Quaternion Gauss Sums

Alexander Pilakoutas   Simon Myerson

October 24, 2023

Abstract

This research paper explores "quaternion Gauss sums", which extend the quadratic Gauss sum to Hurwitz quaternions. The study investigates the properties of Quaternion Gauss sums, including their behavior under similarity transformations, multiplicativity, and reduced forms for diagonal matrices. Practical applications are considered, such as solution counting in quaternion/matrix equations within prime power quotients. The research also provides a computational method for calculating quaternion Gauss sums, yielding data that informs conjectures about Gauss sum values and relates them to existing notions of matrix Gauss sums.

Contents

1 Introduction

The (quadratic) Gauss sum is a sum over the squares of nth roots of unity. More formally we define it as

$$G(a,q)=\sum_{m=0}^{m=q-1}e_q(am^2)$$

where $e_q=e^{2\pi ix/q}$.

This may look a little contrived, but as Gauss found out, they encode important information about the arithmetic of $\mathbb{Z}/p\mathbb{Z}$. Gauss was quickly able to determine the identity $g(1,p)^2=(-1/p)p$, and it led him to (another) proof of quadratic reciprocity. For a comprehensive survey of this, read [1].

2 Extending Gauss Sums to Hurwitz Quaternions

The idea of this paper is to extend this kind of sum to the (Hurwitz) Quaternions. Quaternions are a type of 4-dimensional number system, much like complex numbers are a 2-dimensional number system, and the Hurwitz quaternions are an extension of the concept of integers to quaternions.

More concretely the Quaternions are a ring that can be represented as $\{a+bi+cj+dk : a,b,c,d\in\mathbb{R}\}$ where i, j, and k are defined so that $i^2=j^2=k^2=ijk=-1$ (note that this implies multiplication is non-commutative as $ij=k$ and $ji=-k$). Now, the Hurwitz Quaternions are defined as $\{a+bi+cj+dk : a,b,c,d\in\mathbb{Z}\text{ or }\mathbb{Z}+\frac{1}{2}\}$ under the same operations.

However, the property we use about them is an isomorphism of spaces:

$$\frac{H}{qH}\cong M_2(\mathbb{Z}/q\mathbb{Z})\quad\text{(for odd }q\text{)}.$$

For more information about the Hurwitz Quaternions see[5] (the definition of Hurwitz Quaternions can be found on page 2 and the isomorphism on page 29).

Now, we aim to create a generalization of the Gauss sum for these matrix rings. Rewriting the formula a bit, we get:

$$G(a,q)=\sum_{m\in\mathbb{Z}/q\mathbb{Z}}e_q(am^2).$$

and by substituting, $M_2(\mathbb{Z}/q\mathbb{Z})$, we get:

$$G_2(a,q)=\sum_{m\in M_2(\mathbb{Z}/q\mathbb{Z})}e_q(am^2),$$

but this doesn't quite make sense. What does $e_q(am^2)$ even mean when am^2 is in $M_2(\mathbb{Z}/q\mathbb{Z})$? So, we extend it to this form:

$$G_2(a,m)=\sum_{m\in M_2(\mathbb{Z}/q\mathbb{Z})}e_q(\mathrm{Tr}(am^2)).$$

3 Properties of the Quaternion Gauss Sum

3.1 Similar inputs over m have equal Gauss sums

To see this, we will have to take advantage of the trace identity $\operatorname{Tr} AB = \operatorname{Tr} BA$. Suppose b is similar to a, meaning that $b = uau^{-1}$ for some u that is a unit in $M_2(\mathbb{Z}/q\mathbb{Z})$.

$$\begin{aligned} G_2(b,q) &= \sum_{m \in M_2(\mathbb{Z}/q\mathbb{Z})} e_q(\operatorname{Tr}(bm^2)) \\ &= \sum_{m \in M_2(\mathbb{Z}/q\mathbb{Z})} e_q(\operatorname{Tr}((uau^{-1})m^2)) \\ &= \sum_{m \in M_2(\mathbb{Z}/q\mathbb{Z})} e_q(\operatorname{Tr}(aum^2u^{-1}) \\ &= \sum_{m \in M_2(\mathbb{Z}/q\mathbb{Z})} e_q(\operatorname{Tr}(a(umu^{-1})^2)) \\ &= G_2(a,q) \end{aligned}$$

Let us denote by $\sim$ an equivalence relation over $M_2(\mathbb{Z}/q\mathbb{Z})$ such that $a \sim b$ if and only if $G_2(a,q) = G_2(b,q)$. Now, as similar matrices have the same evaluation, this means that the equivalence relations are closed under conjugation, which means that the conjugacy class of some element a is contained within the equivalence class of a. In particular, any equivalence class is nothing but the union of disjoint conjugacy classes.

3.2 Multiplicativity

Suppose $q = q_1q_2$ and $(q_1, q_2) = 1$. Then, $G_2(a, q_1q_2) = G_2(aq_2, q_1)G_2(aq_1, q_2)$.

The Chinese Remainder Theorem gives an isomorphism, ϕ, from $\mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$ to $\mathbb{Z}/q\mathbb{Z}$, where $\overline{q_1}$ and $\overline{q_2}$ are the multiplicative inverses of q_1 mod q_2 and q_1 mod q_2, respectively.

$\phi(j,k) = q_2\overline{q_1}j + q_1\overline{q_2}k$

This can be extended to matrix rings $M_n(\mathbb{Z}/q\mathbb{Z}) \cong M_n(\mathbb{Z}/q_1\mathbb{Z}) \times M_n(\mathbb{Z}/q_2\mathbb{Z})$ by the same isomorphism (changing the domain and range).

$$\begin{aligned}
\sum_{m\in M_2(\mathbb{Z}/q\mathbb{Z})} e_q(\mathrm{Tr}(am^2)) &= \sum_{(j,k)\in(M_2(\mathbb{Z}/q_1\mathbb{Z})\times M_2(\mathbb{Z}/q_2\mathbb{Z}))} e_q\left(\mathrm{Tr}\left(a(q_2\overline{q_1}j+q_1\overline{q_2}k)^2\right)\right)\\
&= \sum_{(j,k)\in(M_2(\mathbb{Z}/q_1\mathbb{Z})\times M_2(\mathbb{Z}/q_2\mathbb{Z}))} e_q\left(\mathrm{Tr}\left(a(q_2\overline{q_1}j)^2+a(q_1\overline{q_2}k)^2\right.\right.\\
&\quad +q(a\overline{q_1}\overline{q_2})jk+q(a\overline{q_1}\overline{q_2})kj))\\
&= \sum_{j\in M_2(\mathbb{Z}/q_1\mathbb{Z})} e_q\left(a(q_2\overline{q_1}j)^2\right)\sum_{k\in M_2(\mathbb{Z}/q_2\mathbb{Z})} e_q\left(a(q_1\overline{q_2}k)^2\right)\\
&= \sum_{j\in M_2(\mathbb{Z}/q_1\mathbb{Z})} e_{q_1}\left(a(\overline{q_1}j)^2\right)\sum_{k\in M_2(\mathbb{Z}/q_2\mathbb{Z})} e_{q_2}\left(a(\overline{q_2}k)^2\right)\\
&= G_2(aq_2,q_1)G_2(aq_1,q_2)
\end{aligned}$$

3.3 Reduced Form for Diagonal Matrices

Let $a=\begin{bmatrix}a_1 & 0\\ 0 & a_2\end{bmatrix}$,

$$\mathrm{Tr}(\left(\begin{bmatrix}a_1 & 0\\ 0 & a_2\end{bmatrix}\begin{bmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{bmatrix}\begin{bmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{bmatrix}\right) = a_1m_{11}^2+a_2m_{22}^2+a_1m_{12}m_{21}+a_2m_{12}m_{21}$$

Then, $G_2(a,m)=G_2(a_1,m)G_2(a_2,m)\sum_{m_{12},m_{21}\in\mathbb{Z}/m\mathbb{Z})} e_m((a_1+a_2)m_{12}m_{21})$.

3.4 Application to Solution Counting

Gauss Sums can be applied to counting solutions of certain kinds of quaternion/matrix equations (mod q)

Lemma: $$\sum_{a\in M_2(\mathbb{Z}/m\mathbb{Z})} e_q(\mathrm{Tr}(am)) = \begin{cases} q^4, & \text{if } q \text{ divides } m \text{ on the left,}\\ 0, & \text{otherwise.}\end{cases}$$

$$\begin{aligned}
\sum_{a\in M_2(\mathbb{Z}/m\mathbb{Z})} e_q(\mathrm{Tr}(am)) &= \sum_{a\in M_2(\mathbb{Z}/q\mathbb{Z})} e_q(a_{11}m_{11}+a_{12}m_{12}+a_{21}m_{21}+a_{22}m_{22})\\
&= \sum_{a\in\mathbb{Z}/q\mathbb{Z}} e_q\left(a(m_{11})\right)\dots\sum_{a\in\mathbb{Z}/q\mathbb{Z}} e_q\left(a(m_{22})\right)
\end{aligned}$$

and then the lemma follow by using the property that
$\sum_{a\in\mathbb{Z}/q\mathbb{Z}} e_q\left(a(m)\right) = \begin{cases} q, & \text{if } q|m\\ 0, & \text{otherwise}\end{cases}$

Let $Q(q,c)$ be the number of solutions to $c_1x_1^2 + \ldots + c_nx_n^2 \equiv 0 \pmod{q}$ (choosing c_i and x_i in $M_2(\mathbb{Z}/q\mathbb{Z})$). We define being identical to $0 \pmod{q}$ as simply being divisible on the left (or right as q commutes) by q.

Now, we have a generating function for Q which can be expressed as a product of Gauss Sums:

$$\begin{aligned} Q(q,c) &= \sum_{\overline{x}\in(M_2(\mathbb{Z}/q\mathbb{Z}))^n} \frac{1}{q^4} \sum_{a\in M_2(\mathbb{Z}/q\mathbb{Z})} e_q\left(\mathrm{Tr}\left(a(c_1x_1^2 + \ldots + c_nx_n^2)\right)\right) \\ &= \frac{1}{q^4} \sum_{a\in M_2(\mathbb{Z}/q\mathbb{Z})} G_2(ac_1,m)\ldots G_2(ac_2,m) \end{aligned}$$

4 Calculation of Quaternion Gauss Sum

Using property 3.1 and 3.3, we created a program[1] to calculate all conjugacy classes in $M_2(\mathbb{Z}/q\mathbb{Z})$ and then calculate the Gauss sums for each of these conjugacy classes given a q.

We now focus on odd prime power quotients (i.e., $q = p^k$ for p an odd prime). This is justified by property 3.2, and we make the following conjectures based on the collected data.

- If trace$(a) = 0$, then $G_2(a,m) = p^3$ (if $a \neq 0$, in this case $G_2(a,m)$ is trivially p^4).
- If a is invertible (i.e (det(a),m)=1 [2]), then $G_2(a,m) = \pm(\text{trace}(a),m)m^2$.
- If a is invertible and $(\text{trace}(a),m) = 1$, then $G_2(a,m) = (\frac{-\det(a)}{m})m^2$.
- If $(\frac{\det(a)}{m}) = 1$, then $G_2(a,m) = (\frac{-1}{m})(\text{trace}(a),m)m^2$.

5 Relation to Existing Matrix Gauss Sums

A notion of Gauss sum for matrices with elements in finite fields has been discussed in [3].

This notion of gauss sum is equivalent to the quaternion gauss sum for odd prime quotients and in fact using this source we can see, by Lemma 10 (page 195) that in this case $G_2(a,p)$ can determined explicitly as:

[1] The program and the data in the case of m=27 can be found at https://github.com/Pilkied/Matrix-Gauss-Sums. In fact, it uses a generalization of 3.3 to $n \times n$ matrices with $j \in \{1,\ldots,m\}$, $i \in \{1,\ldots,j-1,j+1,\ldots,m\}$ where $a_{ij} = 0$ and $a_{ji} = 0$ to calculate the generalized Matrix Gauss sums $G_k(a,q) = \sum_{m\in M_k(\mathbb{Z}/q\mathbb{Z})} e_q(\text{trace}(am^2))$.

$$G_2(a,p) = \begin{cases} p^4 & \text{if } a = 0 \\ p^3 & \text{if } a \neq 0 \text{ and } T = 0 \\ p^2(\frac{-D}{p}) & \text{if } T \neq 0 \text{ and } D \neq 0 \end{cases}$$

Where T is $\operatorname{Tr} a$ and D is $\det a$. This corroborates the conjectures.

Another notion of a Gauss Sum for matrices has been discussed in [4]. These Gauss sums however are taken over over the general linear group of matrices with elements in a finite field and have a different form. Specialising (again) to the 2x2 case with odd prime quotient this kind of sum can be written (and evaluated using Theorem 2.1 in [4]) as:

$\sum_{m \in \mathrm{M}_2(\mathbb{Z}/q\mathbb{Z})} (\frac{\det(m)}{q}) \operatorname{Tr}(am) = \sum_{m \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})} (\frac{\det(m)}{q}) \operatorname{Tr}(am) = q^2(\frac{-D}{q})$

This is valid for invertible a (otherwise the sum evaluates to 0) and is equal to the quaternion Gauss sum when $\operatorname{Tr} a \neq 0$.

References

[1] Bruce C. Berndt and Ronald J. Evans. The determination of Gauss sums. *Bulletin (New Series) of the American Mathematical Society*, 5(2):107 – 129, 1981.

[2] W. Brown. *Matrices over Commutative Rings*. Chapman & Hall Pure and Applied Mathematics. Taylor & Francis, 1992.

[3] Mitsuru Kuroda. Quadratic gauss sums on matrices. *Linear Algebra and Its Applications*, 384:187–198, 06 2004.

[4] Yan Li and Su Hu. Gauss sums over some matrix groups. *Journal of Number Theory*, 132(12):2967–2976, 2012.

[5] Nikolaos Tsopanidis. *The Hurwitz and Lipschitz integers and some applications, PHD*. PhD thesis, Universidade do Porto, 2020.