

## UNIFORM DISTRIBUTION OF THE WEIGHTS OF THE KLOOSTERMAN CODES

Toyokazu HIRAMATSU

(Received October 3, 1994)

**Abstract.** Let  $C$  be the Kloosterman code over finite fields. In this paper, we give some bound for the weights of codewords in  $C$  and show that the weights of the code  $C$  are uniformly distributed with respect to the Sato-Tate measure by using the result of Katz.

*AMS 1991 Mathematics Subject Classification.* 10F40, 12C25, 94B05.

*Key words and phrases.* Kloosterman sums, code, uniform distribution.

### §1. Kloosterman sums over finite fields and Kloosterman codes

Let  $p$  be a prime, and let  $q = p^k$  for some positive integer  $k$ . We put  $G = GF(q)$ ,  $G_0 = GF(p)$  and  $G^\times = G - \{0\}$ . The Kloosterman sums  $K(a)$  over  $G$  are defined by

$$K(a) = \sum_{x \in G^\times} e\left(\operatorname{tr}\left(ax + \frac{1}{x}\right)\right), \quad a \in G,$$

where  $e(z) = e^{2\pi iz/p}$ , and  $\operatorname{tr}$  denotes the trace of  $G$  over  $G_0$ . The Kloosterman code  $C(q)$  ( $= C$ ) is of length  $n = q - 1$  and dimension  $2k$ , and is the image of the map

$$\varphi : G^2 \rightarrow G^n$$

given by

$$\varphi(\alpha, \beta) = \left\{ \operatorname{tr}\left(\alpha x + \frac{\beta}{x}\right) \right\}_{x \in G^\times}.$$

The code  $C$  is the dual of the Melas code. If  $y = (y_1, \dots, y_n) \in G^n$ , the weight of  $y$  is the number

$$w(y) = \#\{i | y_i \neq 0\}.$$

In the following, we give some bound for the weights of the nonzero words of  $C$ .

**Theorem 1.** For all  $\alpha$  and  $\beta$  in  $G^\times$ , we have

$$\left| w(\varphi(\alpha, \beta)) - \frac{(p-1)(p^k-1)}{p} \right| \leq \frac{p-1}{p} \cdot 2p^{\frac{k}{2}}.$$

*Proof.* It is easy to check that  $w(\varphi(\alpha, \beta)) = w(\varphi(\alpha\beta, 1))$ , and we put  $\alpha\beta = a$ . Then, by Theorem 2 in Remijn and Tiersa ([5]) with the symbol  $x^n (= \eta^i)$  in Theorem 2 being replaced by  $a$ , we have firstly

$$w(\varphi(a, 1)) = \frac{(p-1)(p^k-1)}{p} - \frac{1}{p} \sum_{b \in G_0^\times} K(b^2 a). \quad (1)$$

Applying the Weil-Carlitz-Uchiyama inequality ([5], p.1350) on this, the proof is complete.  $\square$

## §2. Uniform distribution of the weights of $C(q)$

Let  $A(\omega)$  be the number of codewords of weight  $\omega$  in  $C (= C(q))$ . Then the sequence  $\{A(0), A(1), \dots, A(n)\}$  is called the weight distribution of  $C$ . In the following we study some relation between the weight distribution of the code  $C$  and uniform distribution for sequences in the sense of Sato-Tate.

Let  $H$  be a compact group and let  $X$  be the space of conjugacy classes of  $H$ , i.e.,  $X = H / \sim$ , where  $x \sim y$  if and only if there exists  $h \in H$  such that  $x = h^{-1}yh$ . Let  $\mu$  be a Haar measure on  $H$  and use the same notation to define its image in  $X$ . Then the sequence  $\{x_n\} \subset X$  is uniformly distributed if and only if for every irreducible character  $\chi$  of  $H$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \chi(x_i) = \int \chi(h) d\mu(h).$$

We denote by  $f$  a test function. Then

$$\sum_{x \in C} f(w(x)) = \sum_{\omega=0}^n A(\omega) f(\omega).$$

We put

$$Z(x) = \frac{pw(x) - (p-1)(p^k-1)}{2(p-1)p^{k/2}} \quad (x \in C).$$

Then  $Z(x) \in [-1, 1]$  by Theorem 1. The following theorem says that the numbers  $Z(x)$  are uniformly distributed with respect to the density function of total mass 1:

$$\rho(Z) = \frac{2}{\pi} \sqrt{1-Z^2}$$

on  $[-1, 1]$ , when  $q \rightarrow \infty$ .

**Theorem 2.** *If  $f$  is a test function, then*

$$\frac{1}{q^2} \sum_{x \in C} f(Z(x)) = \int_{-1}^1 f(Z) \rho(Z) dZ + O\left(\frac{1}{\sqrt{q}}\right)$$

as  $q \rightarrow \infty$ .

*Proof.* From the equality (1) we have

$$\begin{aligned} \sum_{x \in C} f(w(x)) &= \sum_{(\alpha, \beta) \in G^2} f(w(\varphi(\alpha, \beta))) \\ &= f(0) + 2(q-1)f((p-1)p^{k-1}) \\ &\quad + (q-1) \sum_{a \in G^\times} f\left(\frac{(p-1)(p^k-1)}{p} - \frac{1}{p} \sum_{b \in G_0^\times} K(b^2 a)\right). \end{aligned}$$

On the other hand, by the Weil-Carlitz-Uchiyama inequality we can put

$$K(b^2 a) = 2\sqrt{q} \cos \theta(b^2 a), \quad 0 \leq \theta(b^2 a) \leq \pi.$$

Therefore

$$\sum_{x \in C} f(Z(x)) = f\left(-\frac{p^k-1}{2p^{k/2}}\right) + 2(q-1)f\left(\frac{1}{2\sqrt{q}}\right) + (q-1) \sum_{a \in G^\times} f(\cos \theta(b^2 a)).$$

From the result of Katz ([1], p.241), we know that the sequence  $\{\theta(b^2 a)\}$  is uniformly distributed in  $[0, \pi]$  with respect to the ‘Sato-Tate measure’  $\sin^2 \theta d\theta$ : this means that

$$\frac{1}{q-1} \sum_{a \in G^\times} f(\cos \theta(b^2 a)) = \int_{-1}^1 f(Z) \rho(Z) dZ + O\left(\frac{1}{\sqrt{q}}\right)$$

as  $q \rightarrow \infty$ . Hence we have

$$\begin{aligned} \sum_{x \in C} f(Z(x)) &= (q-1)^2 \int_{-1}^1 f(Z) \rho(Z) dZ + f\left(-\frac{p^k-1}{2p^{k/2}}\right) \\ &\quad + 2(q-1)f\left(\frac{1}{2\sqrt{q}}\right) + O(q\sqrt{q}) \end{aligned}$$

as  $q \rightarrow \infty$ ; and the theorem is thereby proved.  $\square$

**Remark.** The case of  $p = 2$  has been proved by Lachaud ([2]) using the results of Lachaud and Wolfmann ([3] and [4]).

### Acknowledgment

It is a pleasure to express my sincere gratitude to the referee for his many valuable critical comments.

### References

- [1] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Ann. of Math. Studies **116**, Princeton Univ. Press, Princeton, 1988.
- [2] G. Lachaud, *Distribution of the weights of the dual of the Melas codes*, Discrete Math. **79** (1989/90), 103-106.
- [3] G. Lachaud and J. Wolfmann, *Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2*, C. R. Acad. Sci. Paris (I) **305** (1987), 881-883.
- [4] G. Lachaud and J. Wolfmann, *The weight of the orthogonals of the extended quadratic binary Goppa codes*, IEEE, Trans. Inform. Theory **36** (1990), 686-692.
- [5] J. C. C. M. Remijn and H. J. Tiersma, *A duality theorem for the weight distribution of some cyclic codes*, IEEE, Trans. Inform. Theory **34** (1988), 1348-1351.

Toyokazu Hiramatsu  
Division of Mathematical Science, College of Engineering, Hosei University  
Koganei, Tokyo 184, Japan  
*E-mail*: hiramatu@hrmt.sc.hosei.ac.jp