GAUSS SUMS AND KLOOSTERMAN SUMS

HYUN JONG KIM

August 31, 2025

Contents

The purpose of this document is to list definitions of variants of Gauss sums and Kloosterman sums and to discuss how Gauss sums and Kloosterman sums connect to various problems.

Supposedly, the following are some applications/implications of Gauss sums:

1. Proving reciprocity laws: Gauss sums can be used to prove quadratic, cubic, and quartic reciprocity laws, central results in number theory.
2. Counting solutions to equations: They help calculate the number of solutions to certain polynomial equations over finite fields.
3. Relation to exponential sums: Gauss sums appear in the evaluation and estimation of exponential sums, pivotal in analytic number theory.
4. Connection to coding theory: Gauss sums have applications in the study of cyclic codes and related algebraic structures.
5. Transforming sums for stronger bounds: They can convert binomial sums into multiple Kloosterman sums to achieve better estimates, sometimes surpassing the Weil bound.

The following are applications/implications of Kloosterman sums:

1. Solving quadratic form problems: Originally introduced by Kloosterman, these sums were used to solve problems about representations by quadratic forms.

2. Bounds on exponential sums: Kloosterman sums allow bounding exponential sums in arithmetic problems, including sums over primes and prime intervals.
3. Fourier expansions of modular forms: Kloosterman sums appear as finite ring analogues of Bessel functions in modular form theory.
4. Spectral theory and automorphic forms: They have applications in the spectral theory of automorphic functions and related arithmetic subjects.
5. Prime number distribution: Used to study primes in short intervals, primes in arithmetic progressions, and connections to the Riemann zeta function.
6. Estimates via advanced methods: Weil's and Deligne's bounds on Kloosterman sums produce strong error terms in analytic number theory.
7. Applications in additive number theory: They help in problems involving sums and products modulo primes and bounding multilinear sums.
8. Recent research applications: Improved bounds on bilinear forms with Kloosterman sums have further applications in exponential sum estimates and number theory.

1. GAUSS SUMS

Definition 1.0.1 (Gauss Sum). Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial additive (unitary) character (Definition A.0.2), and let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a multiplicative (unitary) character (Definition A.0.2). The *Gauss sum associated to χ and ψ* is defined as

$$G(\chi, \psi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x),$$

where the sum is over the nonzero elements of $\mathbb{F}_q$.

A common choice is $\psi(x) = \exp\left(2\pi i \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)/p\right)$, with $p = \operatorname{Char} \mathbb{F}_q$.

2. KLOOSTERMAN SUMS

2.1. **Definitions.**

Definition 2.1.1 (Kloosterman Sum). Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial additive (unitary) character (Definition A.0.2), and let $a, b \in \mathbb{F}_q^\times$.

The *Kloosterman sum associated to a, b and ψ* is defined by

$$\operatorname{Kl}(a, b; \psi) := \sum_{x \in \mathbb{F}_q^\times} \psi(ax + bx^{-1}),$$

where the summation is over the nonzero elements of $\mathbb{F}_q$.

In particular, when

$$\psi(y) = \exp\left(2\pi i \, \frac{\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y)}{p}\right)$$

2

with $p = \text{char}(\mathbb{F}_q)$, one may write $\text{Kl}(a, b)$ for $K(a, b; \psi)$. In other words,

$$\text{Kl}(a, b) = \sum_{x \in \mathbb{F}_q^\times} \exp\left(2\pi i \, \frac{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax + bx^{-1})}{p}\right).$$

The *clsasical Kloosterman sum*, often denoted by $S(a, b; p)$, is by definition the Kloosterman sum that we denoted by $\text{Kl}(a, b)$ above in the case that $q = p$. In other words,

$$S(a, b; p) = \sum_{x \in \mathbb{F}_p^\times} \exp\left(\frac{2\pi i(ax + bx^{-1})}{p}\right).$$

Proposition 2.1.2 (Weil). (♠ TODO: Can this be extended to more general characters?)
Let p be a prime number. For all $a, b \in \mathbb{F}_p$,

$$|S(a, b; p)| \leq 2\sqrt{p}.$$

(Definition 2.1.1)

Definition 2.1.3 (cf. [Kat98, Introduction]). Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial (unitary) additive character (Definition A.0.2), and let $a \in \mathbb{F}_q^\times$.

We will often let $\text{Kl}(a, n; \psi)$ denote either *the non-normalized or the normalized hyper-Kloosterman sum in n-variables* (also called a *generalized Kloosterman sum*); the non-normalized hyper-Kloosterman sum is defined by

$$\text{Kl}(a, n; \psi) = \sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q \\ x_1 \cdots x_n = a}} \psi(x_1 + \cdots + x_n).$$

whereas the normalized hyper-Kloosterman sum is $q^{\frac{1-n}{2}}$ times the non-normalized sum, i.e.

$$\text{Kl}(a, n; \psi) = q^{\frac{1-n}{2}} \sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q \\ x_1 \cdots x_n = a}} \psi(x_1 + \cdots + x_n).$$

The normalized hyper-Kloosterman sums $\text{Kl}(a, n; \psi)$ satisfy $|\text{Kl}(a, n; \psi)| \leq n$ for all $a \in \mathbb{F}_q^\times$ (Proposition 2.1.4).

When

$$\psi(y) = \exp\left(2\pi i \, \frac{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y)}{p}\right)$$

with $p = \text{char}(\mathbb{F}_q)$, one may write $\text{Kl}(a, n)$ for $K(a, n; \psi)$. In other words,

$$\text{Kl}(a, n) = \sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q \\ x_1 \cdots x_n = a}} \exp\left(2\pi i \, \frac{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_1 + \cdots + x_n)}{p}\right) \quad \text{or}$$

$$\text{Kl}(a, n) = q^{\frac{1-n}{2}} \sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q \\ x_1 \cdots x_n = a}} \exp\left(2\pi i \, \frac{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_1 + \cdots + x_n)}{p}\right)$$

depending on whether we are discussing the non-normalized or normalized sum.

Proposition 2.1.4 ([DBG$^+$77, Sommes trig., Section 7]). *Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial additive character (Definition A.0.2), and let $a \in \mathbb{F}_q^\times$. We have*

$$|\mathrm{Kl}(a, n; \psi)| \leq nq^{\frac{n-1}{2}}$$

where $\mathrm{Kl}(a, n; \psi)$ is the non-normalized hyper-Kloosterman sum in n-variables (Definition 2.1.3).

Remark 2.1.5. In general, there are many different notations used even for equivalent notions of Kloosterman sums. For instance [Kat98] lets $\mathrm{Kl}(p, n, a)$ denote the non-normalized hyper-Kloosterman sum that we denote as $\mathrm{Kl}(a, n)$ in Definition 2.1.3 in the case that $\mathbb{F}_q = \mathbb{F}_p$.

2.2. **Bounding sums of Kloosterman sums.** (♠ TODO: Why are bound son sums of Kloosterman sums important at all?)

The following bound sums of Kloosterman sums in a "small prime interval":

Theorem 2.2.1 ([BFK$^+$17, Theorem 1.8]). *Let p be a prime number. For every X such that $2 \leq x \leq p$ and every $\epsilon > 0$, we have*

$$\sum_{\substack{p' \leq X \\ p' \text{ prime}}} \mathrm{Kl}(p', 2) \ll_\varepsilon p^{\frac{1}{6}+\varepsilon} \cdot X^{\frac{7}{9}}.$$

where $\mathrm{Kl}(p', 2)$ here is the normalized Kloosterman sum (Definition 2.1.3).

Theorem 2.2.2 ([DZ19, Theorem 1.2]). *Let p be a prime number. Let u, v be positive integers such that $(u, v) = 1$ and $1 \leq v \leq p^{\frac{1}{100}}$. For all $1 \leq X \leq p$ and $\varepsilon > 0$,*

$$\sum_{\substack{p' \leq X \\ p' \text{ prime} \\ p' \equiv u \pmod{v}}} \mathrm{Kl}(p', 2) \ll_\varepsilon p^{\frac{11}{192}+\varepsilon} \cdot X^{\frac{15}{16}}.$$

where $\mathrm{Kl}(p', 2)$ here is the normalized Kloosterman sum (Definition 2.1.3).

Remark 2.2.3. Note that Theorem 2.2.1 is stated in terms of the non-normalized Kloosterman sum, whereas [DZ19, Theorem 1.2] is in terms of the normalized Kloosterman sum.

2.3. **Bounds on bilinear forms with Kloosterman sums as coefficients.** Koawlski, Michel, and Sawin [KMS17] proved the bounds Theorem 2.3.4 and Theorem 2.3.5 for bilinear forms constructed with Kloosterman sums. They demonstrated applications to 1. asymptotic approximations for moments of twisted cuspidal L-functions and 2. the distribution in arithmetic progressions to large moduli of certain arithmetic functions.

Notation 2.3.1. (♠ TODO: Define arithmetic functions) Given an arithmetic function K and complex coefficients $\boldsymbol{\alpha} = (\alpha_m)_{m \geq 1}$ and $\boldsymbol{\beta} = (\beta_m)_{m \geq 1}$, let $B(K, \boldsymbol{\alpha}, \boldsymbol{\beta})$ be the sum

$$B(K, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_m \sum_n \alpha_m \beta_n K(mn).$$

Notation 2.3.2. (♠ TODO: define the ℓ^p norm for general sequences) Given a sequence $\boldsymbol{\alpha}$ of complex numbers with finite support, denote by

$$\|\alpha\|_p = \left(\sum_m |\alpha_m|^p\right)^{\frac{1}{p}}$$

the ℓ^p-norm.

Notation 2.3.3. Given $c \in \mathbb{F}_q^\times$, write

$$[\times c]^* \mathrm{Kl} = [\times c]^* \mathrm{Kl}(-, n)$$

for the function

$$a \mapsto \mathrm{Kl}(ca, n)$$

where $\mathrm{Kl}(a, n)$ is the normalized hyper-Kloosterman sum in n variables (Definition 2.1.3)

Koawlski, Michel, and Sawin proved the following bound for general bilinear forms:

Theorem 2.3.4 ([KMS17, Theorem 1.1]). Let p be a prime number. Let c be an integer coprime to p. Let M and N be real numbers such that

$$1 \le M \le Np^{\frac{1}{4}}, \quad p^{\frac{1}{4}} < MN < p^{\frac{5}{4}}.$$

Let $\mathcal{N} \subset [1, p-1]$ be an interval of length $\lfloor N \rfloor$ and let $\boldsymbol{\alpha} = (\alpha_m)_{1 \le m \le M}$ and $\boldsymbol{\beta} = (\beta_n)_{n \in \mathcal{N}}$ be sequences of complex numbers.

For any $\varepsilon > 0$, we have

$$B([\times c]^* \mathrm{Kl}(-, n), \boldsymbol{\alpha}, \boldsymbol{\beta}) \ll p^\varepsilon \cdot \|\boldsymbol{\alpha}\|_2 \cdot \|\boldsymbol{\beta}\|_2 \cdot (MN)^{\frac{1}{2}} \cdot \left(M^{-\frac{1}{2}} + (MN)^{-\frac{3}{16}} \cdot p^{\frac{11}{64}}\right)$$

(Notation 2.3.1) (Notation 2.3.2) (Notation 2.3.3) where the implied constant depends only on n and ε.

Koawlski, Michel, and Sawin also proved the following bound for special bilinear forms:

Theorem 2.3.5 ([KMS17, Theorem 1.3]). Let p be a prime number. Let c be an integer coprime to p. Let M and N be real numbers such that

$$1 \le M \le N^2, \quad N < p, \quad MN < p^{\frac{3}{2}}.$$

Let $\mathcal{N} \subset [1, p-1]$ be an interval of length $\lfloor N \rfloor$ and let $\boldsymbol{\alpha} = (\alpha_m)_{1 \le m \le M}$ be a sequence of complex numbers such that $|\alpha_m| \le 1$..

For any $\varepsilon > 0$, we have

$$B([\times c]^* \mathrm{Kl}(-, n), \boldsymbol{\alpha}, 1_{\mathcal{N}}) \ll p^\varepsilon \cdot \|\boldsymbol{\alpha}\|_2 \cdot \|\boldsymbol{\alpha}\|_2 \cdot M^{\frac{1}{4}} N \cdot \left(\frac{M^2 N^5}{p^3}\right)^{-\frac{1}{12}}.$$

(Notation 2.3.1) (Notation 2.3.2) (Notation 2.3.3) where the implied constant depends only on n and ε.

Appendix A. Miscellaneous definitions

Definition A.0.1. Let G be a locally compact Hausdorff group.

1. A *quasicharacter of G* is a continuous group homomorphism $\chi : G \to \mathbb{C}^\times$.
2. A quasicharacter χ is *unitary* if its image lies in the unit circle $S^1 \subset \mathbb{C}^\times$, i.e. $|\chi(g)| = 1$ for all $g \in G$. Such a quasicharacter is also simply called a *character*.
3. A (quasi)character is *finite* if its image is finite, i.e. its kernel has finite index in its domain.

When G is finite, G is usually equipped with the discrete topology — a character (and even a quasicharacter) is thus simply a group homomorphism $G \to \mathbb{C}^\times$ such that $|\chi(g)| = 1$ for all $g \in G$.

Compare against Definition A.0.2

Definition A.0.2. Let $(R, +, \cdot)$ be a ring. Let F be a ring/field "of values"; usually, F is taken to be $\mathbb{C}$ or $\overline{\mathbb{Q}}_\ell$ for some prime ℓ.

1. An *additive character* often refers to a group homomorphism $(R, +) \to F^\times$. (♠ TODO: Define monoid)
2. A *multiplicative character* often refers to a monoid homomorphism $(R^\times, \cdot) \to F^\times$.

If F and R are equipped with topologies, then *(additive or multiplicative) characters* may more specifically refer to homomorphisms that are continuous with respect to the given topologies.

If F is a field with an absolute value, then what are called (additive or multiplicative) characters above may just be called *(additive or multiplicative) quasi-characters* instead and a *(additive or multiplicative) character*, synonymously also called a *unitary (additive or multiplicative) (quasi-)character*, may in fact refer to a homomorphism whose image lies in the subset of $F^\times$ of elements of absolute value 1.

Compare against Definition A.0.1

References

[BFK⁺17] Valentin Blomer, Étienne Fouvry, Emmanuel Kowalski, Philippe Michel, and Djordje Milićević. Some applications of smooth bilinear forms with kloosterman sums. *Proceedings of the Steklov Institute of Mathematics*, 296:18–29, 2017.

[DBG⁺77] Pierre Deligne, Jean-François Boutot, Alexander Grothendieck, Luc Illusie, and Jean-Louis Verdier. *Étale Cohomology. Séminaire de Géométrie Algébrique due Bois-Marie 1963-1964 (SGA 4 1/2)*. Lecture Notes in Mathematics. Springer-Verlag, 1977.

[DZ19] Alexander Dunn and Alexandru Zaharescu. Sums of Kloosterman sums over primes in an arithmetic progression. *The Quaterly Journal of Mathematics*, 70(1):319–342, 2019.

[Kat98] Nicholas M. Katz. *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, 1998.

[KMS17] Emmanuel Kowalski, Philippe Michel, and Will Sawin. Bilinear forms with Kloosterman sums and applciations. *Annals of Mathematics*, 186:413–500, 2017.