Indicators of Tambara–Yamagami categories and Gauss sums

Tathagata Basak and Ryan Johnson
Indicators of Tambara–Yamagami categories and Gauss sums

Tathagata Basak and Ryan Johnson

We prove that the higher Frobenius–Schur indicators, introduced by Ng and Schauenburg, give a strong-enough invariant to distinguish between any two Tambara–Yamagami fusion categories. Our proofs are based on computation of the higher indicators in terms of Gauss sums for certain quadratic forms on finite abelian groups and rely on the classification of quadratic forms on finite abelian groups, due to Wall.

As a corollary to our work, we show that the state-sum invariants of a Tambara–Yamagami category determine the category as long as we restrict to Tambara–Yamagami categories coming from groups $G$ whose order is not a power of 2. Turaev and Vainerman proved this result under the assumption that $G$ has odd order, and they conjectured that a similar result should hold for groups of even order. We also give an example to show that the assumption that $|G|$ is not a power of 2 cannot be completely relaxed.

1. Introduction

Fusion categories (see [Etingof et al. 2005]) occur in various branches of mathematics: low-dimensional topology, subfactors, and quantum groups, to name a few. Classification of fusion categories, although currently out of reach in general, is a main driving question in the area. A natural method for classifying objects in mathematics is via numerical invariants. Ng and Schauenburg [2007b] introduced a class of invariants of spherical pivotal fusion categories (to be simply called spherical categories) called the higher Frobenius–Schur indicators. Let $C$ denote a spherical category. For each simple object $V$ of $C$ and each integer $k \geq 1$, Ng and Schauenburg define a complex number $\nu_k(V)$, called the $k$-th indicator of $V$. These build on and generalize many previous works, e.g., [Bantay 1997; Fuchs et al. 1999; Fuchs and Schweigert 2003; Kashina et al. 2006; Linchenko and Montgomery 2000; Mason and Ng 2005]; we refer the reader to the introduction of [Ng and Schauenburg 2007b] for more details. For $k = 2$, these invariants

MSC2010: primary 18D10; secondary 15A63, 11L05, 57M27.
Keywords: fusion category, Tambara–Yamagami category, Frobenius–Schur indicator, discriminant form, quadratic form, Gauss sum.
generalize the classical Frobenius–Schur indicator of a finite group representation. The Frobenius–Schur indicators of the simple objects of $C$ can be used to define the Frobenius–Schur exponent of $C$, denoted $\text{FSexp}(C)$. When $C$ is the representation category of a quasi-Hopf algebra, $\text{FSexp}(C)$ is equal to $\exp(C)$ or $2\exp(C)$ [Ng and Schauenburg 2007a, Theorem 6.2] where $\exp(C)$ denotes the exponent of $C$ in the sense of Etingof et al. (see [Etingof 2002] and its references).

The higher indicators are powerful tools for studying pivotal categories. For example, they were used in [Ng and Schauenburg 2010] to prove that the projective representation of $\text{SL}_2(\mathbb{Z})$ obtained from a modular tensor category factors through a finite quotient $\text{SL}_2(\mathbb{Z}/n\mathbb{Z})$ for some $n$. In this article, we demonstrate that the numbers $\nu_k(V)$, as $k$ varies over natural numbers and $V$ varies over the set of simple objects of $C$, give a strong-enough numerical invariant of $C$ that is able to distinguish between any two spherical categories in an interesting class, known as Tambara–Yamagami categories (TY-categories for short).

Susan Montgomery has asked whether the FS-indicators of a semisimple Hopf algebra determine the tensor category of its representations. This was shown to be true for the class of semisimple Hopf algebras of dimension 8 in [Ng and Schauenburg 2008]. The representation categories of these Hopf algebras are TY-categories. Kashina et al. [2012] showed that, for the class of nonsemisimple Hopf algebras called Taft algebras, the second indicator can distinguish between the finite tensor categories of their representations. Along similar lines, Siu-Hung Ng (private communication) has asked whether a spherical fusion category generated by a simple object is completely determined by its FS-indicators. Our results give an affirmative answer to this question for the class of TY-categories.

Let $G$ be a finite group. Let $S$ be a finite set that contains $G$ and one extra element, denoted $m$. Consider the following fusion rule on $S$:

$$g \otimes h = gh, \quad m \otimes g = g \otimes m = m, \quad m \otimes m = \bigoplus_{x \in G} x$$

for all $g, h \in G$.

Tambara and Yamagami [1998] classified all fusion categories that have the above fusion rule; for a conceptual proof of this classification, see [Etingof et al. 2010, Example 9.4]. Such fusion categories exist only if $G$ is abelian and are classified by pairs $(\chi, \tau)$ where $\chi : G \times G \rightarrow \mathbb{C}^\times$ is a nondegenerate symmetric bicharacter on $G$ and $\tau$ is a square root of $|G|^{-1}$. For each tuple $(G, \chi, \tau)$ as above, there exists a spherical category, denoted $\text{TY}(G, \chi, \tau)$. Two TY-categories $\mathcal{C} = \text{TY}(G, \chi, \tau)$ and $\mathcal{C}' = \text{TY}(G', \chi', \tau')$ are isomorphic as spherical categories if and only if $\tau = \tau'$ and $(G, \chi) \simeq (G', \chi')$, that is, there exists an isomorphism $f : G \rightarrow G'$ such that $\chi'(f(x), f(y)) = \chi(x, y)$ for all $x, y \in G$. Let $\text{Irr}(\mathcal{C}) = G \cup \{m_\mathcal{C}\}$ be the simple objects of $\mathcal{C}$. There is a canonical (spherical) pivotal structure on $\mathcal{C}$ such that the pivotal dimension of an object matches the Frobenius–Perron dimension. For an
Indicators of Tambara–Yamagami categories and Gauss sums

object $V$ of $C$, let $\text{pdim}(V)$ denote its pivotal dimension for this canonical pivotal structure.

We shall prove the following theorem:

**Theorem 1.1.** Let $C$ and $C'$ be two TY-categories. If

$$\sum_{V \in \text{Irr}(C)} v_k(V) = \sum_{V \in \text{Irr}(C')} v_k(V),$$

$$\sum_{V \in \text{Irr}(C)} \text{pdim}(V) v_k(V) = \sum_{V \in \text{Irr}(C')} \text{pdim}(V) v_k(V)$$

for all $k \geq 1$, then $C \simeq C'$ as spherical fusion categories.

Now we shall describe our plan for the proof of this theorem and give a summary of contents of the sections. Let $C = \text{TY}(G, \chi, \tau)$ and $C' = \text{TY}(G', \chi', \tau')$ be two TY-categories. Assuming $G$ and $G'$ are nontrivial groups, the assumptions of Theorem 1.1 are quickly seen to be equivalent to $v_k(m_C) = v_k(m_{C'})$ and $\sum_{x \in G} v_k(x) = \sum_{x \in G'} v_k(x)$. Based on work done in [Shimizu 2011], we can easily conclude that $G \simeq G'$ and $\tau = \tau'$.

Most of our work goes into showing that, if $v_k(m_C) = v_k(m_{C'})$ for all $k$, then $(G, \chi) \simeq (G', \chi')$. Shimizu [2011, Theorems 3.3 and 3.4] calculated $v_k(m_C)$ using an expression for the indicator in terms of the twist of the Drinfeld center of $C$ [Ng and Schauenburg 2007a, Theorem 4.1].

This project started for us when Siu-Hung Ng asked us whether the 8-th root of unity in [Shimizu 2011, Theorem 3.5] is related to the signature modulo 8 for some related lattice. This indeed turns out to be the case. A simple restatement of Shimizu’s result gives us a formula relating the indicators $v_{2k}(m_C)$ to certain quadratic Gauss sums; see Lemma 4.1. This formula is the starting point for our calculations, and we want to explain it in precise terms. For this, we need some notation.

Let $G$ be an abelian group, always written additively in this paper unless otherwise stated. Let $q : G \to \mathbb{Q}/\mathbb{Z}$ be a quadratic form on $G$. Given a pair $(G, q)$, one defines the associated quadratic Gauss sum

$$\Theta(G, q) = |G|^{-1/2} \sum_{x \in G} e(q(x)), \quad \text{where } e(x) = e^{2\pi i x}. \quad (1)$$

For $k \in \mathbb{Z}$, it will be also convenient to define the invariant

$$\xi_k(G, q) = \Theta(G, q)^k \Theta(G, -k \cdot q). \quad (2)$$

Let $C = \text{TY}(G, \chi, \tau)$ be a TY-category where $(G, \chi, \tau)$ is a triple as above. We choose a quadratic form $q$ on $G$ such that $\chi(x, y) = e(-\partial q(x, y))$ where $\partial q : G \times G \to \mathbb{Q}/\mathbb{Z}$ denotes the symmetric $\mathbb{Z}$-bilinear form

$$\partial q(x, y) = q(x + y) - q(x) - q(y). \quad (3)$$
One can show that such a \( q \) always exists. In Lemma 4.1, we prove that for \( k \geq 1 \)
\[
v_{2k}(m_C) = \text{sign}(\tau)^k \xi_k(G, q).
\]

Much of the calculation in Sections 3 and 5 is geared towards finding explicit formulae for \( \xi_k(G, q) \) by using the classification of the irreducible quadratic forms and the known values of Gauss sums of these irreducible forms. The calculations are more complicated when \( G \) is a 2-group, which is a well known feature in the theory of quadratic forms on finite abelian groups. When \( G \) is a 2-group, and \( v_2(k) \) (the two-valuation of \( k \)) is at least 1, we relate \( \xi_k(G, q) \) to an invariant \( \sigma_{v_2(k)}(\partial q) \) of the pair \((G, \partial q)\) (see Lemma 3.8). The invariant \( \sigma_n(\partial q) \) is a generalization of the Kervaire–Brown–Peterson–Browder invariant [Brown 1972; Kawauchi and Kojima 1980, p. 33]. Detailed calculation of the values of the Gauss sums and properties of the invariant \( \sigma_n(\partial q) \) lets us conclude that the bicharacter \( \chi \) can be recovered from values of the Gauss sums, thus proving our theorem.

Sections 2 through 4 contain preparatory material. In Section 2, we collect the background material necessary for quadratic and bilinear forms on finite abelian groups and their classification. The results here are mostly due to C. T. C. Wall [1963]; also see [Miranda 1984; Kawauchi and Kojima 1980; Nikulin 1979], wherein the proofs can be found. However, we have chosen to include the proofs of most of what we need in the detailed Appendix. In particular, we give a proof of the existence part of Wall’s theorem (see Theorem 2.1) on the classification of nondegenerate quadratic and bilinear forms on finite abelian groups. We have explained our reason for including the Appendix in Section 2, following the statement of Theorem 2.1.

Section 3 contains the background on values of Gauss sums and calculation of \( \xi_k(G, q) \) in various cases. Section 4 introduces the TY-categories and relates the indicator values \( v_{2k}(C) \) with Gauss sums. With these preparations, we prove Theorem 1.1 in Section 5.

Finally, in Section 6, we apply Theorem 1.1 to address a recent conjecture [Turaev and Vainerman 2012] regarding 3-manifold invariants constructed from TY-categories. Given a compact 3-manifold \( M \) and a spherical category \( C \), one can define an invariant \( |M|_C \), called the state-sum invariant in that paper. Turaev and Virelizier [2013] showed that \( |M|_C = \tau_{Z(C)}(M) \), where \( Z(C) \) is the Drinfeld center of \( C \) and \( \tau_{Z(C)}(M) \) denotes the Reshetikhin–Turaev invariant. For \( k \geq 1 \), let \( L_{k,1} = \{(z_1, z_2) \in \mathbb{C}^2 : |z_1|^2 + |z_2|^2 = 1\}/\langle(z_1, z_2) \sim e^{2\pi i/k}(z_1, z_2)\rangle \) denote the lens spaces. In Theorem 6.3, we show that a TY-category \( C = \text{TY}(G, \chi, \tau) \) is determined by the sequence of state-sum invariants \( \{|L_{k,1}|_C : k \geq 1\} \) as long as we restrict to categories such that \( |G| \) has an odd factor. Turaev and Vainerman proved this result assuming that \( |G| \) is odd and conjectured that a similar result should hold for groups of even order. In Section 6, we exhibit two nonisomorphic
tuples \((G, \chi, \tau)\) and \((G', \chi', \tau')\) such that \(|L_{k,1}|_{TY(G, \chi, \tau)} = |L_{k,1}|_{TY(G', \chi', \tau')}\) for all \(k\). In our example, both \(G\) and \(G'\) have order 64. This example demonstrates that one needs to put some hypothesis on the possible orders of \(G\) or else consider state-sum invariants of other 3-manifolds if one has to recover the category from the data of these invariants.

Quadratic and bilinear forms on finite abelian groups appear in various places in topology and geometry. We give some examples:

- The “torsion linking pairing” on the torsion part of the \(n\)-th integral homology of a \((2n+1)\)-dimensional real compact manifold coming from Poincaré duality and intersection pairing, for example [Kawauchi and Kojima 1980]. For 3-manifolds, we get a pairing on the torsion 1-cycles related to the linking number. For this reason, discriminant forms are called linking pairs in that paper.
- Intersection pairing on the torsion part of middle cohomology of a \((4n+2)\)-dimensional manifold and computation of Kervaire–Arf invariants [Brown 1972].
- Study of integral lattices coming from algebraic geometry, for example study of \(K_3\) surfaces [Nikulin 1979]. Let \(G\) be a finite abelian group and \(b\) be a nondegenerate symmetric bilinear form on \(G\). For each pair \((G, b)\), there exists a pair \((L, B)\), where \(L \cong \mathbb{Z}^n\) and \(B : L \times L \to \mathbb{Z}\) is a nondegenerate symmetric \(\mathbb{Z}\)-bilinear form such that \(G = L'/L\) and \(b\) is the \(\mathbb{Q}/\mathbb{Z}\) valued form induced on \(L'/L\) by \(B\); here \(L'\) denotes the dual lattice of \(L\). For this reason, we have borrowed the name “discriminant form” from [Nikulin 1979] for pairs \((G, b)\).

We hope that the methods of calculation of Gauss sums will have other uses in computations of Gauss sums coming from the above sources.

2. Bilinear and quadratic forms on finite abelian groups

Definitions. Let \(G\) be a finite abelian group (written additively). Let \(\exp(G)\) denote the exponent of \(G\). A discriminant form is a pair \((G, b)\) where \(G\) is a finite abelian group and \(b : G \times G \to \mathbb{Q}/\mathbb{Z}\) is a symmetric bilinear form on \(G\). As all the bilinear forms considered in this article are symmetric, the adjective “symmetric” will sometimes be dropped. Say that \(b\) or \((G, b)\) is nondegenerate if for each nonzero \(x \in G\) there exists \(y \in G\) such that \(b(x, y) \neq 0\).

Let \(G\) be a finite abelian group and \(q\) be a quadratic form on \(G\). We say that the pair \((G, q)\) is a premetric group. We say that \(q\) is nondegenerate and \((G, q)\) is a metric group if the bilinear form \(\partial q\) (see (3)) is nondegenerate.

The morphisms in the categories of discriminant forms and premetric groups are defined as usual. Isomorphisms are often called isometries. There is an obvious notion of an orthogonal direct sum on discriminant forms and premetric groups.
If \((G_1, q_1)\) and \((G_2, q_2)\) are two premetric groups, we let \((G_1, q_1) \perp (G_2, q_2)\) denote their orthogonal direct sum. The map \((G, q) \mapsto (G, \partial q)\) defines a functor from the category of premetric or metric groups to the category of discriminant or nondegenerate discriminant forms, respectively.

**Remark.** Let \(G\) be a finite abelian group. Note that a bilinear form on \(G\) takes values in \(\exp(G)^{-1} \mathbb{Z}/\mathbb{Z}\). Let \((G, q)\) be a premetric group. Let \(a \in G\). Note that \(\partial q(a, a) = 2q(a)\), and so \(q\) takes value in \((2 \exp(G))^{-1} \mathbb{Z}/\mathbb{Z}\). If \(G\) has odd order, then \(a = 2(\frac{1}{2}(\exp(G) + 1))a\). So \(q(a) = \frac{1}{2}(\exp(G) + 1)\partial q(a, a)\). Hence, \(q\) actually takes values in \(\exp(G)^{-1} \mathbb{Z}/\mathbb{Z}\) and \(\partial q\) determines \(q\). But this fails for groups of even order. For example, consider the nondegenerate bilinear form on \(\mathbb{Z}/4\mathbb{Z}\) given by \(b(x, y) = xy/4\). Then \(q(x) = x^2/8\) and \(q'(x) = 5x^2/8\) are two distinct quadratic forms on \(\mathbb{Z}/4\mathbb{Z}\) such that \(\partial q = \partial q' = b\).

**Definitions.** Let \(p\) be a prime. If \(a\) is a rational number, \(v_p(a)\) will denote the \(p\)-valuation of \(a\). It will be convenient to extend the definition of \(p\)-valuation as follows. Let \(G\) be an abelian \(p\)-group. Define \(v_p : G \to \mathbb{Z}_{\leq 0} \cup \{\infty\}\) by \(v_p(x) = -\log_p(\text{order}(x))\) if \(x\) is a nonzero element of \(G\), and \(v_p(0) = \infty\). We say that \(v_p(x)\) is the \(p\)-valuation of \(x\).

This definition of \(p\)-valuation is useful to us because of the following example. Let \(\mathbb{Q}_{(p)}\) be the ring of all rational numbers of the form \(m/p^r\) where \(m \in \mathbb{Z}\) and \(r \in \mathbb{Z}_{\geq 0}\). If \((G, q)\) is a premetric \(p\)-group, then observe that \(q\) and \(\partial q\) take values in the \(\mathbb{Z}\)-module \(\mathbb{Q}_{(p)}/\mathbb{Z}\). If \(\alpha\) is a nonzero element of \(\mathbb{Q}_{(p)}/\mathbb{Z}\), then it can be written as \(p^{-n}a\) for some \(a \in \mathbb{Z}\) relatively prime to \(p\). One has \(v_p(\alpha) = -n\).

Let \((G, b)\) be a discriminant form. Let \(e_1, \ldots, e_k \in G\) and \(b_{ij} = b(e_i, e_j)\). The matrix \(B = (b_{ij})\) is called the Gram matrix of \(e_1, \ldots, e_k\). We shall write \(\text{Gram}_b(e_1, \ldots, e_n) = B\). One has

\[
b\left(\sum_i g_i e_i, \sum_j h_j e_j\right) = (g_1, \ldots, g_k)B(h_1, \ldots, h_k)^\text{tr}, \quad g_1, \ldots, g_k, h_1, \ldots, h_k \in \mathbb{Z}.
\]

A discriminant form or premetric group is called irreducible if it cannot be written as an orthogonal direct sum of two nonzero discriminant forms or premetric groups, respectively. A finite abelian group is homogeneous if it is isomorphic to \((\mathbb{Z}/p^r\mathbb{Z})^n\) for some prime \(p\) and positive integers \(r\) and \(n\). For a \(p\)-group \(G\), we let \(\text{rk}(G)\) denote the minimum number of generators for \(G\) or equivalently \(\dim_{\mathbb{F}_p}(G/\Phi(G))\) where \(\Phi(G)\) is the Frattini subgroup of \(G\). In particular,

\[
\text{rk}((\mathbb{Z}/p^r\mathbb{Z})^n) = n.
\]

An element of \((\mathbb{Z}/p^r\mathbb{Z})^n\) will often be written as a vector whose entries come from \(\mathbb{Z}/p^r\mathbb{Z}\). A discriminant form on a homogeneous finite abelian group will be often written as \(((\mathbb{Z}/p^r\mathbb{Z})^n, B)\) where \(B\) is an \(n \times n\) matrix with entries in \(p^{-r}\mathbb{Z}/\mathbb{Z}\).
Theorem 2.1 [Wall 1963; Miranda 1984; Nikulin 1979]. (a) Theorem 2.1

decompose (is an orthogonal direct sum of

Sylow subgroup of G known to experts, but we have not seen it in the literature.

Proofs in the references above, and we believe it is simpler. It is probably well

abelian group G

groups (p

u

b

such that

Each metric group is an orthogonal direct sum of the irreducible metric groups

Let

denote a quadratic nonresidue modulo

Let

A proof of Theorem 2.1 has been sketched in the Appendix. Here we shall only

It follows that there exists a quadratic form q on G such that

such that

b(x, y) = xBy^{lr} for all x, y ∈ (Z/p^rZ)^n. Let p be an odd prime and

u_p denote a quadratic nonresidue modulo p. Table 1 lists the irreducible metric
groups (G, q) and corresponding irreducible discriminant forms (G, δq).

<table>
<thead>
<tr>
<th>name in [Miranda 1984]</th>
<th>(G, q)</th>
<th>(G, δq)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_{p^r}</td>
<td>( \left( \mathbb{Z}/p^r \mathbb{Z}, q(x) = \frac{(p^r+1)/2}{p^r} x^2 \right) )</td>
<td>( \mathbb{Z}/p^r \mathbb{Z}, \frac{1}{p^r} )</td>
</tr>
<tr>
<td>B_{p^r}</td>
<td>( \left( \mathbb{Z}/p^r \mathbb{Z}, q(x) = \frac{u_p(p^r+1)/2}{p^r} x^2 \right) )</td>
<td>( \mathbb{Z}/p^r \mathbb{Z}, \frac{u_p}{p^r} )</td>
</tr>
<tr>
<td>A_2^r</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}, q(x) = \frac{1}{2^{r+1}} x^2 \right) )</td>
<td>( \mathbb{Z}/2^r \mathbb{Z}, \frac{1}{2^r} )</td>
</tr>
<tr>
<td>B_2^r</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}, q(x) = \frac{-1}{2^{r+1}} x^2 \right) )</td>
<td>( \mathbb{Z}/2^r \mathbb{Z}, -\frac{1}{2^r} )</td>
</tr>
<tr>
<td>C_2^r</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}, q(x) = \frac{5}{2^{r+1}} x^2 \right) )</td>
<td>( \mathbb{Z}/2^r \mathbb{Z}, \frac{5}{2^r} )</td>
</tr>
<tr>
<td>D_2^r</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}, q(x) = \frac{-5}{2^{r+1}} x^2 \right) )</td>
<td>( \mathbb{Z}/2^r \mathbb{Z}, -\frac{5}{2^r} )</td>
</tr>
<tr>
<td>E_{2^r}</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}^2, q(x_1, x_2) = \frac{x_1 x_2}{2^r} \right) )</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}^2, \left( \begin{smallmatrix} 0 &amp; 2^{-r} \ 2^{-r} &amp; 0 \end{smallmatrix} \right) \right) )</td>
</tr>
<tr>
<td>F_{2^r}</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}^2, q(x_1, x_2) = \frac{x_1^2 + x_1 x_2 + x_2^2}{2^r} \right) )</td>
<td>( \left( \mathbb{Z}/2^r \mathbb{Z}^2, \left( \begin{smallmatrix} 1 - r &amp; 2^{-r} \ 2^{-r} &amp; 2^{-r} \end{smallmatrix} \right) \right) )</td>
</tr>
</tbody>
</table>

Table 1. Irreducible quadratic and symmetric bilinear forms. In the first two rows, \( p \) represents an odd prime. For the prime 2 and for \( r = 1 \) or 2, some of the forms above are isometric. For example, \( A_2 \simeq C_2 \).

(b) Each metric group is an orthogonal direct sum of the irreducible metric groups

listed in Table 1.

It follows that, given any nondegenerate symmetric bilinear form \( b \) on a finite

abelian group \( G \), there exists a quadratic form \( q \) on \( G \) such that \( \delta q = b \).

A proof of Theorem 2.1 has been sketched in the Appendix. Here we shall only give a brief indication of our argument. This argument seems to be different from the proofs in the references above, and we believe it is simpler. It is probably well known to experts, but we have not seen it in the literature.

Let \( (G, b) \) be a discriminant form. Write \( G = \bigoplus_p G_{(p)} \) where \( G_{(p)} \) is the \( p \)-Sylow subgroup of \( G \). Let \( b_{(p)} \) be the restriction of \( b \) to \( G_{(p)} \times G_{(p)} \). Clearly \( (G, b) \) is an orthogonal direct sum of \( (G_{(p)}, b_{(p)}) \) as \( p \) varies over primes. So it suffices to decompose \( (G, b) \) into irreducibles when \( G \) is a \( p \)-group for some prime \( p \).
Let $G$ be a finite abelian $p$-group and $b$ be a nondegenerate symmetric bilinear form on $G$. The algorithm for decomposing $(G, b)$ into irreducibles boils down to diagonalizing symmetric matrices with entries in $\mathbb{Q}_p/\mathbb{Z}$ via conjugation. The algorithm for diagonalization is the same as the well known algorithm for diagonalizing quadratic forms over $p$-adic integers; see for example [Conway and Sloane 1999, Chapter 15, §4.4]. This algorithm is the core of our argument. We repeat that we could not find this argument in literature for bilinear forms on finite abelian groups. This is our first reason for including the Appendix. A second reason is that the argument is constructive, and so it can be useful in actually decomposing given bilinear forms over finite abelian groups into irreducibles. A third reason is that part (b) of Theorem 2.1 as well as Lemma 2.2 (which we need in our arguments) are not explicitly stated in [Wall 1963]. They can probably be extracted from the arguments in [Wall 1963] or [Miranda 1984; Nikulin 1979]. But this might require some work mainly because each paper has its own rather complicated set of notations.

The following lemma, describing the nondegenerate quadratic forms on $(\mathbb{Z}/2^r\mathbb{Z})^2$, is essential to the proof of Theorem 2.1. It is stated here because we shall also use it in the computation of some Gauss sums. It can be proved using Hensel’s lemma. A proof is given in the Appendix.

**Lemma 2.2.** Set $G = (\mathbb{Z}/2^r\mathbb{Z})^2$ and let $q$ be an irreducible nondegenerate quadratic form on $G$. Then there exist integers $A$, $B$, $C$ with $B$ odd such that $q(x_1, x_2) = 2^{-r}(Ax_1^2 + Bx_1x_2 + Cx_2^2)$. If $AC$ is even, then $(G, q) \simeq ((\mathbb{Z}/2^r\mathbb{Z})^2, x_1x_2/2^r)$. Otherwise, $(G, q) \simeq ((\mathbb{Z}/2^r\mathbb{Z})^2, (x_1^2 + x_1x_2 + x_2^2)/2^r)$.

### 3. Gauss sums and related invariants of a quadratic form

Let $G$ be a finite abelian group and $q : G \to \mathbb{Q}/\mathbb{Z}$ be a quadratic form on $G$. In Section 1, we defined the quadratic Gauss sums $\Theta(G, q)$ and the related invariant $\xi_k(G, q)$; see (1) and (2). In this section, we shall compute the invariants $\Theta(G, q)$ and $\xi_k(G, q)$ for various pairs $(G, q)$. One verifies that $\Theta$ is multiplicative, that is,

$$\Theta((G_1, q_1) \perp (G_2, q_2)) = \Theta(G_1, q_1)\Theta(G_2, q_2).$$

In the same sense, $\xi_k$ is also multiplicative. We start with the following well known result. The proof is omitted.

**Theorem 3.1.**

(a) Let $\chi : G \to \mathbb{C}^*$ be a character on $G$. Then $\sum_{x \in G} \chi(x) = |G|$ if $\chi = 1$ and $\sum_{x \in G} \chi(x) = 0$ otherwise.

(b) If $q$ is a nondegenerate quadratic form on $G$, then $\Theta(G, q)\Theta(G, -q) = 1$ and, in particular, $|\Theta(G, q)|^2 = 1$.

The next lemma gives the values of the Gauss sums of irreducible nondegenerate forms.
**Lemma 3.2.** (a) Let \( p \) be an odd prime and \( \alpha \) be an integer relatively prime to \( p \). Then

\[
\Theta\left(\mathbb{Z}/p^r\mathbb{Z}, \alpha(p^r + 1)x^2/2p^r\right) = \left(\frac{2\alpha}{p}\right)^r e_{p^r},
\]

where \( \left(\frac{2\alpha}{p}\right) \) denotes the Legendre symbol and \( e_m = 1 \) if \( m \equiv 1 \mod 4 \) and \( e_m = i \) if \( m \equiv 3 \mod 4 \).

(b) Let \( \alpha \) be an odd integer. Then

\[
\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, \alpha x^2/2^{r+1}\right) = (-1)^{r(\alpha^2-1)/8} e(\alpha/8).
\]

(c) Let \( \alpha, \beta, \) and \( \gamma \) be integers with \( \beta \) odd. Then

\[
\Theta\left(\mathbb{Z}/2^r\mathbb{Z}^2, (\alpha x_1^2 + \beta x_1 x_2 + \gamma x_2^2)/2^r\right) = (-1)^{\gamma \alpha r}.
\]

**Proof.** For part (a), see for example [Iwaniec and Kowalski 2004, p. 52]. Let \( G_r \) and \( G'_r \) denote the left-hand sides of the formulae in parts (b) and (c), respectively. Then one verifies that \( G_r = 2G_{r-2} \) and \( G'_r = 4G'_{r-2} \) for \( r > 2 \). Parts (b) and (c) now follow by induction once the formulae for \( r = 1 \) and 2 are verified. \( \square \)

Since \( \Theta \) is multiplicative, one can calculate the Gauss sums of arbitrary non-degenerate forms by first decomposing the forms into orthogonal direct sums of irreducible forms and using Lemma 3.2. We will also need to compute the Gauss sums of some singular forms. This is the purpose of the lemma below.

**Lemma 3.3.** (a) Let \( p \) be a prime. Let \( G = (\mathbb{Z}/p^r\mathbb{Z})^n \), and let \( q \) be a \( p^{-s}\mathbb{Z}/\mathbb{Z} \)-valued quadratic form on \( G \). Let \( 0 \leq s \leq r \). Then \( p^s q \) induces a quadratic form on \( G/p^{r-s} G \) and

\[
\Theta(G, p^s q) = p^{sn/2} \Theta(G/p^{r-s} G, p^s q).
\]

(b) Let \( \alpha \) be an odd integer. Then one has

\[
\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, 2^s \cdot \frac{\alpha x^2}{2^{r+1}}\right) = \begin{cases} 2^{s/2} (-1)^{(r-s)(\alpha^2-1)/8} e(\alpha/8) & \text{if } 0 \leq s < r, \\ 0 & \text{if } s = r, \\ 2^{r/2} & \text{if } s > r. \end{cases}
\]

**Proof.** (a) If \( x \equiv x' \mod p^{r-s} G \), then \( p^s q(x) = p^s q(x') \) since \( q \) and \( \partial q \) take values in \( p^{-s}\mathbb{Z}/\mathbb{Z} \). So \( p^s q(x) \) induces a form on \( G/p^{r-s} G \). One has

\[
|G|^{1/2} \Theta(G, p^s q) = \sum_{x \in G} e(p^s q(x)) = |G^{r-s} G| \sum_{y \in G/p^{r-s} G} e(p^s q(y)) = |G^{r-s} G||G/p^{r-s} G|^{1/2} \Theta(G/p^{r-s} G, p^s q).
\]

Part (a) follows since \( |p^{r-s} G| = p^{sn} \).
(b) First suppose \( r - s \geq 1 \). Note that, if \( y \equiv x \mod 2^r \), then \( \alpha y^2/2^{r-s+1} \equiv \alpha x^2/2^{r-s+1} \mod \mathbb{Z} \). So

\[
2^{r/2} \Theta \left( \mathbb{Z}/2^r \mathbb{Z}, 2^s \cdot \frac{\alpha x^2}{2^{r+1}} \right) = \sum_{x=0}^{2^r-1} e \left( \frac{\alpha x^2}{2^{r-s+1}} \right) = 2^s \sum_{x=0}^{2^r-s-1} e \left( \frac{\alpha x^2}{2^{r-s+1}} \right) = 2^{(r+s)/2} \Theta \left( \mathbb{Z}/2^{r-s} \mathbb{Z}, 2^{(r+s)/2} \alpha \right).
\]

Part (b) now follows from Lemma 3.2 for \( 0 \leq s < r \). Now let \( s = r \). Note that, if \( y \equiv x \mod 2 \), then \( \alpha x^2/2 \equiv \alpha y^2/2 \mod \mathbb{Z} \). So

\[
2^{r/2} \Theta \left( \mathbb{Z}/2^r \mathbb{Z}, 2^s \cdot \frac{\alpha x^2}{2^{r+1}} \right) = \sum_{x=0}^{2^r-1} e \left( \frac{\alpha x^2}{2^{r-s+1}} \right) = 2^{r-1} \sum_{x=0}^{1} e \left( \frac{\alpha x^2}{2} \right) = 0.
\]

For \( s > r \), the quadratic form we have is identically equal to 0, so the result is obvious. \( \square \)

**Lemma 3.4.** Let \( p \) be an odd prime, and let both \( r \) and \( k \) be positive integers. Let \( q_1 \) and \( q_2 \) be the two nonisometric nondegenerate quadratic forms on \( G = \mathbb{Z}/p^r \mathbb{Z} \). Then

\[
\xi_k(G, q_1) = (-1)^e_p \xi_k(G, q_2)
\]

where \( e_p^k = r(k + 1) - \min\{r, v_p(k)\} \).

**Proof.** There are only two distinct nondegenerate quadratic forms on \( G \); see Table 1. Without loss of generality, we may thus assume that \( q_j(x) = u_j(p^r + 1)x^2/2p^r \) for \( j = 1, 2 \), where \( u_1 = 1 \) and \( u_2 = u_p \) is a quadratic nonresidue modulo \( p \). Lemma 3.2(a) implies \( \Theta(G, q_1) = (-1)^r \Theta(G, q_2) \). If \( v_p(k) > r \), the lemma holds by the fact that \( \Theta(G, -kq_1) = \sqrt{|G|} \).

Now assume \( 0 \leq v_p(k) \leq r \). Write \( s = v_p(k) \) and \( -k = p^s a \) with \( a \in \mathbb{Z} \) relatively prime to \( s \). Then \( \Theta(G, -kq_1) \) is equal to

\[
\Theta(G, p^s aq_1) = p^{s/2} \Theta(\mathbb{Z}/p^{r-s} \mathbb{Z}, p^s a u_j(p^r + 1)x^2/2p^r) = p^{s/2} \Theta(\mathbb{Z}/p^{r-s} \mathbb{Z}, (p^{r-s} + 1)u_jx^2/2p^{r-s}).
\]

The first equality follows from Lemma 3.3(a). For the second, we need to observe that the quadratic forms \( (p^{r-s} + 1)\alpha x^2/2p^{r-s} \) and \( (p^r + 1)\alpha x^2/2p^{r-s} \) are identical on \( \mathbb{Z}/p^{r-s} \mathbb{Z} \). From Lemma 3.2(a), we have

\[
\Theta(\mathbb{Z}/p^{r-s} \mathbb{Z}, (p^{r-s} + 1)u_p x^2/2p^{r-s}) = (-1)^{r-s} \Theta(\mathbb{Z}/p^{r-s} \mathbb{Z}, (p^{r-s} + 1)\alpha x^2/2p^{r-s}),
\]

which implies \( \Theta(G, -kq_2) = (-1)^{r-s} v_p(k) \Theta(G, -kq_1) \). The lemma follows once we recall that \( \Theta(G, q_1) = (-1)^r \Theta(G, q_2) \). \( \square \)
Next, we shall introduce an invariant \( \sigma_k(b) \) of a discriminant form \((G, b)\) defined in [Kawauchi and Kojima 1980] and in Lemma 3.6 compare it to our Gauss sums (discriminant forms are called linking pairs in [Kawauchi and Kojima 1980]).

**Definitions.** For the convenience of the reader, we shall recall some of the definitions from [Kawauchi and Kojima 1980; Wall 1963]. Let \( G \) be a finite abelian group. Let

\[
G[n] = \{ x \in G : nx = 0 \}
\]

denote the \( n \)-torsion subgroup of \( G \). Let \( p \) be a prime. Then \( G(p) = \bigcup_n G[p^n] \) is the \( p \)-Sylow subgroup of \( G \). For \( k \geq 1 \), define

\[
\tilde{G}_p^k = G[p^k] / (G[p^{k-1}] + pG[p^{k+1}]).
\]

Take a decomposition of \( G \) into a direct sum of cyclic groups of prime power order. If such a decomposition has \( n \) factors isomorphic to \( \mathbb{Z} / p^k \mathbb{Z} \), then \( \tilde{G}_p^k \) is an elementary abelian \( p \)-group of order \( n \). Let \( b \) be a nondegenerate symmetric bilinear form on \( G \). Then

\[
\tilde{b}_p^k ([x], [y]) = p^{-1} b(x, y)
\]

defines a nondegenerate bilinear form on \( \tilde{G}_p^k \). Here \( x \) and \( y \) denote any two elements of \( G[p^k] \) representing \([x], [y] \in \tilde{G}_p^k\), respectively.

Let \( c^k(b) \) be the characteristic element (also called parity element) of the \( \mathbb{F}_2 \)-quadratic space \((\tilde{G}_2^k, \tilde{b}_2^k)\). Explicitly, \( c^k(b) \) is the unique element of \( \tilde{G}_2^k \) such that \( \tilde{b}_2^k(x, x) = \tilde{b}_2^k(x, c^k(b)) \) for all \( x \in \tilde{G}_2^k \). In other words, \( c^k(b) \) is represented by any \( c \in G[2^k] \) that satisfies

\[
2^{-1} b(x, x) = 2^{-1} b(x, c) \quad \text{for all } x \in G[2^k].
\]

Note that both sides of the above equality can only take the values 0 or 1/2. Also observe that the characteristic element \( c^k(b) \) is zero if and only if \( b(x, x) \in 2^{1-k} \mathbb{Z} / \mathbb{Z} \) for all \( x \in G[2^k] \).

The invariant \( \sigma_k(b) \) takes values in \((\mathbb{Z}/8\mathbb{Z}) \cup \{\infty\}\), which is made into a semigroup by defining \( \infty + \infty = n + \infty = \infty \) for \( n \in \mathbb{Z}/8\mathbb{Z} \). If \( c^k(b) \neq 0 \), then \( \sigma_n(b) = \infty \) by definition. If \( c^k(b) = 0 \), then one checks that

\[
q_k(x) = 2^{k-1} b(x, x)
\]

induces a well defined quadratic form on \( G(2^k) / G[2^k] \) and, following [Kawauchi and Kojima 1980], we can define \( \sigma_k(b) \) by

\[
|G(2^k) / G[2^k]|^{1/2} \Theta(G(2^k) / G[2^k], q_k) = Ce(\sigma_k(b) / 8),
\]

where \( C \) is the absolute value of the left-hand side of the equation [Kawauchi and Kojima 1980, §2]; we shall soon see that \( C \neq 0 \). If \( x, y \in G(2) \) represent \([x], [y] \in G(2) / G[2^k] \), then \( \partial q_k([x], [y]) = 2^k b(x, y) \). Suppose \([x] \in G(2) / G[2^k] \)
such that $\partial q_k([x], [y]) = 0$ for all $[y] \in G_{(2)}/G[2^k]$. Let $x \in G_{(2)}$ be a representative for $[x]$. Then $2^k b(x, y) = 0$ for all $y \in G_{(2)}$. Since $b$ is nondegenerate, it follows that $2^k x = 0$, so $[x] = 0$ in $G_{(2)}/G[2^k]$. So we have argued that, if $c^k(b) = 0$, then $q_k(x)$ is a nondegenerate form on $G_{(2)}/G[2^k]$. Hence, Theorem 3.1(b) gives $C = |G_{(2)}/G[2^k]|^{1/2}$. So $\sigma_k(b)$ is in fact given by the simpler formula

$$\Theta(G_{(2)}/G[2^k], q_k) = e(\sigma_k(b)/8). \quad (4)$$

The following theorem is the reason for our interest in the invariant $\sigma_k(b)$, and it follows from Theorem 4.1 of [Kawauchi and Kojima 1980].

**Theorem 3.5.** Let $G$ be a finite abelian 2-group, and let $b$ and $b'$ be two non-degenerate symmetric bilinear forms on $G$. Then $(G, b) \simeq (G, b')$ if and only if $\sigma_k(b) \simeq \sigma_k(b')$ for all $k \geq 1$.

**Definition.** It will be convenient for us to work with the invariant

$$\varsigma_k(b) = e(\sigma_k(b)/8) \quad (5)$$

rather than $\sigma_k(b)$. If $\sigma_k(b) = \infty$, then we define $\varsigma_k(b) = 0$. So $\varsigma_k$ takes values in the multiplicative semigroup $\mu_8 \cup \{0\}$ where $\mu_8$ is the group of 8-th roots of unity. From Corollary 2.2 of [Kawauchi and Kojima 1980], it follows that, if $(G, b) = (G_1, b_1) \perp (G_2, b_2)$, then $\varsigma_k(b) = \varsigma_k(b_1)\varsigma_k(b_2)$. In other words, $\varsigma_k$ is multiplicative, just like the Gauss sums or the invariant $\xi_k$. The multiplicativity of $\varsigma_k(b)$ also follows from the next lemma.

**Lemma 3.6.** Let $G$ be a finite abelian 2-group, and let $b$ be a nondegenerate symmetric bilinear form on $G$. Let $k \geq 1$. Then

$$\Theta(G, 2^{k-1}b(x, x)) = |G[2^k]|^{1/2}\varsigma_k(b).$$

Let $q$ be a nondegenerate quadratic form on $G$. Then with $b = \partial q$, the above equation yields

$$\varsigma_k(\partial q) = |G[2^k]|^{-1/2}\Theta(G, 2^k q). \quad (6)$$

**Proof.** Let $q_k(x) = 2^{k-1}b(x, x)$. Let $w$ vary over a set of coset representatives of $G/G[2^k]$ and $y$ vary over $G[2^k]$. Then

$$|G|^{1/2}\Theta(G, q_k) = \sum_{w,y} e(q_k(w + y)) = \sum_w e(q_k(w)) \sum_y e(2^{k-1}b(y, c^k(b))). \quad (7)$$

The second equality follows since $2^k b(w, y) = 0$ and $2^{k-1} b(y, y) = 2^{k-1} b(y, c^k(b))$. If $c^k(b) \neq 0$, then $y \mapsto e(2^{k-1}b(y, c^k(b)))$ is a nontrivial character on $G[2^k]$, so the inner sum in (7) is zero; hence, $\Theta(G, 2^{k-1}b(x, x)) = 0$. Now suppose $c^k(b) = 0$. Then we find that $2^{k-1}b(w, w) = 2^{k-1}b(w', w')$ if $w \equiv w' \mod G[2^k]$. Thus,
(w → q_k(w)) induces a quadratic form on G/G[2^k]. From (7), we get
\[ |G|^{1/2} \Theta(G, q_k) = |G[2^k]| \prod_{w \in G/G[2^k]} e(q_k(w)) = |G[2^k]|^{1/2} |G/G[2^k]| \Theta(G/G[2^k], q_k). \]
The lemma follows from (4). □

**Lemma 3.7.** Let \((G, q)\) be an irreducible metric 2-group with \(\exp(G) = 2^r\) (see Table 1). Let \(\beta\) be an odd integer and \(n \geq 1\). Then
\[ \zeta_n(\partial q)^{\beta 2^n} = \begin{cases} 0 & \text{if } n = r \text{ and } \text{rk}(G) = 1, \\ (-1)^{\text{rk}(G)\delta_{n,2} \delta_{r,1}} \Theta(G, \beta 2^n q)^{\beta 2^n} & \text{otherwise,} \end{cases} \]
where \(\delta_{i,j}\) is the Kronecker delta, and
\[ \Theta(G, \beta 2^n q) = |G[2^n]|^{1/2} (-1)^{\text{rk}(G)\max(r-n,0)(\beta^2-1)/8} \zeta_n(\partial q)^{\beta}. \]

**Proof.** We treat the cases \(\text{rk}(G) = 1\) and \(\text{rk}(G) = 2\) separately. First suppose \(G\) has rank 1, that is, \((G, q) \simeq (\mathbb{Z}/2^r\mathbb{Z}, \alpha x^2/2^{r+1})\) where \(\alpha \in \{\pm 1, \pm 5\}\). Then from Lemma 3.2(b), we find that \(\Theta(G, q) = \pm e(\alpha/8). \) Since \(n \geq 1\), we have
\[ \Theta(G, q)^{\beta 2^n} = e(\alpha/8)^{\beta 2^n}. \]

Now we split the argument into three cases.

**Case 1** \((n > r)\). Then \(\Theta(G, 2^n \beta q) = |G|^{1/2} = |G[2^n]|^{1/2}\), and so (6) implies \(\zeta_n(\partial q) = 1\). This verifies (9). From (10), we obtain \(\Theta(G, q)^{\beta 2^n} = e(\alpha/8)^{\beta 2^n} = (-1)^{\delta_{n,2} \delta_{r,1}}\). This verifies (8).

**Case 2** \((n = r)\). Lemma 3.3(b) implies that \(\Theta(G, 2^n \beta q) = 0\). From (6), we get \(\zeta_n(\partial q) = |G[2^n]|^{-1/2} \Theta(G, 2^n q) = 0\) too. This verifies (8) and (9) in this case.

**Case 3** \((1 \leq n < r)\). From (6) and Lemma 3.3(b), we have
\[ \zeta_n(\partial q) = |G[2^n]|^{-1/2} \Theta(G, 2^n q) = 2^{-n/2} \Theta \left( \mathbb{Z}/2^r\mathbb{Z}, 2^n \frac{\alpha x^2}{2^{r+1}} \right) = (-1)^{(r-n)(\alpha^2-1)/8} e(\alpha/8). \]
Since \(n \geq 1\), using (10), we obtain \(\zeta_n(\partial q)^{\beta 2^n} = e(\alpha/8)^{\beta 2^n} = \Theta(G, q)^{\beta 2^n}\), which verifies (8). To verify the expression for \(\Theta(G, \beta 2^n q)\), we compute as follows:
\[ \Theta(G, 2^n \beta q) = \Theta \left( \mathbb{Z}/2^r\mathbb{Z}, 2^n \frac{\beta \alpha x^2}{2^{r+1}} \right) = 2^{n/2} (-1)^{(r-n)(\alpha^2-1)/8} e(\beta \alpha/8) \]
\[ = 2^{n/2} (-1)^{(r-n)(\beta^2-1)/8} ((-1)^{(r-n)(\alpha^2-1)/8} e(\alpha/8))^\beta \]
\[ = 2^{n/2} (-1)^{(r-n)(\beta^2-1)/8} \zeta_n(\partial q)^{\beta}. \]
where the third equality follows from the fact that for odd integers \( \beta \) and \( \alpha \)
\[
(\alpha^2 \beta^2 - 1) - (\beta^2 - 1) - \beta(\alpha^2 - 1) = \beta(\beta - 1)(\alpha^2 - 1) \equiv 0 \bmod 16.
\] 
(11)

This verifies (9) and finishes the argument in the case \( \text{rk}(G) = 1 \).

Now assume \( \text{rk}(G) = 2 \). If \( n < r \), then (6) and Lemmas 3.3(a) and 3.2(c) give us \( \varsigma_n(\partial q) = \pm 1 \) (or else see Corollary 2.2 of [Kawauchi and Kojima 1980]). If \( n \geq r \), then from (4), we obtain, \( \varsigma_n(\partial q) = \Theta(G/G[2^n], 2^n q) \). Since \( G[2^n] = G \), the Gauss sum is equal to 1 and thus \( \varsigma_n(\partial q) = 1 \). Thus, in any case, we find that \( \varsigma_n(\partial q) = \pm 1 \). Lemma 3.2(c) tells us that \( \Theta(G, q) = \pm 1 \) as well. Now (8) follows since \( n \geq 1 \).

Since \( \varsigma_n(\partial q) = \pm 1 \), the right-hand side of (9) becomes

\[
|G[2^n]|^{1/2} \varsigma_n(\partial q).
\]

Since \( G \) is of type \( E_{2r} \) or \( F_{2r} \), Lemma 2.2 implies \( (G, \beta q) \simeq (G, q) \). So \( (G, 2^r \beta q) \simeq (G, 2^r q) \), and (9) follows immediately from (6).

**Lemma 3.8.** Let \( (G, q) \) be a metric 2-group. Let \( n \geq 1 \) and \( \beta \) be an odd positive integer. Let \( \varsigma_n(\partial q) \) be the invariant introduced in (5). Then

\[
\xi_{2^n \beta}(G, q) = (-1)^{\Gamma_{G, \beta, n}} |G[2^n]|^{1/2} \varsigma_n(\partial q)^{(2^n - 1)\beta}
\]

where \( \Gamma_{G, \beta, n} \) is an integer dependent on \( G, \beta, \) and \( n \) and independent of \( q \). More precisely, if we write \( G \simeq \bigoplus_{r=1}^{\infty} (\mathbb{Z}/2^r \mathbb{Z})^{N_r} \), then

\[
\Gamma_{G, \beta, n} = \delta_{n, 2} N_1 + \sum_{r=1}^{\infty} N_r \max\{r - n, 0\}(\beta^2 - 1)/8.
\]

**Proof.** Observe that both sides of the equation we want to prove are multiplicative invariants of a metric group. Since any metric group \( (G, q) \) can be decomposed into irreducibles by Theorem 2.1, it suffices to prove the equation when \( (G, q) \) is an irreducible metric group. Assume \( (G, q) \) is an irreducible metric group of exponent \( 2^r \); the possibilities for these are given in Table 1. Note that \( G \) is isomorphic to \( (\mathbb{Z}/2^r \mathbb{Z}) \) or \( (\mathbb{Z}/2^r \mathbb{Z})^2 \) and \( N_j = \delta_{j, r} \text{rk}(G) \). So the equation we want to prove becomes

\[
\Theta(G, q)^{\beta 2^n} \Theta(G, -\beta 2^n q)
\]

\[
= (-1)^{\text{rk}(G)\delta_{n, 2}\delta_{1, r} + \text{rk}(G) \max\{r - n, 0\}(\beta^2 - 1)/8} |G[2^n]|^{1/2} \varsigma_n(\partial q)^{(2^n - 1)\beta}.
\]

This equation follows directly from Lemma 3.7. \( \square \)

**4. Indicator of Tambara–Yamagami categories as Gauss sums**

Let \( G \) be a finite abelian group. A function \( \chi : G \times G \to \mathbb{C}^* \) is called a symmetric bicharacter on \( G \) if \( \chi(x, \cdot) \) and \( \chi(\cdot, x) \) are characters on \( G \) and \( \chi(x, y) = \chi(y, x) \).
for each \( x, y \in G \). A symmetric bilinear form \( b \) on \( G \) determines a symmetric bicharacter \( \chi : G \times G \to \mathbb{C}^\ast \) given by \( \chi(x, y) = e(-b(x, y)) \) (the minus sign in front of \( b \) is for consistency with notation in [Shimizu 2011]). This sets up a natural correspondence between bilinear forms and bicharacters. We say \( \chi \) is nondegenerate if \( b \) is.

Let \( G \) be a finite abelian group, \( \chi \) be a nondegenerate symmetric bicharacter on \( G \), and \( \tau \) be a square root of \( |G|^{-1} \). Let \( b \) be the bilinear form on \( G \) given by \( \chi(x, y) = e(-b(x, y)) \). Given any triple \((G, \chi, \tau)\), there exists a spherical fusion category \( C \), called the Tambara–Yamagami category or TY-category for short. We shall denote this category by \( TY(G, \chi, \tau) \) or by \( TY(G, b, \tau) \). The simple objects of \( C \) are \( G \cup \{m\} \). We shall write \( m = m_C \) if there is a chance of confusion. The associativity constraint in \( TY(G, \chi, \tau) \) is dictated by the bicharacter \( \chi \) and \( \text{sign}(\tau) \). See [Tambara and Yamagami 1998] or [Shimizu 2011] for more details on the TY-categories. Caution: the abelian groups in [Shimizu 2011] are multiplicative while for our purpose it is convenient to write the group \( G \) additively.

For each simple object \( x \) of a spherical fusion category and each integer \( k \geq 1 \), one can associate a complex number \( \nu_k(x) \), introduced in [Ng and Schauenburg 2007b], called the \( k \)-th Frobenius–Schur indicator of \( x \). The lemma below tells us the indicators of the simple objects of a TY-category. This is an easy translation of results in [Shimizu 2011]. Our main observation is noting that the indicators of the object \( m_C \) can be expressed in terms of certain Gauss sums.

**Lemma 4.1.** Let \( C = TY(G, \chi, \tau) \) be a TY-category. From [Shimizu 2011, Theorem 3.2], we know that \( \nu_k(x) = \delta_{x, 1} \) for \( x \in G \). Let \( b \) be the bilinear form on \( G \) given by \( \chi(x, y) = e(-b(x, y)) \). Let \( q \) be any quadratic form such that \( \partial q = b \). Then for all \( k \geq 1 \), one has \( \nu_{2k-1}(m_C) = 0 \) and

\[
\nu_{2k}(m_C) = \text{sign}(\tau)^k \Theta(G, q)^k \Theta(G, -kq) = \text{sign}(\tau)^k \xi_k(G, q),
\]

and this value does not depend on the choice of \( q \).

**Proof.** From Theorem 3.3 of [Shimizu 2011], we know that \( \nu_{2k-1}(m) = 0 \). Let

\[
C(\chi) = \{ \varphi : G \to \mathbb{C} : \varphi(x)\varphi(y)\varphi(x + y)^{-1} = \chi(x, y) \text{ for } x, y \in G \}.
\]

From the proof of that result, we have

\[
\nu_{2k}(m_C) = \frac{1}{|G|} \sum_{\varphi \in C(\chi)} \left( \tau \sum_{x \in G} \varphi(x) \right)^k \sqrt{|G|}. \tag{12}
\]

By definition, \( e \circ q \in C(\chi) \). One checks that \( G \) acts simply transitively on \( C(\chi) \) by \( \varphi \cdot a \varphi(x) = \varphi(x) \chi(a, x)^{-1} \). So \( C(\chi) = \{ \varphi_a : a \in G \} \) where \( \varphi_a(x) = e(q(x)) \chi(a, x)^{-1} \).
One has
\[
\sum_{x \in G} \varphi_a(x) \varphi_b(x) = \frac{\text{sign}(\tau)}{\sqrt{|G|}} \sum_{x \in G} e(q(x) + b(a, x) + q(a) - q(a))
\]
\[
= \frac{\text{sign}(\tau)e(-q(a))}{\sqrt{|G|}} \sum_{x \in G} e(q(x + a))
\]
\[
= \text{sign}(\tau)e(-q(a))\Theta(G, q).
\]

From (12), it follows that
\[
\nu_{2k}(m_C) = \frac{\text{sign}(\tau)^k}{\sqrt{|G|}} \sum_{a \in G} e(-kq(a))\Theta(G, q)^k
\]
\[
= \text{sign}(\tau)^k\Theta(G, q)^k\Theta(G, -kq).
\]

To complete the proof, observe that the expression on the right-hand side of (12) only depends on \(\chi\) and is independent of the choice of \(q\).

We shall need the following.

**Lemma 4.2 [Shimizu 2011, Theorem 3.5].** Let \(C = TY(G, b, \tau)\) be a TY-category. Let \(q\) be a quadratic form such that \(\partial q = b\). Then \(\nu_{2k}(m) = |G[k]|^{1/2}\psi\) where \(\psi \in \mu_8 \cup \{0\}\) (recall that \(\mu_8\) denotes the set of 8-th roots of unity). One has \(\psi = 0\) if and only if there exists \(a \in G[k]\) such that \(kq(a) \neq 0\).

**Remark.** We should mention that, from the values of the Gauss sums given in the previous section and the decomposition of \((G, q)\) into irreducibles, we can show that \(\xi_k(G, q) = 0\) if and only if \((G, q)\) contains an irreducible component that equals \(A_{2r}, B_{2r}, C_{2r},\) or \(D_{2r}\) where \(r = \nu_2(k)\) for some even \(k\) and that this yields another proof of Lemma 4.2.

Let \((G, q)\) be a premetric group. The invariant \(\xi_k(G, q)\) can itself be expressed as a Gauss sum as follows. Let \(F_k(G, q)\) denote the premetric group given by the abelian group \(\{ (g_1, \ldots, g_k) \in G^k : \sum_j g_j = 0 \}\) with the quadratic form \(q(g_1, \ldots, g_k) = \sum_j q(g_j)\). Then one can show that \(\xi_k(G, q) = F_k(G, q)\). In view of this formula, the appearance of the 8-th root of unity \(\psi\) in the above lemma becomes a consequence of Milgram’s formula.

**5. Tambara–Yamagami categories are determined by the higher Frobenius–Schur-indicators**

In this section, we shall prove Theorem 1.1. Let \(C = TY(G, \chi, \tau)\) be a TY-category. We shall show that the Frobenius–Schur indicators of the simple objects of \(C\) determine the triple \((G, \chi, \tau)\). So the indicators can distinguish between any two TY-categories. Most of the work goes into showing that the indicators \(\nu_k(m_C)\)
We will also use the notation $C$ where $n \in \mathbb{N}$. It follows that $(\xi_k(G, q_1) \neq \xi_k(G, q_2)$ or else, for each natural number $\gamma$, there exists a positive integer $k$ with $v_2(k) = \gamma$ and $\xi_k(G, q_1) \neq \xi_k(G, q_2)$.}

**Lemma 5.1.** Let $G$ be an abelian group of odd order. Let $b_1$ and $b_2$ be two nonisometric nondegenerate symmetric bilinear forms on $G$. Let $q_1$ and $q_2$ be quadratic forms such that $\partial q_1 = b_j$ for $j = 1, 2$. Then either there exists an odd positive integer $k$ such that $\xi_k(G, q_1) = \xi_k(G, q_2)$ or else, for each natural number $\gamma$, there exists a positive integer $k$ with $v_2(k) = \gamma$ and $\xi_k(G, q_1) \neq \xi_k(G, q_2)$.

**Proof.** Fix a nonsquare $u_p$ modulo $p$ for each odd prime $p$. Recall from Table 1

\[
A_{p^r} = \left( \mathbb{Z}/p^r \mathbb{Z}, q(x) = \frac{2^{-1}x^2}{p^r} \right) \quad \text{and} \quad B_{p^r} = \left( \mathbb{Z}/p^r \mathbb{Z}, q(x) = \frac{2^{-1}u_px^2}{p^r} \right).
\]

We will also use the notation

\[
n \cdot A_{p^r} = \left( \mathbb{Z}/p^r \mathbb{Z}, q(x) = \frac{2^{-1}n^2}{p^r} \right) \quad \text{and} \quad n \cdot B_{p^r} = \left( \mathbb{Z}/p^r \mathbb{Z}, q(x) = \frac{2^{-1}u_pnx^2}{p^r} \right)
\]

for $n \in \mathbb{Z}$. Write $G \simeq \bigoplus_{p^r} (\mathbb{Z}/p^r \mathbb{Z})^{N_{p^r}}$ where $p$ ranges over odd primes and $r \geq 1$. Since $A_{p^r} \perp A_{p^r} \simeq B_{p^r} \perp B_{p^r}$ [Wall 1963, Theorem 4], the metric group $(G, q_j)$ is an orthogonal direct sum, over all $(p, r)$ such that $N_{p^r} \neq 0$, of the homogeneous metric groups

\[
A_{p^r}^{N_{p^r}-1} \perp C^r_{p^r},
\]

where $C^r_{p^r}$ is either $A_{p^r}$ or $B_{p^r}$. Since $\xi_k$ is multiplicative, we have

\[
\xi_k(G, q_j) = \prod_{p^r : N_{p^r} \neq 0} \xi_k(A_{p^r})^{N_{p^r}-1} \xi_k(C^r_{p^r}). \tag{13}
\]

Let

\[
\mathcal{A} = \{(p, r) : N_{p^r} \neq 0, \quad C^r_{p^r} \neq C^r_{p^r}, \}
\]

\[
\mathcal{A}_{\text{max}} = \{(p, r) \in \mathcal{A} : (p, r') \notin \mathcal{A} \text{ for all } r' > r\}.
\]

If $(p, r) \notin \mathcal{A}$, then the $(p, r)$-th term in the product in (13) is the same for $j = 1, 2$. If $(p, r) \in \mathcal{A}$, then the $(p, r)$-th terms differ by a factor $(-1)^{\xi_{k_{p^r}}}$ given in Lemma 3.4. It follows that

\[
\xi_k(G, q_1) = (-1)^{\Lambda} \xi_k(G, q_2) \quad \text{where} \quad \Lambda = \sum_{(p, r) \in \mathcal{A}} \xi_{k_{p^r}}.
\]
Case 1. If there is a prime $p$ such that $(p, 1) \in \mathcal{A}_{\max}$, then choose such a prime $p_0$ and let $k = p_0$. We find
\[
\sum_{r:(p_0, r) \in \mathcal{A}} \mathbb{e}_{p_0, r}^k = \mathbb{e}_{p_0, 1}^k = 1(k + 1) - \min\{1, v_{p_0}(k)\} = p_0 \equiv 1 \mod 2.
\]
For all prime $(p, r) \in \mathcal{A}$ such that $p \neq p_0$, we have $\mathbb{e}_{p, r}^k = r(p_0 + 1) \equiv 0 \mod 2$. It follows that $\Lambda \equiv 1 \mod 2$, so $\xi_k(G, q_1) \neq \xi_k(G, q_2)$.

Case 2. Otherwise, choose $(p_0, r_0) \in \mathcal{A}_{\max}$ such that $r_0 > 1$. Choose any $\gamma \geq 1$, and let
\[
k = 2^\gamma p_0^{-\gamma} \prod_{(p, r) \in \mathcal{A}_{\max}} p^r.
\]
Note that $k$ is an integer with $v_2(k) = \gamma$ and $v_{p_0}(k) = r_0 - 1$. One has
\[
\mathbb{e}_{p_0, r_0}^k = r_0(k + 1) - \min\{r_0, v_{p_0}(k)\} \equiv r_0 - (r_0 - 1) = 1 \mod 2.
\]
If $r < r_0$, then $r \leq v_{p_0}(k)$, so $\mathbb{e}_{p_0, r}^k = r(k - 1) - r \equiv 0 \mod 2$. Finally if $p \neq p_0$, then $(p, r) \in \mathcal{A}$ implies $r \leq v_p(k)$ by our choice of $k$, so $\mathbb{e}_{p, r}^k = r(k + 1) - r \equiv 0 \mod 2$. Again, $\Lambda \equiv 1 \mod 2$, so $\xi_k(G, q_1) \neq \xi_k(G, q_2)$. □

**Lemma 5.2.** Let $b$ and $b'$ be two nondegenerate symmetric bilinear forms on a finite abelian $2$-group $G$. Let $q$ and $q'$ be quadratic forms such that $\delta q = b$ and $\delta q' = b'$. Let $k$ be a positive integer such that $v_2(k) = 0$ or $v_2(k) > \max\{2, v_2(\exp(G))\}$. Then $\xi_k(G, q) = \xi_k(G, q')$.

**Proof.** By the structure theorem of finite abelian groups and by Theorem 2.1, we can decompose $G$ and $(G, q)$ as
\[
G \cong \bigoplus_{r=1}^\infty (\mathbb{Z}/2^r\mathbb{Z})^{N_r} \quad \text{and} \quad (G, q) \cong (H_1, \mu_1) \perp \cdots \perp (H_m, \mu_m),
\]
respectively, where each $H_i \cong \mathbb{Z}/2^r\mathbb{Z}$ or $H_i \cong (\mathbb{Z}/2^r\mathbb{Z})^2$ and $\mu_i$ is an irreducible nondegenerate quadratic form on $H_i$.

Suppose $k$ is odd. By Lemmas 3.2(b) and 3.3, if $(H_i, \mu_i) \cong (\mathbb{Z}/2^r\mathbb{Z}, \alpha x^2/2^{r+1})$, then
\[
\xi_k(H_i, \mu_i) = (-1)^{kr_i(\alpha^2-1)/8} \mathbb{e}(\alpha/8)^k(-1)^r_1(k^2\alpha^2-1)/8 \mathbb{e}(-k\alpha/8).
\]
Using (11), this simplifies to
\[
\xi_k(H_i, \mu_i) = (-1)^{kr_i(k^2-1)/8}.
\]
By Lemma 3.2, if $(H_i, \mu_i) \cong ((\mathbb{Z}/2^r\mathbb{Z})^2, (\alpha x_1^2 + x_1 x_2 + \alpha x_2^2)/2^r)$ with $\alpha \in \{0, 1\}$, then
\[
\xi_k(H_i, \mu_i) = (-1)^{r_2 r_i k}(-1)^{(-k\alpha)^2 r_i} = (-1)^{r_2 r_i + \alpha r_i k^2} = 1.
\]
We summarize both cases with the equation
\[ \xi_k(H_i, \mu_i) = (-1)^{rk(H_i)r_i(k^2-1)/8}. \]

Summing over all \( i \) such that \( r_i = r \) yields \( \sum_i \, rk(H_i)r_i = \sum_r \, rN_r \). So
\[ \xi_k(G, q) = (-1)\sum_r \, rN_r(k^2-1)/8. \]

The expression for \( \xi_k(G, q) \) does not depend on \( q \), so we get \( \xi_k(G, q) = \xi_k(G, q') \) for \( k \) odd.

Now suppose that \( k = 2^n\beta \) with \( \beta \) odd and \( n > \max\{2, v_2(\exp(G))\} \). Then \( \max(r - n, 0) = 0 \) for all \( r \) such that \( N_r > 0 \). Since \( n > v_2(\exp(G)) \), the quadratic forms \( 2^{n-1}b(x, x) \) and \( 2^{n-1}b'(x, x) \) are identically equal to 0, so Lemma 3.6 implies that \( \zeta_n(b) = \zeta_n(b') = 1 \). From Lemma 3.8, we get
\[ \xi_{2^n\beta}(G, q) = |G[2^n]|^{1/2} \zeta_n(b)^{(2^n-1)\beta} = |G|^{1/2}. \]

Thus, \( \xi_{2^n\beta}(G, q) \) does not depend on \( q \) and we get \( \xi_{2^n\beta}(G, q) = \xi_{2^n\beta}(G, q') \). \( \square \)

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Write \( C_1 = TY(G_1, b_1, \tau_1) \) and \( C_2 = TY(G_2, b_2, \tau_2) \). Let \( m_1 = m_{C_1} \) and \( m_2 = m_{C_2} \). We have pdim\( (x) = 1 \) for \( x \in G_j \) and pdim\( (m_j) = \sqrt{|G_j|} \). So the hypothesis in the theorem yields
\[ (\sqrt{|G_1|} - 1)v_k(m_1) = (\sqrt{|G_2|} - 1)v_k(m_2) \quad \text{for all } k \geq 1. \] (14)

Lemma 4.1 implies that, if \( k \) is a multiple of 8\(|G_1|\)|\(|G_2|\), then \( v_k(m_j) = \sqrt{|G_j|} \) for \( j = 1, 2 \). It follows that \( (\sqrt{|G_1|} - 1)\sqrt{|G_1|} = (\sqrt{|G_2|} - 1)\sqrt{|G_2|} \) and hence \( |G_1| = |G_2| \).

First consider the trivial case: \( |G_1| = |G_2| = 1 \). Then the bilinear forms \( b_1 \) and \( b_2 \) are trivial. So there are only two such TY-categories, and they are only distinguished by the value of \( \tau \in \{\pm 1\} \). We know \( \sum_{x \in G_j} v_k(x) = |G_j[k]| \) and \( \text{sign}(\tau_j) = v_2(m_{C_j}) \). (See Theorem 3.2 of [Shimizu 2011] and the remark following the proof of Theorem 3.4 of [Shimizu 2011]. Or else, see Lemma 4.1.) It follows that \( 1 + \text{sign}(\tau_1) = \sum_{V \in \text{Irr}_C} v_2(V) = \sum_{V \in \text{Irr}_{C_2}} v_2(V) = 1 + \text{sign}(\tau_2) \). So \( \text{sign}(\tau_1) = \text{sign}(\tau_2) \), and the theorem holds in the trivial case.

We may now assume that \( |G_1| > |G_2| \). Equation (14) implies \( v_k(m_1) = v_k(m_2) \) for all \( k \geq 1 \). It follows that \( |G_1[k]| = |G_2[k]| \) for each \( k \geq 1 \). This forces \( G_1 \cong G_2 \), and so we may assume without loss of generality that \( G_1 = G_2 = G \). By [Shimizu 2011], \( \text{sign}(\tau_j) = v_2(m_{C_j}) \), and so it follows that \( \tau_1 = \tau_2 \). Assume that \( b_1 \) and \( b_2 \) are nonisomorphic.

Write \( G = G_e \oplus G_o \) where \( G_e \) is the 2-Sylow subgroup of \( G \) and \( G_o = \bigoplus_{p \neq 2} G_{(p)} \) is the “odd part”. Then \( (G, b_j) = (G_o, b_o^j) \perp (G_e, b_e^j) \). Choose quadratic forms \( q_j^o \) and \( q_j^e \) such that \( b_o^j = \delta q_j^o \) and \( b_e^j = \delta q_j^e \). Then \( q_j = q_j^o \perp q_j^e \) is a quadratic form.
such that $\partial q_j = b_j$. By Lemma 4.1, it is enough to show that $\xi_k(G, q_j) \neq \xi_k(G, q_2)$ for some $k$. Since $\xi_k$ is multiplicative for $j \in \{1, 2\}$, we have

$$\xi_k(G, q_j) = \xi_k(G_o, q_j') \xi_k(G_e, q_j).$$

We split the argument into two cases.

**Case 1** ($b'_1 \cong b'_2$). Then Lemma 5.1 implies that there is an integer $k > 1$ that is either odd or $v_2(k) > \max\{2, v_2(\exp(G_e))\}$ such that $\xi_k(G_o, q'_1) \neq \xi_k(G_o, q'_2)$ and Lemma 5.2 implies that $\xi_k(G_e, q'_1) = \xi_k(G_e, q'_2)$. So $v_2k(m_1) \neq v_2k(m_2)$ if $b'_1 \neq b'_2$.

**Case 2** ($b'_1 \cong b'_2$). In this case, we must have $b'_1 \neq b'_2$. From Theorem 3.5, there exists some $n \geq 1$ such that $\sigma_n(b'_1) \neq \sigma_n(b'_2)$, which implies $\xi_n(b'_1) \neq \xi_n(b'_2)$. Now Lemma 3.8 implies that

$$\xi_{2^n}(G, q'_j) = (-1)^{\Gamma_{G_e, 1, n} |G_e[2^n]|} \xi_n(b'_j) 2^{n-1}$$

where $\Gamma_{G_e, 1, n}$ is an integer dependent on $G_e$ and $n$ but independent of $q'_j$. It follows that $\xi_{2^n}(G_e, q'_1) \neq \xi_{2^n}(G_e, q'_2)$. On the other hand, since $(G_o, b'_1) \cong (G_o, b'_2)$, we have $\xi_{2^n}(G_o, q'_1) = \xi_{2^n}(G_o, q'_2)$. So $v_{2^n+1}(m_1) \neq v_{2^n+1}(m_2)$.

6. Tambara–Yamagami categories associated to groups with an odd factor are determined by the state-sum invariants

Let $G$ be a finite abelian group, $\chi$ be a nondegenerate symmetric bicharacter on $G$ and $\tau$ be a square root of $|G|^{-1}$. Let $C = TY(G, \chi, \tau)$ denote the associated Tambara–Yamagami category. If $M$ is a closed compact 3-manifold, we denote by $|M|_C$ the state-sum invariant of $M$ defined using the category $C$, as in [Turaev and Vainerman 2012]. Let $L_{m,n}$ denote the lens spaces.

**Lemma 6.1.** For all $k \geq 1$, one has $|L_{k,1}|_C = (|G[k]| + |G|^{1/2}v_k(m_C))/2|G|$.

This lemma follows directly from Theorem 0.3 of [Turaev and Vainerman 2012] as well as Lemma 4.1. The former expresses $|L_{2k,1}|_C$ in terms of a quantity $\xi_k(\chi)$ that is essentially the right-hand side of the equation in Lemma 4.1.

**Corollary 6.2.** For all $k \geq 1$, $|L_{k,1}|_C = (\text{pdim}(C))^{-1} \sum_{V \in \text{Irr}(C)} v_k(V) \text{pdim}(V)$.

The corollary follows from Theorem 3.2 of [Shimizu 2011], which implies $\sum_{x \in C} v_k(x) = |G[k]|$.

**Theorem 6.3.** Let $C = TY(G, \chi, \tau)$ and $C' = TY(G', \chi', \tau')$ be any two TY-categories. Suppose $|G|$ is not a power of 2. If $|L_{k,1}|_C = |L_{k,1}|_{C'}$ for all $k \geq 1$, then $C \cong C'$.

**Proof.** Let $G_e$ and $G'_e$ be the 2-Sylow subgroups of $G$ and $G'$, respectively. Let $G_o$ and $G'_o$ be the sums of the $p$-Sylow subgroups for all odd $p$. From Theorem 0.1 of [Turaev and Vainerman 2012], we already know that $|G| = |G'|$ and that the $p$-Sylow
We claim that \( G \) and \( G' \) are isomorphic for all odd \( p \). It follows that \( |G_e| = |G'_e| \). We claim that \( G_e \simeq G'_e \) as well. The claim implies \( G \simeq G' \), and then Lemma 6.1 tells us \( v_k(m_C) = v_k(m'_C) \) for all \( k \), which forces \( \chi \simeq \chi' \) by Theorem 1.1. Thus, to complete the proof, we need to show \( G_e \simeq G'_e \). For this, it suffices to show that \( |G[2^n]| = |G'[2^n]| \) for all \( n \geq 0 \). Suppose this is false. Since \( |G[2^0]| = |G'[2^0]| = 1 \), we may pick the smallest \( n \geq 0 \) such that \( |G[2^{n+1}]| > |G'[2^{n+1}]| \) (without loss of generality) and \( |G[2^m]| = |G'[2^m]| \) for all \( m < n \).

Let \( a = |G_o| = |G'_o| \). Let \( n \geq 0 \). Then \( G[2^na] = G_o \oplus G[2^n] \). By Lemma 4.2, we can write \( v_{2n+1}(m_C) = |G[2^n]|^{1/2} \psi_n \), where \( \psi_n \in \mu_8 \cup \{0\} \). Define \( \psi'_n \) similarly for \( C' \). We have

\[
2|G||L_{2n+1,1}|_C = |G[2^{n+1}]a| + |G|^{1/2}v_{2n+1}(m_C) = |G_o|(1/2, |G[2^{n+1}]| + |G_e|^{1/2} |G[2^n]|^{1/2}\psi_n).
\]

So \( |L_{2n+1,1}|_C = |L_{2n+1,1}|_{C'} \) implies

\[
|G[2^{n+1}]| + |G_e|^{1/2} |G[2^n]|^{1/2}\psi_n = |G'[2^{n+1}]| + |G'_e|^{1/2} |G'[2^n]|^{1/2}\psi'_n.
\]

If \( \psi_n = \psi'_n = 0 \), then the above equation would imply \( |G[2^{n+1}]| = |G'[2^{n+1}]| \). So \( \psi_n \neq 0 \) or \( \psi'_n \neq 0 \). Rearranging the above equation and remembering that \( |G_e| = |G'_e| \), we get

\[
|G[2^{n+1}]| - |G'[2^{n+1}]| = |G_e|^{1/2} |G[2^n]|^{1/2}(\psi'_n - \psi_n).
\]

Each side of (15) belong to \( \mathbb{Z}[e^{2\pi i/8}] \). Consider the absolute norm of each side. If \( \psi \in \mu_8 \cup \{0\} \), one verifies that the absolute norm of \( (\psi - 1) \) is a power of 2 or zero. For example, if \( \psi \) is a primitive 8-th root of unity, then \( N_{\mathbb{Q}}(\psi^2 - 1) = \prod_{j=0}^3(e((2j + 1)/8) - 1) = 2 \). If \( \psi_n \neq 0 \) or \( \psi'_n \neq 0 \), then writing \( (\psi'_n - \psi_n) = \psi_n(\psi'_n/\psi_n - 1) \) or \( (\psi'_n - \psi_n) = \psi_n(1 - \psi_n/\psi'_n) \), respectively, we find that the norm of \( (\psi'_n - \psi_n) \) is a power of 2 or zero. So the norm of the right-hand side of (15) is also a power of 2. However, note that the left-hand side is already an integer, so it must also be a power of 2. The only way this is possible is if \( |G[2^{n+1}]| = 2|G'[2^{n+1}]| \). Write \( v_{2n+1}(m_C) = |G[2^n]|^{1/2} \lambda_n \) and \( v_{2n+1}(m'_C) = |G'[2^n]|^{1/2} \lambda'_n \) for some \( \lambda_n, \lambda'_n \in \mu_8 \cup \{0\} \). Now the equality \( |L_{2n+1,1}|_C = |L_{2n+1,1}|_{C'} \) yields

\[
|G'[2^{n+1}]| = |G[2^{n+1}]| - |G'[2^{n+1}]| = |G|^{1/2} |G[2^n]|^{1/2}(\lambda'_n - \lambda_n).
\]

Now the left-hand side is a power of 2, so the norm of the right-hand side must also be a power of 2. Since \( N(\lambda'_n - \lambda_n) \) is a power of 2, it follows that \( |G| \) is also a power of 2, which contradicts our assumption. It follows that \( (G, \chi) \simeq (G', \chi') \). Now since \( v_2(m_C) = \text{sgn}(\tau) \), the equality \( |L_{2,1}|_C = |L_{2,1}|_{C'} \) implies \( \tau = \tau' \). \( \square \)
Example. We exhibit two Tambara–Yamagami categories that have the same state-sum invariant for all lens spaces $L_{k,1}$. Recall that $A_{2^k}$ denotes the metric group $((\mathbb{Z}/2^n\mathbb{Z}), x^2/2^{n+1})$. For $k \in \mathbb{Z}$, we shall denote the premetric group $((\mathbb{Z}/2^n\mathbb{Z}), kx^2/2^{n+1})$ by $(k \cdot A_{2^k})$. Let $(G_1, b_1) = (A_2)^4 \perp A_4$ and $(G_2, b_2) = (A_2)^2 \perp (A_4)^2$. Let $C_1 = \text{TY}(G_1, b_1, -\frac{1}{8})$ and $C_2 = \text{TY}(G_2, b_2, \frac{1}{8})$. Then we claim that $|L_{n,1}|_{C_1} = |L_{n,1}|_{C_2}$ for all positive integers $n$.

Proof of claim. Let $q_i$ be a quadratic form such that $q_i = b_i$ for $i \in \{1, 2\}$. We will break the proof into cases according to possible 2-valuations of $n$. The trivial case is that $|L_{n,1}|_{C_1} = \frac{1}{128} = |L_{n,1}|_{C_2}$ if $n$ is odd. By Lemmas 6.1 and 4.1, to prove $|L_{2k,1}|_{C_1} = |L_{2k,1}|_{C_2}$, it is enough to show that

$$|G_1[2k]| + (-1)^k 8\xi_k(G, q_1) = |G_2[2k]| + 8\xi_k(G, q_2).$$

Since $\xi_k$ is multiplicative,

$$\xi_k(G, q_1) = \xi_k(A_2)^4 \xi_k(A_4) \quad \text{and} \quad \xi_k(G, q_2) = \xi_k(A_2)^2 \xi_k(A_4)^2.$$

From Lemma 3.2, we have $\xi_k(A_{2^k}) = \Theta(A_{2^k})^k \Theta(-k \cdot A_{2^k}) = e(k/8)\Theta(-k \cdot A_{2^k})$. The values of $\Theta(-k \cdot A_{2^k})$ were computed in Lemma 3.3. This lets us compute the invariants.

We shall consider three cases.

Case 1. Suppose $k$ is odd. Then we have $\Theta(-k \cdot A_2) = (-1)^{(k^2-1)/8} e(-k/8)$, so $\xi_k(A_2) = (-1)^{(k^2-1)/8}$. We have $\Theta(-k \cdot A_4) = (-1)^{2(k^2-1)/8} e(-k/8) = e(-k/8)$, so $\xi_k(A_4) = 1$. It follows that $\xi_k(G, q_1) = 1 = \xi_k(G, q_2)$. Since $|G_1[2k]| = 32$ and $|G_2[2k]| = 16$, we get $|L_{2k,1}|_{C_1} = |L_{2k,1}|_{C_2}$ in this case.

Case 2. Suppose $v_2(k) = 1$ or 2. Then $\Theta(-k \cdot A_2) = 0$ or $\Theta(-k \cdot A_4) = 0$, so $\xi_k(A_2) = 0$ or $\xi_k(A_4) = 0$. Since both $(G_1, b_1)$ and $(G_2, b_2)$ have components of type $A_2$ and $A_4$ and since $\xi_k$ is multiplicative, it follows that $\xi_k(G, q_1) = \xi_k(G, q_2) = 0$. Since $|G_1[2k]| = 64$, we get $|L_{2k,1}|_{C_1} = |L_{2k,1}|_{C_2}$ in this case.

Case 3. Finally suppose $v_2(k) \geq 3$. Let $r = 1$ or $r = 2$. Then $\Theta(A_{2^r})^k = e(k/8) = 1$. The quadratic form $-k \cdot A_{2^r}$ is identically equal to 1, so $\xi_k(A_{2^r}) = \Theta(-k \cdot A_{2^r}) = 2^{r/2}$. It follows that $\xi_k(G, q_j) = |G[1/2]^2 = 8$ for $j = 1, 2$. Since $|G_1[2k]| = 64$ and $(-1)^k = 1$, we get $|L_{2k,1}|_{C_1} = |L_{2k,1}|_{C_2}$ in this case too.

Appendix: Diagonalization of bilinear and quadratic forms

In this appendix, we discuss the problem of decomposing quadratic and bilinear forms on finite abelian groups into irreducible components.

Notation. If $R$ is an abelian group, we let $M_n(R)$ be the set of all $n \times n$ matrices with entries in $R$. If $R$ is a commutative ring and $S$ is an $R$-module, then $S^n$ is a (left) $M_n(R)$-module and $M_n(S)$ is an $M_n(R)$-bimodule. The action of $M_n(R)$ on $S^n$ is obtained by writing elements of $S^n$ as column vectors and multiplying by
the matrix on the left. The two actions of $M_n(R)$ on $M_n(S)$ are by left and right multiplication.

Recall from Section 2 that, if $x$ is an element in a $p$-group of finite order, then we write $v_p(x) = -\log_p(\text{order}(x))$ and $v_p(0) = \infty$. The lemma below is elementary. We leave the proof as an easy exercise.

**Lemma A.1.** Let $p$ be a prime. Let $G$ be an abelian $p$-group.

(a) Let $x \in G$ and $r \in \mathbb{Z}$. Then $rx = 0$ if and only if $v_p(r) + v_p(x) \geq 0$.

(b) If $x \in G$ and $r \in \mathbb{Z}$ such that $rx \neq 0$, then $v_p(r) + v_p(x) = v_p(rx)$.

(c) Let $x_1, x_2 \in G$. Then $v_p(x_1 + x_2) \geq \min\{v_p(x_1), v_p(x_2)\}$, and equality holds if $(x_1) \cap (x_2) = 0$ or $v_p(x_1) \neq v_p(x_2)$. (Here and later, $(x)$ denotes the cyclic subgroup generated by $x$.)

(d) Let $b$ be a symmetric bilinear form on a finite abelian $p$-group $G$. If $g \in G$, then $v_p(g) \leq v_p(b(g, h))$ for all $h \in G$. Further, if $b$ is nondegenerate, then $v_p(g) = \min\{v_p(b(g, h)) : h \in G\}$.

Decomposing symmetric bilinear forms into irreducible components is almost equivalent to diagonalizing matrices by row and column operations. We introduce these operations next.

**Definitions.** Let $E_{ij}$ be the $n \times n$ matrix whose $(i, j)$-th entry is 1 and all other entries are 0. Let $I_n$ denote the $n \times n$ identity matrix. Let $R$ be a commutative ring. Let $A$ be an $n \times n$ matrix with entries in some $R$-module $M$. The operations $\text{Flip}_{ij}(A)$, $\text{Add}_{i-j}(A)$, and $\text{Scale}_{i}(A)$ defined below are called row-column operations on $A$.

- Let $\text{Flip}_{ij}(A) = S^{ij}AS$ where $S = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$. This operation interchanges the $i$-th and $j$-th rows of $A$ and then interchanges the $i$-th and $j$-th columns of $A$.

- Let $\text{Add}_{i-j}(A) = S^{ij}AS$, where $S = I_n + rE_{ji}$ for some $r \in R$ and $i \neq j$. This operation adds $r$ times the $j$-th row of $A$ to the $i$-th row of $A$ and then adds $r$ times the $j$-th column of $A$ to the $i$-th column of $A$.

- Let $\text{Scale}_{i}(A) = S^{ij}AS$ where $S = I_n + (r-1)E_{ii}$ for some $r \in R$. This operation multiplies the $i$-th row of $A$ by $r$ and then multiplies the $i$-th column of $A$ by $r$.

Let $(G, b)$ be a discriminant form and $(e_1, \ldots, e_n) \in G^n$. For each $i \neq j$, the operation $\text{Flip}_{ij}$ converts $\text{Gram}_b(e_1, \ldots, e_n)$ to $\text{Gram}_b(f_1, \ldots, f_n)$ where $f_j = e_i$, $f_i = e_j$, and $f_k = e_k$ for $k \notin \{i, j\}$. The operation $\text{Add}_{i-j}$ converts $\text{Gram}_b(e_1, \ldots, e_n)$ to $\text{Gram}_b(f_1, \ldots, f_n)$ where $f_i = e_i + re_j$ and $f_k = e_k$ for $k \neq i$. The operation $\text{Scale}_{i}$ converts $\text{Gram}_b(e_1, \ldots, e_n)$ to $\text{Gram}_b(f_1, \ldots, f_n)$ where $f_i = re_i$ and $f_k = e_k$ for $k \neq i$. We shall say that a row-column operation on $\text{Gram}_b(e_1, \ldots, e_n)$ is valid
if \( G = \bigoplus_k \langle e_k \rangle \) implies \( G = \bigoplus_k \langle f_k \rangle \). Clearly, \( \text{Flip}_{ij} \) is always valid. The operation \( \text{Scale}_i^j \) is valid if \( r \) is relatively prime to the exponent of \( G \). Lemma A.2 lets us decide when \( \text{Add}_i^j \) is valid.

**Lemma A.2.** Let \( G \) be a finite abelian group and \( e_1, \ldots, e_n \in G \) such that \( G = \bigoplus_k \langle e_k \rangle \). Let \( f_1, \ldots, f_n \in G \) such that \( \text{ord}(f_k) = \text{ord}(e_k) \) for all \( k \) and \( f_1, \ldots, f_n \) generate \( G \). Then there exists \( \phi \in \text{Aut}(G) \) such that \( \phi(e_k) = f_k \). In particular, \( G = \bigoplus_k \langle f_k \rangle \).

**Proof.** Let \( n_k = \text{ord}(e_k) = \text{ord}(f_k) \). Since \( \langle e_k \rangle \) is a cyclic group of order \( n_k \) and \( f_k \) is an element of order \( n_k \) in \( G \), there exists a homomorphism \( \phi_k : \langle e_k \rangle \to G \) given by \( \phi_k(e_k) = f_k \). By the universal property of the direct sum, there exists a homomorphism \( \phi : G \to G \) such that \( \phi(e_k) = f_k \) for all \( k \). Since the \( f_k \) generate \( G \), the map \( \phi \) is onto. Since \( G \) is a finite group, \( \phi \) must be injective as well. \( \square \)

Let \( A \in M_n(\mathbb{Q}(p)/\mathbb{Z}) \). The proofs of Lemmas A.3 and A.4 are based on the algorithm to reduce \( A \) to a diagonal matrix (or a block-diagonal matrix with blocks of size at most 2 when \( p = 2 \)) by conjugation or equivalently using the elementary row-column operations introduced above. This paves the way to proving Theorem 2.1 of [Wall 1963]. Let \( \text{diag}(a_1, \ldots, a_n) \) denote the diagonal \( n \times n \) matrix with diagonal entries \( a_1, \ldots, a_n \).

**Lemma A.3.** Let \( p \) be an odd prime. Let \( u_p \) be a quadratic nonresidue modulo \( p \). Let \( A \neq 0 \) be a symmetric matrix in \( M_n(\mathbb{Q}(p)/\mathbb{Z}) \). Let \( r_1 \) be the smallest number such that \( p^{r_1}A = 0 \).

(a) Then there exists a matrix \( S \in \text{GL}_n(\mathbb{Z}) \) such that \( S \mod p \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z}) \) and \( S^{tr}AS = \text{diag}(p^{-r_1}e_1, \ldots, p^{-r_n}e_n) \)

with \( r_1 \geq r_2 \geq \cdots \geq r_n \geq 0, e_j \in \{1, u_p, 0\}, \) and \( e_1 \neq 0 \).

(b) Let \((G,b)\) be a nondegenerate discriminant form where \( G \) is a \( p \)-group. Let \( G = \bigoplus_{j=1}^n \langle e_j \rangle \). Then there exists \( f_1, \ldots, f_n \in G \) such that \( G = \bigoplus_{j=1}^n \langle f_j \rangle \) and \( \text{Gram}_b(f_1, \ldots, f_n) = \text{diag}(p^{-r_1}e_1, \ldots, p^{-r_n}e_n) \) with \( r_1 \geq r_2 \geq \cdots \geq r_n > 0 \) and \( e_j \in \{1, u_p\} \).

**Proof.** (a) One proceeds by finding a pivot with the smallest \( p \)-valuation and then using this pivot to sweep out the rows and columns. Let \( A = ((a_{ij})) \in M_n(\mathbb{Q}(p)/\mathbb{Z}) \) be a symmetric nonzero matrix. Let \( r_1 > 0 \) be the smallest integer such that \( p^{r_1}A = 0 \). By induction on \( n \), it suffices to show that there is a sequence of row-column operations that converts \( A \) to a matrix of the form \( \begin{pmatrix} d_1 & 0 \\ 0 & A' \end{pmatrix} \) where \( d_1 = p^{-r_1} \) or \( d_1 = u_p^{-1}p^{-r_1} \) and \( A' \in M_{n-1}(\mathbb{Q}(p)/\mathbb{Z}) \) is a symmetric matrix such that \( p^{r_1}A' = 0 \).

**Claim** (finding a pivot). After changing \( A \) by row-column operations, we may assume that \( a_{11} = p^{-r_1} \) or \( a_{11} = u_p^{-1}p^{-r_1} \).
Proof of claim. If there is a diagonal entry \( a_{ii} \) such that \( v_p(a_{ii}) = -r_1 \), then apply \( \text{Flip}_{ii} \) to \( A \) to get \( v_p(a_{11}) = -r_1 \). Otherwise, there exists \( i \neq j \) such that \( v_p(a_{ii}) = -r_1 \) and \( v_p(a_{jj}) > -r_1 \) and \( v_p(a_{ij}) > -r_1 \). In this case, apply \( \text{Add}_{i,j}^{1,j} \) to \( A \). This changes the \((i, i)\)-th entry of the matrix from \( a_{ii} \) to \( (a_{ii} + 2a_{ij} + a_{jj}) \), whose \( p \)-valuation is \( -r_1 \). Now we apply \( \text{Flip}_{ii} \). Either way, we get \( v_p(a_{11}) = -r_1 \). Using the operation \( \text{Scale}_{\epsilon_i}^r \), we can change \( a_{11} \) to \( r^2 a_{11} \). By choosing \( r \) appropriately, we can make \( a_{11} = p^{-r_1} \) or \( a_{11} = u_p p^{-r_1} \). This proves the claim.

Sweeping out. Now \( a_{11} = \epsilon_1 p^{-r_1} \) with \( \epsilon_1 = 1 \) or \( u_p \). Since \( \epsilon_1 \) is relatively prime to \( p \), we can pick \( \epsilon' \in \mathbb{Z} \) such that \( \epsilon' \epsilon_1 \equiv 1 \mod p^{r_1} \). We can represent \( a_{ii} \) in the form \( \beta_i p^{-r_1} \) with \( \beta_i \in \mathbb{Z} \). We add \(-\beta_i \epsilon'\) times the first row to the \( i \)-th row and then add \(-\beta_i \epsilon'\) times the first column to the \( i \)-th column to make \( a_{ii} = 0 \) and \( a_{1i} = 0 \). Performing this operation for \( i = 2, 3, \ldots, n \) converts \( A \) to a matrix of the form \( \begin{pmatrix} \epsilon_1 p^{-r_1} & 0 & \cdots & 0 \\ 0 & A' \end{pmatrix} \). Finally note that the entries of \( A' \) are \( \mathbb{Z} \)-linear combinations of entries of \( A \), so \( p^{r_1} A = 0 \) implies \( p^{r_1} A' = 0 \). The row-column operations above correspond to conjugating \( A \) by certain matrices that are always invertible modulo \( p \).

Now part (a) follows by induction.

(b) Assume the setup of part (b). Let \( A = \text{Gram}_b(e_1, \ldots, e_n) \). Part (a) shows that the matrix \( A \) can be diagonalized by a sequence of row-column operations. Performing a row-column operation on \( \text{Gram}_b(e_1, \ldots, e_n) \) converts it to \( \text{Gram}_b(f_1, \ldots, f_n) \) where the \( f_j \) are given in the definition preceding Lemma A.2. We need to verify that all the row-column operation used in the proof of part (a) are valid (see the definition preceding Lemma A.2). While finding the pivot, we may perform \( \text{Add}_{i,j}^{1,j} \) to a matrix \( \text{Gram}_b(e_1, \ldots, e_n) \) if a nondiagonal entry of the matrix, say \( a_{ij} \), has the highest power of \( p \) in the denominator. Since \( a_{ij} = a_{ji} \), Lemma A.1(d) implies that \( \text{ord}(e_i) = \text{ord}(e_j) \). Since \( \langle e_i \rangle \cap \langle e_j \rangle = 0 \), Lemma A.1 implies that \( \text{ord}(e_i + e_j) = \text{ord}(e_i) \). Now Lemma A.2 implies that \( \text{Add}_{i,j}^{1,j} \) is valid.

While sweeping out, we perform the row-column operation \( \text{Add}_{i}^{-\beta_i \epsilon'} \), where \( a_{ii} = \beta_i p^{-r_1} \). This operation changes \( \text{Gram}_b(e_1, \ldots, e_n) \) to \( \text{Gram}_b(f_1, \ldots, f_n) \) where \( f_i = e_i - \beta_i \epsilon' e_1 \) and \( f_k = e_k \) for \( k \neq i \). Assume \( G = \bigoplus \langle e_k \rangle \). Since the discriminant form on \( G \) is nondegenerate, we have \( v_p(e_1) = -r_1 \) and hence \( v_p(-\beta_i \epsilon' e_1) = v_p(\beta_i) - r_1 \). Also, \( v_p(e_1) \leq v_p(a_{ii}) = v_p(\beta_i) - r_1 \). Since \( \langle e_i \rangle \cap (-\beta_i \epsilon' e_1) = \{0\} \), we have \( v_p(f_i) = \min\{v_p(e_i), v_p(-\beta_i \epsilon' e_1)\} = v_p(e_i) \). Lemma A.2 implies that the row-column operations performed while sweeping out are valid.

It follows that there exist \( f_1, \ldots, f_n \in G \) such that \( G = \bigoplus \langle f_j \rangle \) and that \( \text{Gram}_b(f_1, \ldots, f_n) = \text{diag}(p^{-r_1} \epsilon_1, \ldots, p^{-r_n} \epsilon_n) \) with \( r_1 \geq r_2 \geq \cdots \geq r_n \geq 0 \) and \( \epsilon_j \in \{1, u_p, 0\} \). Since \( (G, b) \) is nondegenerate, it follows that we must have \( \epsilon_j \neq 0 \) and \( \text{ord}(f_j) = p^{r_j} \) for all \( j \).

\footnote{This is the step in the argument that fails for \( p = 2 \).}
The next lemma handles the case of the prime \( p = 2 \). This proof is similar to the proof of Lemma A.3 but somewhat more complicated. We only elaborate on the necessary modifications.

**Lemma A.4.** (a) Let \( A \neq 0 \) be a symmetric matrix in \( M_n(\mathbb{Q}_2) / \mathbb{Z} \). Let \( m \) be the smallest number such that \( 2^m A = 0 \). Then there exists a matrix \( S \in GL_n(\mathbb{Z}) \) such that \( (S \mod 2) \in GL_n(\mathbb{Z}/2\mathbb{Z}) \) and \( S^rAS \) is block-diagonal with blocks of size 1 or 2. Each block is of the form

\[
(2^{-r} \delta) \quad \text{or} \quad 2^{-r}(\begin{smallmatrix} a & b \\ b & 2c \end{smallmatrix})
\]

where \( r \) is some nonnegative integer, \( a, b, \) and \( c \) are integers with \( b \) odd, and \( \delta \in \{0, \pm 1, \pm 5\} \). The largest \( r \) that occurs is equal to \( m \).

(b) Let \( (G, b) \) be a nondegenerate discriminant form where \( G \) is a 2-group. Let \( G = \bigoplus_{j=1}^n (e_j) \). Then there exists \( f_1, \ldots, f_n \in G \) such that \( G = \bigoplus_{j=1}^n (f_j) \) and \( \text{Gram}_b(f_1, \ldots, f_n) \) is a block-diagonal matrix with blocks of size 1 or 2. Each block is of the form given in (16) where \( r \) is some positive integer, \( a, b, \) and \( c \) are integers with \( b \) odd, and \( \delta \in \{\pm 1, \pm 5\} \).

**Proof.** (a) As above, we try to get a diagonal entry of \( A \) to have minimum 2-valuation. If this succeeds, then we can proceed with the sweep out as before and split off a \( 1 \times 1 \) block from \( A \). This procedure fails only in the situation when there exists \( i \neq j \) such that \( (a_{ij}, a_{ji}) = 2^{-m}(\begin{smallmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{smallmatrix}) \) where \( \alpha, \beta, \gamma \in \mathbb{Z}, \beta \) is odd, and all the diagonal entries of \( A \) have 2-valuation strictly larger than \(-m\). In this case, we can use row-column flips to move this \( 2 \times 2 \) submatrix to the upper-left corner of \( A \) so that \( (a_{11}, a_{12}) = 2^{-m}(\begin{smallmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{smallmatrix}) \) and then use this \( 2 \times 2 \) block to sweep out the first two rows and first two columns simultaneously.

This is how it is done. Suppose the first two entries of the \( i \)-th row are \( 2^{-m}(u, v) \) for \( u, v \in \mathbb{Z} \) where \( i > 2 \). We want to find \( r_1 \) and \( r_2 \) such that

\[
(r_1, r_2)2^{-m}(\begin{smallmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{smallmatrix}) = 2^{-m}(u, v) \mod \mathbb{Z}.
\]

This system can always be solved since the determinant \( (4\alpha\gamma - \beta^2) \) of the coefficient matrix is odd. Solving the equation yields

\[
(r_1, r_2) = d(2\gamma u - \beta v, 2\alpha v - \beta u)
\]

where \( d \) is an inverse of \( (4\alpha\gamma - \beta^2) \) modulo \( 2^m \). Now we add to the \( i \)-th row \(-r_1 \) times the first row and \(-r_2 \) times the second row and then perform the corresponding column operations to the \( i \)-th column. Verify that after these operations the first two entries of the \( i \)-th row and \( i \)-th column become zero. Part (a) follows.

(b) Let \( A = \text{Gram}_b(e_1, \ldots, e_n) \). The sweep-out operation above corresponds to replacing \( \text{Gram}_b(e_1, \ldots, e_n) \) by \( \text{Gram}_b(f_1, \ldots, f_n) \) where \( f_i = e_i + r_1e_1 + r_2e_2 \) and \( f_j = e_j \) for all \( j \neq i \). The extra work needed in part (b) is to check that
this operation is valid. Note that, since $2^m$ is the maximum denominator in $A$, \( \text{order}(e_1) = \text{order}(e_2) = 2^m \). Suppose \( \text{order}(e_i) = 2^k \). Then \( u \) and \( v \) must be divisible by \( 2^{m-k} \) because the entries of the \( i \)-th row can have denominator at most \( 2^k \). From the formula for \( r_1 \) and \( r_2 \), we see that \( 2^{m-k} \) divides \( r_1 \) and \( r_2 \). It follows that \( 2^k f_i = 0 \). On the other hand, since \( \langle e_i \rangle \cap \langle e_1, e_2 \rangle = 0 \), we have \( \text{order}(f_i) \geq 2^k \). So \( \text{order}(f_i) = \text{order}(e_i) \) and Lemma A.2 implies the sweep-out operations using \( 2 \times 2 \) blocks described above are valid. \( \square \)

For \( p \)-groups with \( p \) odd, Wall’s Theorem 2.1(a) follows from Lemma A.3. For \( p = 2 \), we need Lemma A.4 and we also need Lemmas 2.2 and A.7, which describe the irreducible nondegenerate quadratic and bilinear forms on \((\mathbb{Z}/2^r\mathbb{Z})^2\). Proving Lemmas 2.2 and A.7 depends on solving a system of congruence equations modulo \( 2^n \) for all \( n \). This can be done by a standard application of Hensel’s lemma, which we now state in the necessary form.

**Lemma A.5** (Hensel’s lemma). Let \( p \) be a prime. Let \( f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n] \) and \( f = (f_1, \ldots, f_m) \). Let \( Df = ((\partial f_i/\partial x_j)) \) be the Jacobian of \( f \). Let \( t_1 \in \mathbb{Z}^n \) such that \( f(t_1) \equiv 0 \mod p \) and the \( m \times n \) matrix \( (Df(t_1) \mod p) \) has rank \( m \) over \( \mathbb{F}_p \). Then, for all \( k \geq 1 \), there exists \( t_k \in \mathbb{Z}^n \) such that \( t_{k+1} \equiv t_k \mod p^k \) and \( f(t_k) \equiv 0 \mod p^k \).

The proof is omitted.

**Lemma A.6.** \( \text{ (a) Let } s = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \text{ be a } 2 \times 2 \text{ matrix of indeterminates. Let} \)

\[
(A(s), B(s), C(s)) = (s_{11}^2 + s_{11}s_{12} + s_{12}^2, 2s_{11}s_{21} + s_{11}s_{22} + s_{21}s_{12} + 2s_{12}s_{22}, s_{21}^2 + s_{21}s_{22} + s_{22}^2).
\]

Let \( A, B, \) and \( C \) be odd integers. Let \( n \geq 1 \). Then the equation

\[
(A(s), B(s), C(s)) \equiv (A, B, C) \mod 2^n
\]  \hspace{2cm} (17)

has a solution \( S \in M_2(\mathbb{Z}) \) such that \( S \equiv I \mod 2 \) (here \( I \) denotes the \( 2 \times 2 \) identity matrix).

\( \text{(b) Let } s = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \text{ be a } 2 \times 2 \text{ matrix of indeterminates. Let} \)

\[
(A(s), B(s), C(s)) = (s_{11}s_{12}, s_{11}s_{22} + s_{21}s_{12}, s_{21}s_{22}).
\]

Let \( A, B, \) and \( C \) be integers such that \( B \) is odd and \( AC \) is even. Let \( n \geq 1 \). Then the equation

\[
(A(s), B(s), C(s)) \equiv (A, B, C) \mod 2^n
\]  \hspace{2cm} (18)

has a solution \( S \in M_2(\mathbb{Z}) \) such that \( S \equiv \begin{pmatrix} A & 1 \\ 1 & C \end{pmatrix} \mod 2 \).
Proof. (a) Apply Hensel’s lemma to \( f = (f_1, f_2, f_3) \) for \( f_1(s) = s_{11}^2 + s_{11}s_{12} + s_{12}^2 - A, \) \( f_2(s) = 2s_{11}s_{21} + s_{11}s_{22} + s_{21}s_{12} + 2s_{12}s_{22} - B, \) and \( f_3(s) = s_{21}^2 + s_{21}s_{22} + s_{22}^2 - C. \) Since \( A, B, \) and \( C \) are odd, \( s = I \) is a solution to \( f(s) \equiv 0 \mod 2. \) One computes

\[
Df = \begin{pmatrix}
2s_{11} + s_{12} & 0 & s_{11} + 2s_{12} & 0 \\
2s_{21} + s_{22} & 2s_{11} + s_{12} & s_{21} + 2s_{22} & s_{11} + 2s_{12} \\
0 & 2s_{21} + s_{22} & 0 & s_{21} + 2s_{22}
\end{pmatrix},
\]

so \( Df(I) \equiv \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \mod 2, \)

which has rank 3. For part (b), let \( f_1(s) = s_{11}s_{12} - A, \) \( f_2(s) = s_{11}s_{22} + s_{21}s_{12} - B, \) and \( f_3(s) = s_{21}s_{22} - C. \) Since \( B \) is odd and \( AC \) is even, \( s_* = (A \ 1 \ C) \) satisfies \( f(s_*) \equiv 0 \mod 2. \) One computes

\[
Df = \begin{pmatrix}
s_{12} & 0 & s_{11} & 0 \\
s_{22} & s_{12} & s_{21} & s_{11} \\
0 & s_{22} & 0 & s_{21}
\end{pmatrix}, \quad \text{so} \quad Df(s_*) \equiv \begin{pmatrix} 1 & 0 & A & 0 \\ C & 1 & 1 & A \\ 0 & C & 0 & 1 \end{pmatrix} \mod 2.
\]

Since \( A \) or \( C \) is even, either the second or the third column of the above matrix is equal to \((0, 1, 0)^t\). So the matrix \((Df(s_*) \mod 2)\) has rank 3.

Proof of Lemma 2.2. (a) Note that \( 2q(x) = \partial q(x, x) \in 2^{-r}Z/Z. \) So \( q(x) \) takes values in \( 2^{-r-1}Z/Z, \) and

\[
q(x_1, x_2) = 2^{-r-1}(\alpha x_1^2 + 2Bx_1x_2 + \gamma x_2^2)
\]

where \( q(1, 0) = 2^{-r-1} \alpha, \) \( q(0, 1) = 2^{-r-1} \gamma, \) and \( \partial q((1, 0), (0, 1)) = 2^{-r}B. \) Suppose \( \alpha \) is odd. Let \( \tilde{\alpha} \) be an inverse of \( \alpha \) modulo \( 2^{r+1}. \) Then we can complete squares to write

\[
q(x_1, x_2) = 2^{-r-1}(\alpha(x_1 + B\tilde{\alpha}x_2)^2 + (\gamma - B^2\tilde{\alpha})x_2^2).
\]

This contradicts the irreducibility of \( q, \) and thus, \( \alpha \) has to be even. For the same reason, \( \gamma \) has to be even. So we can write

\[
q(x_1, x_2) = 2^{-r}(Ax_1^2 + Bx_1x_2 + Cx_2^2).
\]

If \( A, B, \) and \( C \) are all even, then \( \partial q \) takes values in \( 2^{-r+1}Z/Z \) and hence cannot be nondegenerate. If \( B \) is even, then \( A \) or \( C \) must be odd, and we can once again complete squares (as above) and decompose \((G, q)\) into an orthogonal direct sum of two metric groups. So \( B \) must be odd.

First, suppose \( AC \) is odd. Let \( F(x_1, x_2) = x_1^2 + x_1x_2 + x_2^2. \) Let \( s = (s_{11} \ s_{12}). \) Note that

\[
F((x_1, x_2)s) = A(s)x_1^2 + B(s)x_1x_2 + C(s)x_2^2
\]
where \((A(s), B(s), C(s))\) are the polynomials given in Lemma A.6(a). We want to show \(q(x_1, x_2) \simeq 2^{-r} F(x_1, x_2)\). This is equivalent to finding a matrix \(s \in M_2(\mathbb{Z})\) with odd determinant such that

\[
F((x_1, x_2)s) \equiv (Ax_1^2 + Bx_1x_2 + Cx_2^2) \mod 2^r
\]

or equivalently \((A(s), B(s), C(s)) \equiv (A, B, C) \mod 2^r\). The proof follows from Lemma A.6(a) if \(AC\) is odd. If \(AC\) is even, then the proof is identical, using \(F(x_1, x_2) = x_1x_2\) and using part (b) of Lemma A.6 instead of part (a). □

**Lemma A.7.** (a) Let \(A, B,\) and \(C\) be odd integers. Let \(r \geq 1\). Then there exists a matrix \(S \in M_2(\mathbb{Z})\) such that \(S\bigl(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\bigr)\bigl(S^{\text{tr}} \equiv \bigl(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\bigr) \mod 2^r\text{ and } S \equiv I \mod 2\).

(b) Let \(A, B,\) and \(C\) be integers such that \(AC\) is even and \(B\) is odd. Let \(r \geq 1\). Then there exists a matrix \(S \in M_2(\mathbb{Z})\) such that \(S\bigl(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\bigr)\bigl(S^{\text{tr}} \equiv \bigl(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\bigr) \mod 2^r\text{ and } S \equiv \bigl(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\bigr) \mod 2\).

**Proof.** (a) The congruences in part (a) translate into \(A(s) \equiv A \mod 2^{r-1}, B(s) \equiv B \mod 2^r\), and \(C(s) = C \mod 2^{r-1}\) where \(A(s), B(s),\) and \(C(s)\) are as in Lemma A.6(a). Part (a) follows from Lemma A.6. Similarly part (b) follows from part (b) of Lemma A.6. □

**Proof of Theorem 2.1.** (a) Let \((G, b)\) be a nondegenerate discriminant form. It suffices to decompose \((G, b)\) into irreducibles when \(G\) is a \(p\)-group for some prime \(p\). First suppose \(p\) is odd. From Lemma A.3, it follows that there exist \(f_1, \ldots, f_n \in G\) such that \(G = \bigoplus\langle f_j \rangle\) and \(\text{Gram}_b(f_1, \ldots, f_n) = \text{diag}(p^{-r_1} \epsilon_1, \ldots, p^{-r_n} \epsilon_n)\) with \(r_1 \geq r_2 \geq \cdots \geq r_n \geq 0\) and \(\epsilon_j \in \{1, u_p\}\). Since \((G, b)\) is nondegenerate, it follows that we must have order \(f_j = p^{r_j}\) for all \(j\). Thus, \((G, b)\) is an orthogonal direct sum of the rank-1 discriminant forms \((\langle f_j \rangle, b|_{\langle f_j \rangle})\) and each of these are of type \(A\) or \(B\). This completes the argument for odd \(p\).

Now we consider the case \(p = 2\). From Lemma A.4, it follows that there exist \(f_1, \ldots, f_n \in G\) such that \(G = \bigoplus\langle f_j \rangle\) and \(\text{Gram}_b(f_1, \ldots, f_n)\) is block-diagonal with blocks of size 1 or 2 as given in Lemma A.4. Accordingly, \((G, b)\) is an orthogonal direct sum of rank-1 or -2 discriminant forms spanned by one or two of the \(f_j\). The rank-1 forms among these are clearly of type \(A\), \(B\), \(C\), or \(D\). The Gram matrix of a rank-2 piece has the form \(2^{-r} \bigl(\begin{smallmatrix} 2a & b \\ B & 2c \end{smallmatrix}\bigr)\). Lemma A.7 shows that such a rank-2 piece is either of type \(E\) or \(F\).

(b) Let \((G, q)\) be a metric group. By part (a), \((G, \partial q)\) is an orthogonal direct sum of irreducible forms \((G_j, b_j)\). Each \(G_j\) is a homogeneous \(p\)-group of rank 1 or 2. Further, \(G_j\) can have rank 2 only if \(p = 2\). It follows that \((G, q)\) is also an orthogonal direct sum of \((G_j, q_j)\) where \(q_j = q|_{G_j}\). The rank-1 forms are clearly of type \(A\), \(B\), \(C\), or \(D\). The rank-2 forms either decompose into two rank-1 forms or they are irreducible as metric groups. In the latter case, Lemma 2.2 shows that \((G_j, q_j)\) is of type \(E\) or \(F\). □
Acknowledgments

This work would not be possible without the guidance of Siu-Hung Ng during the inception of the project. We are grateful to him for suggesting the problem for this project. We would also like to thank him for his encouragement, for many useful conversations, and for pointing out many references. We would like to thank both of our referees for their thoughtful reviews. The referee’s suggested revision of an earlier draft led to a simplification of our previous proof and a significant reduction in preparatory lemmas needed.

References

Indicators of Tambara–Yamagami categories and Gauss sums


Communicated by Susan Montgomery
Received 2014-07-24 Revised 2015-06-18 Accepted 2015-07-25

tathagat@iastate.edu Department of Mathematics, Iowa State University, Ames, IA 50011, United States

johnsor@grace.edu Department of Mathematics, Grace College, Winona Lake, IN 46590, United States
G-valued crystalline representations with minuscule $p$-adic Hodge type 1741

Brandon Levin

Indicators of Tambara–Yamagami categories and Gauss sums 1793

Tathagata Basak and Ryan Johnson

The number of nonzero coefficients of modular forms (mod $p$) 1825

Joël Bellaïche and Kannan Soundararajan

Noetherianity for infinite-dimensional toric varieties 1857

Jan Draisma, Rob Eggermont, Robert Krone and Anton Leykin

On differential modules associated to de Rham representations in the imperfect residue field case 1881

Shun Ohkubo