{\Gamma,m}, \mathbb{Z}_m, f_{\Gamma,m})$ is an instance of the cyclic sieving phenomenon.*

References

[Ale20] Per Alexandersson. The symmetric functions catalog. urlhttps://www.math.upenn.edu/ peal/polynomials/cyclic-sieving.htm#cyclicSieving, 2020. Accessed: 2020-05-06.

[Big74] Norman Biggs. *Algebraic graph theory.* Cambridge U.P., London, 1974.

[Big02] Norman Biggs. *Discrete mathematics.* Oxford Univ. Press, Oxford, 2. ed. edition, 2002.

[Cio06] S. M. Cioba. Closed walks and eigenvalues of abelian cayley graphs. *Compt.Rend. Math.*, (342):625–638, 2006.

[DF04] David Steven Dummit and Richard M. Foote. *Abstract algebra.* Wiley, Hoboken, N.J., 3. ed. edition, 2004.

[DK13] Keith Dsouza and Mike Krebs. A combinatorial trace method: Counting closed walks to assay graph eigenvalues. *The Rocky Mountain Journal of Mathematics*, 43(2):469–478, 2013.

[FH11] Dominique Foata and Guo-Niu Han. The q-series in combinatorics; permutation statistics (preliminary version). urlhttp://irma.math.unistra.fr/ guoniu/papers/p56lectnotes2.pdf, 2011. Accessed: 2020-05-06.

[HU14] Anders Holst and Victor Ufnarovski. *Matrix theory.* Studentlitteratur, Lund, 1. ed. edition, 2014.

[Löh17] Clara Löh. *Geometric Group Theory An Introduction.* Springer International Publishing, Cham, 2017.

[Oli65] Gloria Olive. Generalized powers. *The American Mathematical Monthly*, 72(6):619, June 1965.

[RB00] A.R. Rao and P. Bhimasankaram. *Linear Algebra [Elektronisk resurs].* Hindustan Book Agency, Gurgaon, 2000.

[RSW04] V. Reiner, D. Stanton, and D. White. The cyclic sieving phenomenon. *Journal of Combinatorial Theory, Series A*, 108(1):17 – 50, 2004.

[Sag92] Bruce E Sagan. Congruence properties of q-analogs. *Advances in Mathematics*, 95(1):127 – 143, 1992.

[Sag11] Bruce Sagan. *The cyclic sieving phenomenon: a survey*, page 183–234. London Mathematical Society Lecture Note Series. Cambridge University Press, 2011.

[Sta12] Richard P. Stanley. *Enumerative Combinatorics [Elektronisk resurs]. Volume 1.* Cambridge University Press, Cambridge, 2. ed. edition, 2012.