Gauss Sum Tables in Finite Fields

James Evans, *put your name here*

University of Michigan

February 21, 2025

Introduction

- Gauss sums are essential in number theory and finite field analysis.
- We break down key concepts before defining Gauss sums rigorously.
- This will provide a structured understanding before analyzing the code.

Research Goals

University of Michigan LoG(M)

James Evans, *put your name here*

- **Reproduce Counterexamples:** Verify the correctness of prior counterexamples found by **Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang** for $n = 2$ [2].
- **Generalization to Larger n:** Investigate whether these failures extend to larger values of n.
- **Refining Conjectures:** Develop a refined conjecture specifying the conditions under which the theorem holds or fails.
- **Computational Exploration:** Utilize SageMath and other computational tools to generate and analyze new examples.

Definition of a Group

University of Michigan LoG(M)

James Evans, *put your name here*

- A **group** is a set G with an operation $\cdot$ satisfying:
  1. Closure: If $a, b \in G$, then $a \cdot b \in G$.
  2. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
  3. Identity: There exists an element e such that $e \cdot a = a \cdot e = a$ for all $a \in G$.
  4. Inverse: Each $a \in G$ has an inverse a^{-1} such that $a \cdot a^{-1} = e$.
- A group is **abelian** if $a \cdot b = b \cdot a$ for all $a, b \in G$.
- A group is **cyclic** if it can be generated by a single element.

Definition of a Field

- A **field** F is a set with two operations: addition and multiplication.
- It satisfies:
  1. $(F, +)$ is an abelian group (additive group).
  2. $(F \setminus \{0\}, \cdot)$ is an abelian group (multiplicative group).
  3. Distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.
- A **finite field** (or Galois field) $GF(q)$ has q elements, where q is a prime power.

Example: The Field $GF(3)$

University of Michigan LoG(M)

James Evans, *put your name here*

- Elements: $GF(3) = \{0, 1, 2\}$.
- **Identity Elements:**
  - Additive identity: 0, since $a + 0 = a$ for all a.
  - Multiplicative identity: 1, since $a \cdot 1 = a$ for all $a \neq 0$.
- **Inverses:**
  - Additive inverse: $1^{-1} = 2$, $2^{-1} = 1 \pmod 3$, $0^{-1} = 0$.
  - Multiplicative inverse: $1^{-1} = 1$, $2^{-1} = 2 \pmod 3$.
- **Example of Closure and Associativity:**
  - Closure: $1 + 2 = 0 \mod 3$, stays in $GF(3)$.
  - Associativity: $(1 + 2) + 1 = 0 + 1 = 1$ is the same as $1 + (2 + 1) = 1 + 0 = 1$.
- This satisfies all field axioms.

Gauss Sums: Definition

University of Michigan LoG(M)

James Evans, *put your name here*

- The Gauss sum is an element of $\mathbb{C}^*$ and is associated with the field $GF(q^m)$.
- Given a finite field $GF(q^m)$ and two characters:
  - Multiplicative character $\alpha : GF(q^m)^* \to \mathbb{C}^*$.
  - Additive character $\psi : GF(q^m) \to \mathbb{C}^*$.
  - Auxiliary multiplicative character $\theta : GF(q^m)^* \to \mathbb{C}^*$.
- The Gauss sum is defined as:

$$G(\alpha, \theta, \psi) = \sum_{a \in GF(q^m)^*} \alpha(a)\theta(a)\psi(a).$$

- The function θ is an additional multiplicative character used to adjust contributions in the sum.

Twisted Gauss Sum

University of Michigan LoG(M)

James Evans, *put your name here*

Definition: The twisted Gauss sum is an element of $\mathbb{C}^*$ and is associated with the field $GF(q^2)$. If $G(\alpha, \psi)$ is a standard Gauss sum for a multiplicative character α and an additive character ψ, a twisted Gauss sum is of the form:

$$G(\Theta, \alpha, \Psi) = \sum_{x \in GF(q^2)^*} \Theta(x) \cdot \alpha(N(x)) \cdot \Psi(\mathrm{tr}(x)), \qquad (1)$$

where:

- Θ and α are multiplicative characters of $GF(q^2)^*$, mapping $GF(q^2)^*$ to $\mathbb{C}^*$.
- Ψ is an additive character of $GF(q^2)$, mapping $GF(q^2)$ to $\mathbb{C}^*$.
- $N(x)$ represents the norm function $N : GF(q^2) \to GF(q)$.
- $\mathrm{tr}(x)$ represents the trace function $\mathrm{tr} : GF(q^2) \to GF(q)$.

The Converse Theorem of Gauss Sums [1]

University of Michigan LoG(M)

James Evans, *put your name here*

Theorem

Consider two multiplicative characters θ_1 and θ_2 defined on the multiplicative group of a finite field $GF(q^m)^*$. If for all additive characters ψ on $GF(q^m)$ and all multiplicative characters α on $GF(q^m)^*$, the following equality holds:

$$G(\alpha, \theta_1, \psi) = G(\alpha, \theta_2, \psi),$$

$$\sum_{a \in GF(q^m)^*} \alpha(a)\theta_1(a)\psi(a) = \sum_{a \in GF(q^m)^*} \alpha(a)\theta_2(a)\psi(a),$$

then it must be the case that θ_1 and θ_2 are identical, or at least related by a well-understood transformation.

Macro Purpose of the Code

- The purpose of this code is to generate a **table of Gauss sums** for a finite field $GF(q^2)$.
- It systematically computes Gauss sums for **different character pairs**:
  - Multiplicative characters α and θ.
  - Additive character ψ.
- The table stores values of the twisted Gauss sum:

$$G(\alpha, \theta, \psi) = \sum_{a \in GF(q^2)^*} \alpha(a)\theta(a)\psi(a).$$

Constructing the Table

University of Michigan LoG(M)

James Evans, *put your name here*

- The multiplicative generator of $GF(q^2)^*$ is used to systematically construct different possible characters.
- Raising the generator to different powers gives distinct character mappings for α and θ.
- Each row and each column corresponds to a different possible character created from the generator.
- An entry in the table represents the twisted Gauss sum for the combination of those two particular characters.

Relation to the Converse Theorem

- This structure allows us to compare different character mappings.
- The table provides a framework for analyzing the behavior of twisted Gauss sums in relation to the Converse Theorem.
- Understanding how character mappings interact helps in proving or refuting generalizations of Gauss sum identities.

Gauss Sum Table Example Output

University of Michigan LoG(M)

James Evans, *put your name here*

$\theta \backslash \alpha$	0	1	$\dots$	$q-1$
0	$G(0,0)$	$G(0,1)$	$\dots$	$G(0,q-1)$
1	$G(1,0)$	$G(1,1)$	$\dots$	$G(1,q-1)$
2	$G(2,0)$	$G(2,1)$	$\dots$	$G(2,q-1)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
q^2-1	$G(q^2-1,0)$	$G(q^2-1,1)$	$\dots$	$G(q^2-1,q-1)$

Applying the Converse Theorem

University of Michigan LoG(M)

James Evans, *put your name here*

- The Converse Theorem of Gauss Sums states that if two multiplicative characters produce identical Gauss sums across all additive characters ψ and all multiplicative characters α, then θ_1 and θ_2 must be identical or related by a well-understood transformation.
- In the Gauss sum table, each row corresponds to a different multiplicative character θ, and each column corresponds to a different multiplicative character α.
- To apply the theorem:
  - Identify two rows in the table where all entries match across all ψ and α values.
  - Highlight these rows and investigate the corresponding θ_1 and θ_2.
  - Check whether θ_1 and θ_2 are identical or related by a known transformation.
- This process helps verify whether the Converse Theorem holds in our computed Gauss sum table.

References

[1] Chufeng Nien and Lei Zhang. “Converse Theorem Meets Gauss Sums (with an appendix by Zhiwei Yun).” *arXiv preprint arXiv:1806.04850* (2018). `https://arxiv.org/abs/1806.04850`.

[2] Elad Zelingher. “Failure of Converse Theorems of Gauss Sums Modulo ℓ.” Preprint, available from `https://lsa.umich.edu/content/dam/math-assets/logm/wn2025/ELAD-ZELINGHER.pdf`, 2025.