On arithmetic Dijkgraaf-Witten invariants of real quadratic fields

鄧, 宇琪

出版情報：Kyushu University, 2024, 博士（数理学），課程博士
バージョン：
権利関係：

On arithmetic Dijkgraaf–Witten invariants of real quadratic fields

Yuqi Deng

Graduate School of Mathematics
Kyushu University

February 11, 2025

Abstract

Dijkgraaf–Witten theory is the Chern–Simons theory with finite gauge groups. Over the past several years, Minhyong Kim and his collaborators have been studying an arithmetic analog for number rings of Dijkgraaf–Witten theory of 3-manifolds, based on the analogies between 3-manifolds and number rings, knots and primes in arithmetic topology. Then Hirano computed the mod 2 arithmetic Dijkgraaf–Witten invariant Z_k for the ring of integers of the quadratic field $k = \mathbb{Q}(\sqrt{p_1 \cdots p_r})$, where p_i's are distinct prime numbers with $p_i \equiv 1 \pmod 4$. We compute Hirano's formula for the mod 2 arithmetic Dijkgraaf–Witten invariant Z_k, and give a simple formula for Z_k in terms of the graph obtained from quadratic residues among $p_1, \cdots, p_r$. Our result answers the question posed by Ken Ono. We also give a density formula for mod 2 arithmetic Dijkgraaf–Witten invariants.

Acknowledgement

The author would like to thank Professor Ken Ono for suggesting the question which motivated this study. The author also expresses gratitude to her supervisor, Professor Masanori Morishita, for his valuable advice. Additionally, the author extends her thanks to Yuta Suzuki for introducing her to Theorem 6.7, and to her collaborators Riku Kurimaru and Toshiki Matsusaka.

Contents

1 Introduction

In [Kim20], Minhyong Kim initiated the study of arithmetic Chern–Simons theory for number rings, based on Dijkgraaf–Witten theory of 3-manifolds ([DW90]) and the analogies between number rings and 3-manifolds, primes and knots in arithmetic topology ([Mor24]). Kim's theory is concerned with totally imaginary number fields since it employs some results on étale cohomology groups of the integer rings of totally imaginary number fields ([Maz73]). Later Kim's construction was extended for any number field which may have real primes by Hirano [Hir23] and by Lee–Park [LP23], and Hirano [Hir23] introduced the mod n arithmetic Dijkgraaf–Witten invariant for any number ring containing a primitive n-th root of unity. As an interesting example, Hirano computed the mod 2 arithmetic Dijkgraaf–Witten invariant Z_k for the real quadratic field $k = \mathbb{Q}(\sqrt{p_1 \cdots p_r})$, where p_i's are distinct prime numbers with $p_i \equiv 1 \pmod 4$, and showed the following formula expressing Z_k in terms of the quadratic residue symbols among p_i's:

$$Z_k = \frac{1}{2} \sum_{\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})} \left(\prod_{i<j} \left(\frac{p_i}{p_j} \right)^{\rho(b_{ij})} \right), \tag{1.1}$$

where $T := \{(x_1, \cdots, x_r) \in (\mathbb{Z}/2\mathbb{Z})^r \mid \sum_{i=1}^r x_i = 0\}$, $b_{ij} = (0, \cdots, 0, \overset{i}{\check{1}}, 0, \cdots, 0, \overset{j}{\check{1}}, 0, \cdots, 0)$, and $\mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$ is the set of homomorphisms $T \to \mathbb{Z}/2\mathbb{Z}$.

At the conference of "Low dimensional topology and number theory XI" held at Osaka University in March of 2019, Ken Ono asked us if the right-hand side of Hirano's formula (1.1) could be simplified and suggested computing numerically many examples for p_i's in order to find such a simple formula.

In this paper, we answer Ono's question. In fact, after many numerical computer calculations, we found and proved the following simple formula for Z_k using a certain graph $G(S)$, called the quadratic residue graph associated with the set $S = \{p_1, \ldots, p_r\}$, which is determined by the quadratic residue symbols $\left(\frac{p_i}{p_j}\right)$, (see Section 4.3 for the definition of $G(S)$).

Theorem A (Theorem 4.4 below)**.** *We have*

$$Z_k = \begin{cases} 2^{r-2} & \text{if any connected component of } G(S) \text{ is a circuit,} \\ 0 & \text{if otherwise.} \end{cases} \tag{1.2}$$

We note that the graph $G(S)$ is an arithmetic analog of the linking diagram in link theory, and the idea to use the graph $G(S)$ was suggested by the analogy between primes and knots in arithmetic topology. In fact, we can show a similar formula for the topological mod 2 Dijkgraaf–Witten invariants for double covers of S^3 using the linking diagram of branched knots.

Let $\mathfrak{G}_r$ be the set of all graphs with the vertex set $\{1, 2, \ldots, r\}$ and $\mathfrak{C}_r$ be the subset of $\mathfrak{G}_r$ consisting of graphs whose connected components are all circuits. We compute the density of $\mathfrak{C}_r$ in $\mathfrak{G}_r$ (Theorem 6.3 below). Let $\mathcal{P}$ denote the set of all prime numbers and $P_r(x) := \{\{p_1, \cdots, p_r\} \subset \mathcal{P} \cap [1, x] \mid p_i \equiv 1 \pmod 4, p_i \neq p_j \ (i \neq j)\}$. Then we show the density formula for mod 2 arithmetic Dijkgraaf–Witten invariants among all real quadratic field $k = \mathbb{Q}(\sqrt{p_1 \cdots p_r})$, where $p_1, \cdots, p_r$ are distinct prime numbers with $p_i \equiv 1 \pmod 4$.

Theorem B (Theorem 6.4 below)**.** *We have*

$$\lim_{x \to \infty} \frac{\#\left\{\{p_1, \cdots, p_r\} \in P_r(x) \mid Z_k = 2^{r-2}\right\}}{\# P_r(x)} = \frac{\#\mathfrak{C}_r}{\#\mathfrak{G}_r} = \frac{1}{2^{r-1}}.$$

The contents of this paper are organized as follows. In Section 2, we provide an overview of the Dijkgraaf–Witten theory for 3-manifolds, which is a topological quantum field theory associated with finite gauge groups. Then Section 3 introduces the mod n arithmetic Dijkgraaf–Witten invariants Z_k for the ring of integers of a number field k containing a primitive n-th root of unity, based on analogies between 3-manifolds and number rings in arithmetic topology. In Section 4.1, we recall Hirano's formula for the mod 2 arithmetic Dijkgraaf–Witten invariant Z_k of real quadratic field $k = \mathbb{Q}(\sqrt{p_1 \cdots p_r})$, where p_i's are distinct prime numbers with $p_i \equiv 1 \pmod 4$. In Section 4.2, we recall some basic notions on graphs. In Section 4.3, we introduce the quadratic residue graph $G(S)$ associated with the set $S = \{p_1, \ldots, p_r\}$, and state our main theorem (cf. Theorem 4.4 below), which is a simple formula expressing Z_k, $k = \mathbb{Q}(\sqrt{p_1 \cdots p_r})$, in terms of $G(S)$. In Section 4.4, we give a proof of the main theorem. In Section 5, we give a topological counterpart of our result for the mod 2 topological Dijkgraaf–Witten invariant for a double cover of the 3-sphere S^3 branched over a link. In Section 6.1, we calculate the density of graphs with r vertices whose connected components are all circuits. In Section 6.2, we propose a density formula for mod 2 arithmetic Dijkgraaf–Witten invariants, based on the properties of quadratic residue graphs, and we prove it based on Theorem 6.7 [HB95]. Finally, we find the density of graphs whose connected components are all circuits and the density of mod 2 arithmetic Dijkgraaf–Witten invariants are equal.

2 Dijkgraaf–Witten invariants of 3-manifolds

In this section, we recall the Dijkgraaf–Witten theory for closed 3-manifolds ([DW90]). The contents of this section are based on [Hir23].

In order to define the Dijkgraaf–Witten invariant, we recall the following proposition.

Proposition 2.1. *Let M be a connected compact 3-manifold. Then, for $n \geq 2$, there exists a cohomological spectral sequence*

$$H^p(\pi_1(M), H^q(\widetilde{M}, \mathbb{Z}/n\mathbb{Z})) \Rightarrow H^{p+q}(M, \mathbb{Z}/n\mathbb{Z}),$$

where $\widetilde{M}$ denotes the universal cover of M.

Then we define the Dijkgraaf–Witten invariant for a 3-manifold.

Definition 2.2. Let M be a connected oriented closed 3-manifold. For a finite group A and an integer $n \geq 2$, let $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$ for a finite group A and $n \geq 2$. Let $\mathrm{Hom}(\pi_1(M), A)$ denote the set of all homomorphisms $\pi_1(M) \to A$. Note that the fundamental class $[M]$ generates $H_3(M, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. For each $\rho \in \mathrm{Hom}(\pi_1(M), A)$, the Chern–Simons invariant $\mathrm{CS}_c(\rho)$ of ρ associated to c is defined by the image of c under the composition of the maps

$$H^3(A, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\rho^*} H^3(\pi_1(M), \mathbb{Z}/n\mathbb{Z}) \xrightarrow{j_3} H^3(M, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\langle -, [M] \rangle} \mathbb{Z}/n\mathbb{Z},$$

where j_3 denotes the edge homomorphism in the spectral sequence

$$H^p(\pi_1(M), H^q(\widetilde{M}, \mathbb{Z}/n\mathbb{Z})) \Rightarrow H^{p+q}(M, \mathbb{Z}/n\mathbb{Z})$$

of Proposition 2.1. The Dijkgraaf–Witten invariant of M associated to c is then defined by

$$Z_c(M) = \frac{1}{\#A} \sum_{\rho \in \mathrm{Hom}(\pi_1(M), A)} \exp\left(\frac{2\pi i}{n} \mathrm{CS}_c(\rho)\right).$$

We call $\mathrm{CS}_c(\rho)$ and $Z_c(M)$ the mod n Chern–Simons invariant and the mod n Dijkgraaf–Witten invariant respectively.

3 Arithmetic Dijkgraaf–Witten invariants of number fields

In this section, we introduce the mod n arithmetic Dijkgraaf–Witten invariants for number rings, based on the analogies between 3-manifolds and number rings, as well as knots and primes.

Let k be a number field of finite degree over $\mathbb{Q}$. We fix a primitive n-th root of unity ζ_n and assume that k contains ζ_n. Let $\mathcal{O}_k$ denote the ring of integers of k and S_k^∞ the set of infinite primes of k. Define $\overline{X}_k = \mathrm{Spec}(\mathcal{O}_k) \sqcup S_k^\infty$, and let $\pi_1(\overline{X}_k)$ be the modified étale fundamental group of $\overline{X}_k$ defined by considering the Artin–Verdier topology over $\overline{X}_k$, which takes the real primes of k into account (cf. [Hir23, §2.1]). It is the Galois group of the maximal extension over k unramified at all finite and infinite primes.

Let A be a finite group with discrete topology, and c be a fixed cohomology class $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. Let $\mathrm{Hom}_c(\pi_1(\overline{X}_k), A)$ be the set of continuous homomorphisms from $\pi_1(\overline{X}_k)$ to A. For $\rho \in \mathrm{Hom}_c(\pi_1(\overline{X}_k), A)$, we define the mod n *arithmetic Chern–Simons invariant* $CS_c(\rho)$ by the image of c under the composition

$$H^3(A, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\rho^*} H^3(\pi_1(\overline{X}_k), \mathbb{Z}/n\mathbb{Z}) \xrightarrow{j} H^3(\overline{X}_k, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z},$$

where the cohomology group of $\overline{X}_k$ is the modified étale cohomology group defined in the Artin–Verdier topology, and j is the edge homomorphisms in the modified Hochschild–Serre spectral sequence

$$H^p(\pi_1(\overline{X}_k), H^q(\widetilde{\overline{X}}_k, \mathbb{Z}/n\mathbb{Z})) \Rightarrow H^{p+q}(\overline{X}_k, \mathbb{Z}/n\mathbb{Z}),$$

where $\widetilde{\overline{X}}_k = \varprojlim Y_i$, Y_i running over a finite Galois covering of $\overline{X}_k$ (cf. [Hir23, §2.2]). Note that the isomorphism $H^3(\overline{X}_k, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ depends on the choice of ζ_n.

We then define the mod n *arithmetic Dijkgraaf–Witten invariant* $Z_c(\overline{X}_k)$ of $\overline{X}_k$ by

$$Z_c(\overline{X}_k) := \frac{1}{\#A} \sum_{\rho \in \mathrm{Hom}_c(\pi_1(\overline{X}_k), A)} {\zeta_n}^{CS_c(\rho)}.$$

This definition differs from [Hir23] by a factor of $1/\#A$. In the following, we write simply Z_k for $Z_c(\overline{X}_k)$.

4 Mod 2 arithmetic Dijkgraaf–Witten invariants of real quadratic fields

4.1 Hirano's formula

In this section, we recall Hirano's formula for the mod 2 arithmetic Dijkgraaf–Witten invariant Z_k of real quadratic fields $k = \mathbb{Q}(\sqrt{p_1 \cdots p_r})$, where p_i's are distinct primes satisfying $p_i \equiv 1 \pmod 4$, and Ono's question.

We consider the case that $n = 2$ and $A = \mathbb{Z}/2\mathbb{Z}$. Let c be the unique non-trivial class in $H^3(A, \mathbb{Z}/2\mathbb{Z})$. We set

$$T := \{(x_1, \cdots, x_r) \in (\mathbb{Z}/2\mathbb{Z})^r \mid \sum_{i=1}^{r} x_i = 0\}$$

and $b_{ij} := (0, \cdots, 0, \overset{i}{\check{1}}, 0, \cdots, 0, \overset{j}{\check{1}}, 0, \cdots, 0) \in T$. Let $\mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$ be the abelian group of homomorphisms from T to $\mathbb{Z}/2\mathbb{Z}$. Then Hirano showed the following formula for the mod 2 Dijkgraaf–Witten invariants Z_k.

Theorem 4.1 ([Hir23, Corollary 4.2.4])**.** *We have*

$$Z_k = \frac{1}{2} \sum_{\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})} \left(\prod_{i<j} \left(\frac{p_i}{p_j} \right)^{\rho(b_{ij})} \right).$$

Ken Ono asked us the question, "Can we simplify the right-hand side of the formula in Theorem 4.1", and he suggested computing numerically the right-hand side for many examples of p_i's.

In the following, we shall compute the right-hand side of Hirano's formula in Theorem Theorem 4.1 and establish a simple formula, by introducing graphs attached to primes $p_1, \ldots, p_r$.

4.2 Preliminaries on graphs

In this section, we recall some basic notions on graphs, which will be used in the subsequent sections.

A *graph* G consists of two sets $V = V(G)$ and $E = E(G)$, where V is the set of *vertices* and E is the set of *edges*. The graph is denoted by $G = (V, E)$. The set E is regarded as a subset of the power set $\mathfrak{P}(V)$ consisting of 2-sets, $E \subset \{e \in \mathfrak{P}(V) \mid \#e =$

2}. We denote by e_{ij} ($= \{v_i, v_j\}$) the edge joining the vertices v_i and v_j. Here e_{ii} is not considered as an edge.

We say that $G' = (V', E')$ is a *subgraph* of $G = (V, E)$ if $V' \subset V$, $E' \subset E$, denoted by $G' \subset G$. Two graphs G and H are *isomorphic* if there is a bijection f between the vertex sets $V(G)$ and $V(H)$ such that any two vertices u and v of G are adjacent in G if and only if $f(u)$ and $f(v)$ are adjacent in H.

The *degree* of a vertex $v \in V$, denoted by $\deg(v)$, is the number of vertices that are adjacent to v. We say that v is an *even* (resp. *odd*) vertex if $\deg(v)$ is even (resp. odd), ($\deg(v) = 0$ included). We call a graph G an even (resp. odd) graph if all $v \in V$ are even (resp. odd).

A *path* is a graph $P = (V, E)$ of the form

$$V = \{v_0, v_1, \cdots, v_l\}, E = \{e_{01}, e_{12}, e_{23}, \cdots, e_{l-1,l}\},$$

where vertices $v_0, v_1, \ldots, v_l$ are distinct each other. This path P is denoted by $v_0 v_1 \cdots v_l$. A graph is *connected* if there exists a path between any two vertices in the graph. A graph with only one vertex is regarded as a connected graph. A maximal connected subgraph of a graph G is called a *connected component* of G.

A sequence $v_{i_1} e_{i_1 i_2} v_{i_2} \cdots v_{i_j} \cdots v_{i_{r-1}} e_{i_{r-1} i_r} v_{i_r}$ is called a *trail* in a graph, when vertices $v_{i_1}, \ldots, v_{i_r}$ and edges $e_{i_1 i_2}, \ldots, e_{i_{r-1} i_r}$ appear alternately and every edge appear exactly once, as in Figure 1 below. The path is an example of the trail. The first vertex v_{i_1}, the last vertex v_{i_r}, and the other vertices v_{i_j} of the trail are called the *starting vertex*, the *terminal vertex*, and *passing vertices*, respectively. When the starting vertex and the terminal vertex of a trail coincide, the trail is called a *circuit*. (In some references, it is called an *Euler tour*.) A graph G consisting of a single vertex is considered to be a circuit.

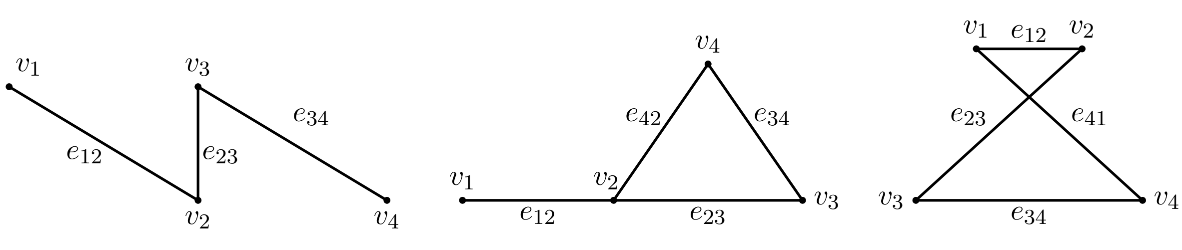


Figure 1: Examples for trails. The right one is a circuit.

The following is Euler's famous result concerning the classification of graphs that we will use later (cf. [Bol98, Chapter I, Theorem 12]).

Theorem 4.2 (Euler 1736)**.** *For a graph G, the following conditions are equivalent.*

(1) *Any connected component of G is a circuit.*

(2) *G is an even graph.*

4.3 Main theorem

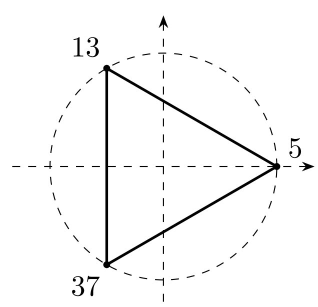
In this section, we introduce the quadratic residue graph associated to a finite set of prime numbers $p_1, \cdots, p_r \equiv 1 \pmod 4$, and we present the main theorem of this paper, which computes Hirano's formula explicitly. The contents of this chapter are based on [DKM23].

Let $S = \{p_1, p_2, \cdots, p_r\}$ be a finite set of distinct prime numbers, where $p_i \equiv 1 \pmod 4$ $(1 \le i \le r)$. We define the *quadratic residue graph* $G(S)$ associated to S by

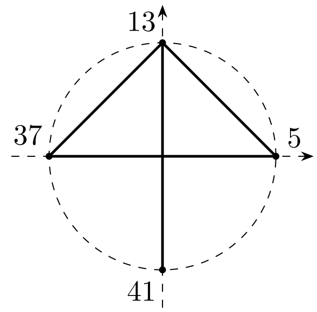
- $V = V(G(S)) = \{p_1, \ldots, p_r\}$.
- $E = E(G(S)) = \{e = \{p_i, p_j\} \in \mathfrak{P}(V) \mid \left(\frac{p_i}{p_j}\right) = -1\}$.

We can also illustrate the graph $G(S)$ as follows. We set primes $p_1, p_2, \cdots, p_r$ in order so that $p_1 < p_2 < \cdots < p_r$. Then, we put the vertices of $G(S)$ evenly on a unit circle counterclockwise starting at the point $(1, 0)$. Namely, the vertex $(\cos \frac{2\pi(i-1)}{r}, \sin \frac{2\pi(i-1)}{r})$ corresponds to the prime p_i, and we denote the vertices by p_i's. Then, two vertices p_i and p_j are linked (adjacent) if and only if $\left(\frac{p_i}{p_j}\right) = -1$ $(i \ne j)$. Since $p_i \equiv 1 \pmod 4$, the graph $G(S)$ is uniquely well-defined by the quadratic reciprocity.

Example 4.3. (1) $r = 3$, $S = \{5, 13, 37\}$.



(2) $r = 4, S = \{5, 13, 37, 41\}$.

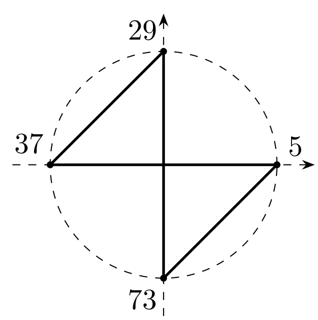


Many numerical examples are given in Appendix A, from which we find the following main theorem.

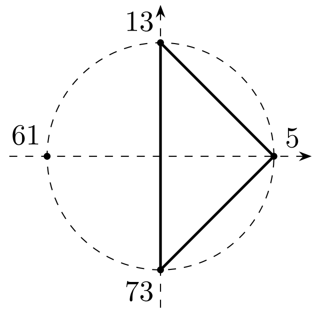
Theorem 4.4. *We have*

$$Z_k = \frac{1}{2} \sum_{\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})} \left(\prod_{i<j} \left(\frac{p_i}{p_j} \right)^{\rho(b_{ij})} \right)$$
$$= \begin{cases} 2^{r-2} & \text{if any connected component of } G(S) \text{ is a circuit,} \\ 0 & \text{if otherwise.} \end{cases}$$

Example 4.5. Let $S = \{5, 29, 37, 73\}$ so that $\left(\frac{5}{37}\right) = \left(\frac{5}{73}\right) = \left(\frac{29}{37}\right) = \left(\frac{29}{73}\right) = -1$, $\left(\frac{5}{29}\right) = \left(\frac{37}{73}\right) = 1$. Then the quadratic residue graph $G(S)$ is given by the following figure. Let $k = \mathbb{Q}(\sqrt{5 \cdot 29 \cdot 37 \cdot 73}) = \mathbb{Q}(\sqrt{391645})$. By Theorem 4.4, we have $Z_k = 2^2 = 4$.



Example 4.6. Let $S = \{5, 13, 61, 73\}$ so that $\left(\frac{5}{13}\right) = \left(\frac{5}{73}\right) = \left(\frac{13}{73}\right) = -1$, $\left(\frac{5}{61}\right) = \left(\frac{13}{61}\right) = \left(\frac{61}{73}\right) = 1$. Then the quadratic residue graph $G(S)$ is given by the following figure. Let $k = \mathbb{Q}(\sqrt{5 \cdot 13 \cdot 61 \cdot 73}) = \mathbb{Q}(\sqrt{289445})$. By Theorem 4.4, we have $Z_k = 2^2 = 4$.



4.4 Proof of the main theorem

We give a proof of Theorem 4.4 by using the orthogonality of characters of a finite abelian group. Throughout this section, we use the notations given in the previous sections.

Lemma 4.7. *Let $G(S)$ be the quadratic residue graph associated to $S = \{p_1, \cdots, p_r\}$, $p_i \equiv 1 \pmod 4$ $(1 \leq i \leq r)$. Then, $G(S)$ is an even graph if and only if*

$$\sum_{\{p_i,p_j\} \in E(G(S))} b_{ij} = \mathbf{0}.$$

Proof. By the definition of $b_{ij} \in T$, we easily see that

$$\sum_{\{p_i,p_j\} \in E(G(S))} b_{ij} = (\deg(p_i) \bmod 2)_{1 \leq i \leq r}.$$

Therefore, the right-hand side equals $\mathbf{0}$ if and only if $G(S)$ is an even graph. □

Next we recall that the following orthogonality of characters of a finite abelian group, (see, for example, [Ono90, Section 1.12].)

Lemma 4.8. *Let A be a finite abelian group of order n. Let $\chi : A \to \mathbb{C}^\times$ be a homomorphism (character of A). Then we have*

$$\sum_{a \in A} \chi(a) = \begin{cases} n & \text{if } \chi = \varepsilon, \\ 0 & \text{if } \chi \neq \varepsilon, \end{cases}$$

where ε is the identity character defined by $\varepsilon(a) = 1$ for any $a \in A$.

Now we define the map $\varphi : \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z}) \to \mathbb{C}^\times$ by

$$\varphi(\rho) := \prod_{i<j} \left(\frac{p_i}{p_j}\right)^{\rho(b_{ij})} \in \{\pm 1\}.$$

Since we have, for $\rho_1, \rho_2 \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$,

$$\varphi(\rho_1 + \rho_2) = \prod_{i<j} \left(\frac{p_i}{p_j}\right)^{\rho_1(b_{ij})+\rho_2(b_{ij})} = \varphi(\rho_1)\varphi(\rho_2),$$

φ is a homomorphism. By Lemma 4.8, we have

$$\sum_{\rho \in \mathrm{Hom}(T,\mathbb{Z}/2\mathbb{Z})} \varphi(\rho) = \begin{cases} 2^{r-1} & \text{if } \varphi = \varepsilon, \\ 0 & \text{if } \varphi \neq \varepsilon, \end{cases}$$

since the order of $\mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$ is 2^{r-1}.

Therefore, proving Theorem 4.4 is equivalent to showing the following theorem.

Theorem 4.9. *For a quadratic residue graph $G(S)$, the following conditions are equivalent.*

(1) $\varphi = \varepsilon$.

(2) *Any connected component of $G(S)$ is a circuit.*

Proof. Suppose that any connected component of $G(S)$ is a circuit. According to Lemma 4.7, we know that $\sum_{\{p_i,p_j\}\in E(G(S))} b_{ij} = \mathbf{0}$. For any $\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$,

$$\varphi(\rho) = \prod_{i<j} \left(\frac{p_i}{p_j}\right)^{\rho(b_{ij})} = \prod_{\{p_i,p_j\}\in E(G(S))} (-1)^{\rho(b_{ij})} = (-1)^{\sum_{\{p_i,p_j\}\in E(G(S))} \rho(b_{ij})}. \tag{4.1}$$

Since the exponent equals $\rho(\mathbf{0}) = 0$, we have $\varphi = \varepsilon$.

On the other hand, if $\varphi = \varepsilon$, then (4.1) implies that $\rho\left(\sum_{\{p_i,p_j\}\in E(G(S))} b_{ij}\right) = 0$ for any $\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$. Therefore, we have $\sum_{\{p_i,p_j\}\in E(G(S))} b_{ij} = \mathbf{0}$. By Lemma 4.7 again, the graph $G(S)$ is even and any connected component of $G(S)$ is a circuit. □

5 Mod 2 Dijkgraaf–Witten invariants for double covers of the 3-sphere

In this section, we give a topological counterpart of Theorem 4.4 for the mod 2 topological Dijkgraaf–Witten invariant for a double cover of the 3-sphere S^3 branched over a link (cf. [Hir23, §5]). Let M be a connected, oriented, and closed 3-manifold, and let n be an integer with $n \geq 2$. Let A be a finite group and let $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. We have $H_3(M, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ and we denote by $[M] \in H_3(M, \mathbb{Z}/n\mathbb{Z})$ the fundamental homology class of M.

According to Definition 2.2, Dijkgraaf–Witten invariant of M associated to c is

$$Z_c(M) = \frac{1}{\#A} \sum_{\rho \in \mathrm{Hom}(\pi_1(M), A)} \exp\left(\frac{2\pi i}{n} CS_c(\rho)\right).$$

We write simply Z_M for $Z_c(M)$.

Now consider the case where $A = \mathbb{Z}/2\mathbb{Z}$ and $c \in H^3(A, \mathbb{Z}/2\mathbb{Z})$ is the unique non-trivial class. Let $\mathcal{L} = \mathcal{K}_1 \cup \mathcal{K}_2 \cup \cdots \cup \mathcal{K}_r$ be a tame link in the 3-sphere S^3 and let $h : M \to S^3$ be the double covering ramified over $\mathcal{L}$ obtained by the unramified covering $Y \to X := S^3 \setminus \mathcal{L}$ corresponding to the kernel of the surjective homomorphism $H_1(X) \to \mathbb{Z}/2\mathbb{Z}$ that maps any meridian of $\mathcal{K}_i$ to $1 \in \mathbb{Z}/2\mathbb{Z}$.

Then Hirano showed the following formula for the mod 2 Dijkgraaf–Witten invariants of double covers of the 3-sphere.

Theorem 5.1 ([Hir23, Corollary 5.3.2])**.** *We have*

$$Z_M = \frac{1}{2} \sum_{\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})} \exp\left(\pi i \sum_{i<j} \rho\left(b_{ij}\right) \mathrm{lk}\left(\mathcal{K}_i, \mathcal{K}_j\right) \bmod 2\right),$$

where $\mathrm{lk}(\cdot, \cdot) \bmod 2$ *denotes the mod* 2 *linking number.*

Then, we define the *linking graph* $D_{\mathcal{L}}$ associated to $\mathcal{L}$ as follows.

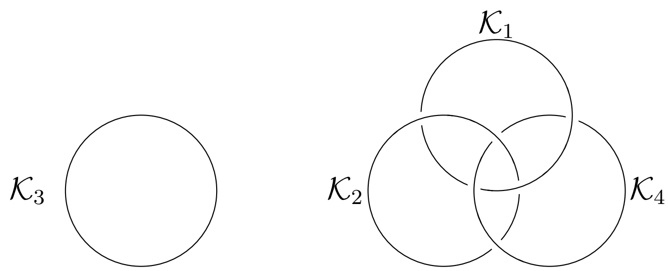
We arrange $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_r$ in counterclockwise order as vertices of the regular r-polygon. Two vertices $\mathcal{K}_i$ and $\mathcal{K}_j$ are linked (adjacent) if $\mathrm{lk}\left(\mathcal{K}_i, \mathcal{K}_j\right) \equiv 1 \bmod 2$. Since $\mathrm{lk}\left(\mathcal{K}_i, \mathcal{K}_j\right) = \mathrm{lk}\left(\mathcal{K}_j, \mathcal{K}_i\right)$, $D_{\mathcal{L}}$ is well-defined.

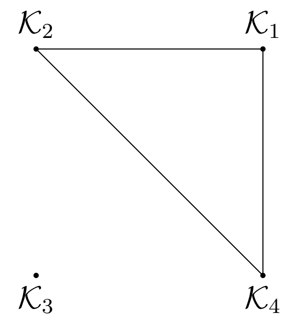
Then by the same method as in the arithmetic case, we have,

Theorem 5.2. *We have*

$$Z_M = \begin{cases} 2^{r-2} & \text{if any connected component of } D_{\mathcal{L}} \text{ is a circuit,} \\ 0 & \text{if otherwise.} \end{cases}$$

Example 5.3. Let $\mathcal{L} = \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3 \cup \mathcal{K}_4$ be the following link (left figure) in S^3 so that the linking graph $D_{\mathcal{L}}$ is given by the right figure. Let M be the double covering of S^3 ramified along $\mathcal{L}$. By Theorem 5.2, we have $Z_M = 2^2 = 4$.





6 A density formula for mod 2 arithmetic Dijkgraaf–Witten invariants

6.1 The number of quadratic residue graphs with r vertices

In this section, we calculate the number of quadratic residue graphs with r vertices ($r \geq 1$). Let $\mathfrak{G}_r$ the set of all graphs with the vertex set $V = \{1, 2, \ldots, r\}$, and $\mathfrak{C}_r$ be the subset of $\mathfrak{G}_r$ consisting of graphs whose connected components are all circuits. We recall by Theorem 4.2 that $\mathfrak{C}_r$ is the subset of $\mathfrak{G}_r$ consisting of even graphs. It is a crucial remark that, for instance, the graphs $G, G' \in \mathfrak{G}_3$, defined by $E(G) = \{\{1, 2\}, \{1, 3\}\}$, and $E(G') = \{\{1, 2\}, \{2, 3\}\}$, are isomorphic but are distinct in $\mathfrak{G}_3$.

Lemma 6.1. *We have* $\#\mathfrak{G}_r = 2^{\frac{r(r-1)}{2}}$.

Proof. For two distinct vertices v_i and v_j, there are 2 possible ways according that v_i and v_j are connected by an edge or not. Since there are $\binom{r}{2} = \frac{1}{2}r(r-1)$ ways for choosing 2 distinct vertices, the number of all graphs is $2^{\frac{r(r-1)}{2}}$. □

Lemma 6.2. *For any graph $G = (V, E)$, the number of odd vertices is even.*

Proof. Let $t := \sum_{v \in V} \deg(v)$. Then we have $t = 2 \cdot \#E$ and so t is even, from which the assertion follows. □

Theorem 6.3. *We have* $\#\mathfrak{C}_r = 2^{\frac{(r-1)(r-2)}{2}}$. *Hence*

$$\frac{\#\mathfrak{C}_r}{\#\mathfrak{G}_r} = \frac{1}{2^{r-1}}.$$

Proof. For $r = 1$, we have $\#\mathfrak{C}_1 = 1$. For any $r \geq 2$, we define a map $\gamma : \mathfrak{G}_{r-1} \to \mathfrak{C}_r$ as follows. For $G = (V, E) \in \mathfrak{G}_{r-1}$, $V(G) = \{1, 2, \cdots, r-1\}$, $E(G) \subseteq \{\{i, j\} \mid 1 \leqslant i, j \leqslant r, i \neq j\}$, we have $\gamma(V(G)) = \{1, 2, \cdots, r\}$, $\gamma(E(G)) = E(G) \cup \{\{s, r\} \mid \text{s is odd vertex in } G\}$. Because odd vertices always come in even numbers, we have $\gamma(G) \in \mathfrak{C}_r$.

To prove γ is injective, assuming $\gamma(G^1_{r-1}) = \gamma(G^2_{r-1})$. $G^1_{r-1}, G^2_{r-1} \in \mathfrak{G}_{r-1}$, meaning $\gamma(E(G^1_{r-1})) = \gamma(E(G^2_{r-1}))$. So $E(G^1_{r-1}) \cup \{\{s, r\} \mid \text{s is odd vertex in } G^1_{r-1}\} = E(G^2_{r-1}) \cup \{\{s, r\} \mid \text{s is odd vertex in } G^2_{r-1}\}$. Since the equality holds, all elements in the form of $\{*, r\}$ on both sides of the equation must be identical. So $\{\{s, r\} \mid \text{s is odd vertex in } G^1_{r-1}\} = \{\{s, r\} \mid \text{s is odd vertex in } G^2_{r-1}\}$. Thus $E(G^1_{r-1}) = E(G^2_{r-1})$. Since $V(G^1_{r-1}) = V(G^2_{r-1}) = \{1, 2, \cdots, r-1\}$, we have $G^1_{r-1} = G^2_{r-1}$, γ is injective.

To prove γ is surjective, let $G_r^0 \in \mathfrak{C}_r$. We need to find a $G_{r-1}^0 \in \mathfrak{G}_{r-1}$ such that $\gamma(G_{r-1}^0) = G_r^0$. Define $E(G_{r-1}^0)$ as the set obtained by removing all edges connected to the vertex r from $E(G_r^0)$. Combining $V(G_{r-1}^0) = \{1, 2, \cdots, r-1\}$, we have $G_{r-1}^0 = \{V(G_{r-1}^0), E(G_{r-1}^0)\} \in \mathfrak{G}_{r-1}$. So γ is surjective.

Since γ is bijective, we have $\#\mathfrak{C}_r = \#\mathfrak{G}_{r-1} = 2^{\frac{(r-1)(r-2)}{2}}$. □

6.2 The density formula for mod 2 arithmetic Dijkgraaf–Witten invariants and its proof

In this section, we propose a density formula for mod 2 arithmetic Dijkgraaf–Witten invariants, based on the properties of quadratic residue graphs. First, we prepare some notations. Let $\mathcal{P}$ be the set of all prime numbers and $\mathcal{P}_{\equiv b(a)}$ the subset defined by $\mathcal{P}_{\equiv b(a)} = \{p \in \mathcal{P} \mid p \equiv b \pmod a\}$. For a positive integer $r > 0$, we define $P_r(x) = \{\{p_1, \ldots, p_r\} \subset \mathcal{P}_{\equiv 1(4)} \cap [1, x] \mid p_i \neq p_j \ (i \neq j)\}$. Our objective is to calculate the natural density of mod 2 arithmetic Dijkgraaf–Witten invariants defined by

$$d_r := \lim_{x\to\infty} \frac{\#\{\{p_1, \ldots, p_r\} \in P_r(x) \mid Z_k = 2^{r-2}\}}{\#P_r(x)}.$$

Let $S_r(x) = \{\{p_1, \ldots, p_r\} \in P_r(x) \mid$ any connected component of $G(\{p_1, \ldots, p_r\})$ is a circuit$\}$, where $G(\{p_1, \ldots, p_r\})$ is the quadratic residue graph associated to $\{p_1, \ldots, p_r\}$. According to Theorem 4.2 and Theorem 4.4, the above density is also expressed as $d_r = \lim_{x\to\infty} \#S_r(x)/\#P_r(x)$. Since we have

$$\prod_{1\le j\le r}\left(1 + \prod_{\substack{1\le i\le r\\ i\neq j}} \left(\frac{p_i}{p_j}\right)\right) = \begin{cases} 2^r & \text{if } G(\{p_1, \ldots, p_r\}) \text{ is an even graph,} \\ 0 & \text{if otherwise,} \end{cases}$$

the number $\#S_r(x)$ is given by

$$\#S_r(x) = \frac{1}{2^r} \sum_{\{p_1,\ldots,p_r\}\in P_r(x)} \prod_{1\le j\le r}\left(1 + \prod_{\substack{1\le i\le r\\ i\neq j}} \left(\frac{p_i}{p_j}\right)\right).$$

Theorem 6.4. *The density d_r is given by*

$$d_r = \frac{1}{2^{r-1}} = \frac{\#\mathfrak{C}_r}{\#\mathfrak{G}_r}.$$

To prove this theorem, we begin by rephrasing the above counting formula for $\#S_r(x)$.

Lemma 6.5. *For any positive integer $r > 0$, we have*

$$\#S_r(x) = \frac{1}{2^r}\frac{1}{r!} \sum_{\substack{(p_1,\dots,p_r)\in(\mathcal{P}_{\equiv 1(4)}\cap[1,x])^r \\ p_i\neq p_j \ (i\neq j)}} \prod_{1\leq j\leq r} \left(1 + \prod_{\substack{1\leq i\leq r \\ i\neq j}} \left(\frac{p_i}{p_j}\right)\right).$$

Proof. The action of the symmetric group $\mathfrak{S}_r$ to the set

$$Q_r(x) := \{(p_1,\dots,p_r) \in (\mathcal{P}_{\equiv 1(4)} \cap [1,x])^r \mid p_i \neq p_j \ (i \neq j)\} \tag{6.1}$$

implies a natural $r!$ to 1 correspondence between $Q_r(x)$ and $P_r(x)$, which immediately gives the desired equation. □

Furthermore, the right-hand side can be expanded as follows.

$$\begin{aligned}
\#S_r(x) &= \frac{1}{2^r r!} \sum_{(p_1,\dots,p_r)\in Q_r(x)} \left(2 + \sum_{\substack{e_1,\dots,e_r\in\{0,1\} \\ 0<e_1+\cdots+e_r<r}} \left(\frac{\prod_{1\leq i\leq r} p_i^{e_i}}{\prod_{1\leq i\leq r} p_i^{1-e_i}}\right)\right) \\
&= \frac{\#Q_r(x)}{2^{r-1} r!} + \frac{1}{2^r r!} \sum_{\substack{e_1,\dots,e_r\in\{0,1\} \\ 0<e_1+\cdots+e_r<r}} \sum_{(p_1,\dots,p_r)\in Q_r(x)} \left(\frac{\prod_{1\leq i\leq r} p_i^{e_i}}{\prod_{1\leq i\leq r} p_i^{1-e_i}}\right),
\end{aligned}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol. To evaluate each term, we recall the following classical result (cf. [LeV56, Section 7-4]).

Proposition 6.6 (The prime number theorem for arithmetic progressions)**.** *For positive integers a and b with $(a,b) = 1$, the number $\pi_{a,b}(x) = \#(\mathcal{P}_{\equiv b(a)} \cap [1,x])$ satisfies*

$$\pi_{a,b}(x) \sim \frac{1}{\varphi(a)}\frac{x}{\log x}$$

as $x \to \infty$, where $\varphi(a)$ is the Euler function.

The estimation of the term $\#Q_r(x)$ immediately follows from the proposition. In fact, we have

$$\#Q_r(x) = \prod_{j=0}^{r-1}(\pi_{4,1}(x) - j) \sim \pi_{4,1}(x)^r \sim \frac{1}{2^r}\frac{x^r}{\log^r x}$$

as $x \to \infty$. To evaluate the remaining terms, a more detailed evaluation on Jacobi symbols is required.

Theorem 6.7 ([HB95, Theorem 1])**.** *For any $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ such that the following holds. Let M, N be positive integers, and let $a_1, \ldots, a_N$ be arbitrary complex numbers. Then*

$$\sum_{m\le M}^{*} \left| \sum_{n\le N}^{*} a_n \left(\frac{n}{m}\right) \right|^2 \le C_\varepsilon (MN)^\varepsilon (M+N) \sum_{n\le N}^{*} |a_n|^2,$$

where $\sum^*$ indicates restriction to positive odd square-free values and $\left(\frac{\cdot}{\cdot}\right)$ stands for the Jacobi symbol.

By symmetric properties, all we need to estimate are the following cases.

Lemma 6.8. *For any positive integer $0 < s < r$, we have*

$$E_s(x) := \sum_{(p_1,\ldots,p_r)\in Q_r(x)} \left(\frac{p_{s+1}\cdots p_r}{p_1\cdots p_s}\right) = o_r(\pi_{4,1}(x)^r)$$

as $x \to \infty$.

Proof. We define

$$a_m^{(s)}(x) = \begin{cases} s! & \text{if } m \text{ is a product of } s \text{ distinct primes in } \mathcal{P}_{\equiv 1(4)} \cap [1,x], \\ 0 & \text{otherwise} \end{cases}$$

and

$$b_m(x) = \begin{cases} \displaystyle\sum_{\substack{(p_{s+1},\ldots,p_r)\in(\mathcal{P}_{\equiv 1(4)}\cap[1,x])^{r-s} \\ p_i\ne p_j \ (i\ne j)}} \left(\frac{p_{s+1}\cdots p_r}{m}\right) & \text{if } m \text{ is square-free and odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Then we have $E_s(x) = \sum_{m\le x^s} a_m^{(s)}(x) b_m(x)$, where we change the variables via $m = p_1\cdots p_s$. By the Cauchy–Schwarz inequality,

$$\begin{aligned} E_s(x)^2 &\le \left(\sum_{m\le x^s} a_m^{(s)}(x)^2\right)\cdot\left(\sum_{m\le x^s} b_m(x)^2\right) \\ &\le (s!)^2 \pi_{4,1}(x)^s \sum_{m\le x^s}^{*} \left| \sum_{\substack{(p_{s+1},\ldots,p_r)\in(\mathcal{P}_{\equiv 1(4)}\cap[1,x])^{r-s} \\ p_i\ne p_j \ (i\ne j)}} \left(\frac{p_{s+1}\cdots p_r}{m}\right) \right|^2 \end{aligned}$$

$$= (s!)^2 \pi_{4,1}(x)^s \sideset{}{^*}\sum_{m \le x^s} \left| \sideset{}{^*}\sum_{n \le x^{r-s}} a_n^{(r-s)}(x) \left(\frac{n}{m}\right) \right|^2,$$

where we change the variables via $n = p_{s+1} \cdots p_r$. Therefore, by applying Theorem 6.7, we obtain

$$\begin{aligned} E_s(x)^2 &\ll_{r,\varepsilon} \pi_{4,1}(x)^s x^{r\varepsilon}(x^s + x^{r-s}) \sideset{}{^*}\sum_{n \le x^{r-s}} |a_n^{(r-s)}(x)|^2 \\ &\ll_{r,\varepsilon} \pi_{4,1}(x)^s x^{r\varepsilon + r - 1} \pi_{4,1}(x)^{r-s}, \end{aligned}$$

which implies $E_s(x) \ll_{r,\varepsilon} x^{(r\varepsilon+r-1)/2} \pi_{4,1}(x)^{r/2}$. By taking $0 < \varepsilon < 1/2r$, we have $E_s(x) = o_r(\pi_{4,1}(x)^r)$. □

In conclusion, we have

$$\#S_r(x) = \frac{\#Q_r(x)}{2^{r-1} r!} + o_r(\pi_{4,1}(x)^r) \sim \frac{\pi_{4,1}(x)^r}{2^{r-1} r!}$$

as $x \to \infty$. Since $\#P_r(x) = \binom{\pi_{4,1}(x)}{r} \sim \pi_{4,1}(x)^r / r!$, we conclude the proof of Theorem 6.4.

References

[Bol98] B. Bollobás, *Modern graph theory*, Graduate Texts in Mathematics, vol. 184, Springer-Verlag, New York, 1998.

[DKM23] Y. Deng, R. Kurimaru and T. Matsusaka, *Arithmetic Dijkgraaf–Witten invariants of real quadratic fields, quadratic residue graphs, and density formulas*, Research in Number Theory, **9**, 70 (2023).

[DW90] R. Dijkgraaf and E. Witten, *Topological gauge theories and group cohomology*, Comm. Math. Phys., **129** (1990), no. 2, 393–429.

[HB95] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), no. 3, 235–275.

[Hir23] H. Hirano, *On mod* 2 *arithmetic Dijkgraaf–Witten invariants for certain real quadratic number fields*, Osaka J. Math., **60** (2023) no. 4, 933–954.

[Kim20] M. Kim, *Arithmetic Chern-Simons theory I*, Galois covers, Grothendieck-Teichmüller Theory and Dessins d'Enfants, Springer Proc. Math. Stat., vol. 330, Springer, Cham, [2020] ©2020, pp. 155–180.

[LeV56] W. J. LeVeque, *Topics in number theory. Vol.* 2, Addison-Wesley Publishing Co., Inc., Reading, Mass., 1956.

[LP23] J. Lee and J. Park, *Arithmetic Chern-Simons theory with real places*, J. Knot Theory Ramifications, Vol. **32**, No. 4, 2350027 (2023).

[Maz73] B. Mazur, *Notes on étale cohomology of number fields*, Ann. Sci. École Norm. Sup. (4) **6** (1973), 521–552 (1974).

[Mor24] M. Morishita, *Knots and primes*, An introduction to arithmetic topology, 2nd edition, Universitext, Springer, 2024.

[Ono90] T. Ono, *An introduction to algebraic number theory*, The University Series in Mathematics, Plenum Press, New York, 1990, Translated from the second Japanese edition by the author.

A Appendix: Some numerical examples of Z_k

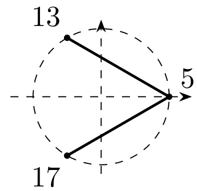
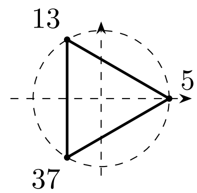
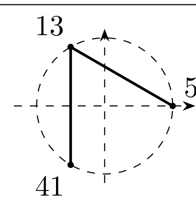
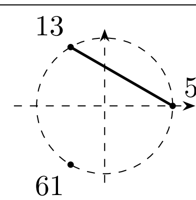
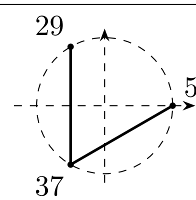
We give numerical computer calculations for Hirano's formula,

$$Z_k = \frac{1}{2} \sum_{\rho \in \mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})} \left(\prod_{i<j} \left(\frac{p_i}{p_j} \right)^{\rho(b_{ij})} \right).$$

The case that $r = 3$

We define ρ_0, ρ_1, ρ_2, and ρ_3 in $\mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$ by

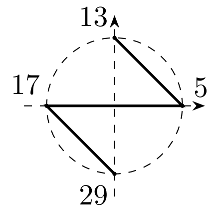
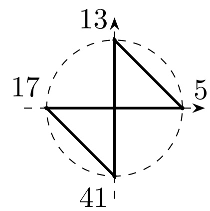
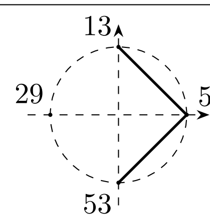
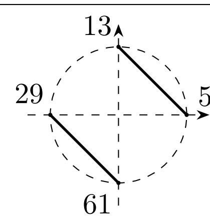
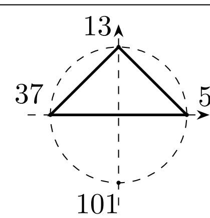
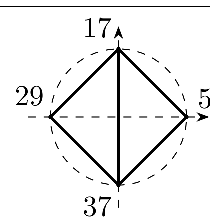
x	$(0,0,0)$	$(1,1,0)$	$(0,1,1)$	$(1,0,1)$
$\rho_0(x)$	0	0	0	0
$\rho_1(x)$	0	1	0	1
$\rho_2(x)$	0	0	1	1
$\rho_3(x)$	0	1	1	0

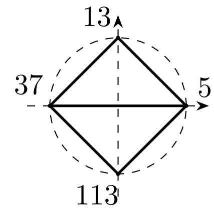
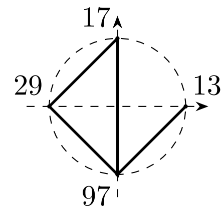
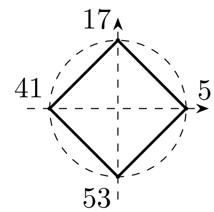
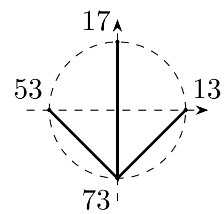
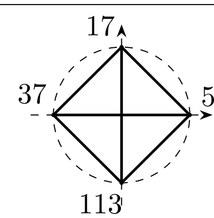
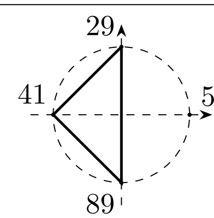
A set of prime numbers S	Quadratic residue graph	Z_k
5 , 13 , 17		0
5 , 13 , 37		2
5 , 13 , 41		0
5 , 13 , 61		0
5 , 29 , 37		0

The case that $r = 4$

We define $\rho_0, \rho_1, \ldots, \rho_7$ in $\mathrm{Hom}(T, \mathbb{Z}/2\mathbb{Z})$ by

x	$(0,0,0,0)$	$(1,1,0,0)$	$(1,0,1,0)$	$(1,0,0,1)$	$(0,1,1,0)$	$(0,1,0,1)$	$(0,0,1,1)$	$(1,1,1,1)$
$\rho_0(x)$	0	0	0	0	0	0	0	0
$\rho_1(x)$	0	1	0	0	1	1	0	1
$\rho_2(x)$	0	0	1	0	1	0	1	1
$\rho_3(x)$	0	0	0	1	0	1	1	1
$\rho_4(x)$	0	1	1	0	0	1	1	0
$\rho_5(x)$	0	1	0	1	1	0	1	0
$\rho_6(x)$	0	0	1	1	1	1	0	0
$\rho_7(x)$	0	1	1	1	0	0	0	1

A set of prime numbers S	Quadratic residue graph	Z_k
5 , 13 , 17 , 29		0
5 , 13 , 17 , 41		4
5 , 13 , 29 , 53		0
5 , 13 , 29 , 61		0
5 , 13 , 37 , 101		4
5 , 17 , 29 , 37		0

A set of prime numbers S	Quadratic residue graph	Z_k
5 , 13 , 37 , 113		0
13 , 17 , 29 , 97		0
5 , 17 , 41 , 53		4
13 , 17 , 53 , 73		0
5 , 17 , 37 , 113		0
5 , 29 , 41 , 89		4