COMMUNICATION

DISTRIBUTION OF THE WEIGHTS OF THE DUAL OF THE MELAS CODE

Gilles LACHAUD

Équipe C.N.R.S. "Arithmétique et Théorie de l'Information", C.I.R.M.,
Luminy case 916, 13288 Marseille Cedex 9, France

Communicated by P. Camion

Received 31 May 1989

Let \( m \geq 1 \), and \( q = 2^m \); note \( F_q \) the field with \( q \) elements. The Kloosterman code \( C_{Kl}(q) \) is of length \( n = q - 1 \) and dimension \( 2m \), and is the image of the map
\[
c : F_q^2 \rightarrow F_q^n
\]
given by
\[
c(a, b) = \left\{ \text{Trace}_{F_q/K_l}(ax + b/x) \right\}_{x \in F_q^*}.
\]
The code \( C_{Kl}(q) \) is the dual of the Melas code (cf. [6], [7] and also [8]). Denote by \( w(x) \) the weight of a word \( x \in C_{Kl}(q) \); then
\[
w(c(0, 0)) = 0, \quad w(c(a, 0)) = \frac{q}{2} \quad \text{for } a \in F_q^*, \quad w(c(0, b)) = \frac{q}{2} \quad \text{for } b \in F_q^*.
\]
Let \( W_{Kl}(a) \) be the Kloosterman sum defined by
\[
W_{Kl}(a) = \sum_{x \in F_q^*} (-1)^{\text{tr}(x^{-1} + ax)} (a \in F_q^*).
\]
The following is proven in [6], [7];

**Proposition.** If \( a \in F_q^* \), then
\[
w(c(a, 1)) = \frac{q - 1 - W_{Kl}(a)}{2},
\]
where \( W_{Kl}(a) \) is the Kloosterman sum defined by
\[
W_{Kl}(a) = \sum_{x \in F_q^*} (-1)^{\text{tr}(x^{-1} + ax)} (a \in F_q^*).
\]
It is moreover proved in [6], [7] that the Kloosterman sum \( W_{Kl}(a) \) satisfy on one hand the congruence
\[
W_{Kl}(a) = -1 \pmod{4}
\]
and on the other hand the classical \textit{Weil inequality}

\[ |W_{K_0}(a)| \leq 2\sqrt{q} \]

(cf. [9], app. 5; we refer for instance to [5] or its resumé in [4] for a proof and for references on these topics); and that the image of the map \( a \mapsto W_{K_0}(a) \) from \( F_q^* \) to the ring \( \mathbb{Z} \) of integers is equal to the set

\[ \{ W \in \mathbb{Z} \mid W = -1 \pmod{4} \text{ and } |W| \leq 2\sqrt{q} \}. \]

Hence the weights of \( C_{K_1}(q) \) are all the numbers

\[ w = \frac{q - 1 - t}{2} \quad \text{with } t = -1 \pmod{4} \]

which lie within the interval \([w_-, w_+]\) where

\[ w_\pm = \frac{q - 1 \pm 2\sqrt{q}}{2}. \]

Now denote by \( A(w) \) the number of words of weight \( w \); if \( f \) is a test function (i.e. a continuous function with compact support on the real line), then

\[ \sum_{x \in C_{K_1}(q)} f(w(x)) = \sum_{i=0}^{n} A(w)f(w). \]

If \( x \in C_{K_1}(q) \), let

\[ z(x) = \frac{2w(x) - (q - 1)}{2\sqrt{q}}; \]

then \( z(x) \in [-1, +1] \). The following says that the numbers \( z(x) \) are equidistributed with respect to the density function of total mass 1:

\[ \varphi(z) = \frac{2}{\pi} \sqrt{1 - z^2} \]

in the interval \([-1, +1]\), when \( q \to \infty \).

\textbf{Theorem.} If \( f \) is a test function, then

\[ \frac{1}{q^2} \sum_{x \in C_{K_1}(q)} f(z(x)) = \int_{-1}^{+1} f(z)\varphi(z) \, dz + O\left(\frac{1}{\sqrt{q}}\right), \]

when \( q \to \infty \), where the hidden constant in the remainder depends only of \( f \).

\textbf{Proof.} We have

\[ \sum_{x \in C_{K_1}(q)} f(w(x)) = \sum_{(a, b) \in F_q \times F_q} f(w(c(a, b))); \]
from the preceding proposition we obtain

\[
\sum_{x \in C_{w}(q)} f(w(x)) = f(0) + 2(q - 1) f\left(\frac{q}{2}\right) + (q - 1) \sum_{a \in F_{q}} f\left(\frac{q - 1 + W_{K_{1}}(a)}{2}\right).
\]

Since \(|W_{K_{1}}(a)| \leq 2\sqrt{q}\), we can write

\[
W_{K_{1}}(a) = 2\sqrt{q} \cos \theta(a)
\]

with \(0 \leq \theta(a) \leq \pi\); then after a transformation of \(f\) we get

\[
\sum_{x \in C_{w}(q)} f(z(x)) = f\left(\frac{q - 1}{2\sqrt{q}}\right) + 2(q - 1) f\left(\frac{-1}{2\sqrt{q}}\right) + (q - 1) \sum_{a \in F_{q}} f(\cos \theta(a)). \quad (1)
\]

From the results of Deligne (cf. [2], 3.5.7) and Katz [3] (cf. [3], 3.6 and 13.5.3), we know that the numbers \(\theta(a)\) are equidistributed with respect to the Sato–Tate measure \(\sin^{2} \theta \, d\theta\); this means that for a fixed test function \(f\) we have

\[
\frac{1}{q - 1} \sum_{a \in F_{q}} f(\theta(a)) = \frac{2}{\pi} \int_{0}^{\pi} f(\theta) \sin^{2} \theta \, d\theta + O\left(\frac{1}{\sqrt{q}}\right)
\]

when \(q \to \infty\). If we perform the change of variables \(u = \arccos z\), the preceding relation becomes

\[
\frac{1}{q - 1} \sum_{a \in F_{q}} f(\cos \theta(a)) = \int_{-1}^{+1} f(z) \varphi(z) \, dz + O\left(\frac{1}{\sqrt{q}}\right), \quad (2)
\]

where \(\varphi\) is as defined above. By (1) and (2) we get

\[
\sum_{x \in C_{w}(q)} f(z(x)) = (q - 1)^{2} \int_{-1}^{+1} f(z) \varphi(z) \, dz + f\left(\frac{q - 1}{2\sqrt{q}}\right) + 2(q - 1)f\left(\frac{-1}{2\sqrt{q}}\right) + O(q\sqrt{q}),
\]

and the theorem is thereby proved. \(\square\)

Instead of the results of Deligne and Katz, we could deduce the preceding theorem from an adaptation of those of Yoshida [10]; see also Adolphson [1] for a more direct proof in the case considered here, but with a less precise remainder term.

**Remark.** If we perform the change of variables

\[
w = \frac{q - 1 - 2\sqrt{q}}{2},
\]

the preceding theorem says in some sense that in the interval \([w_{-}, w_{+}]\), the measure

\[
\sum_{x \in C_{w}(q)} f(w(x))
\]
"behaves like" the distribution function
\[ q_q(w) = \frac{1}{\pi q} \sqrt{wq - (q - 1 - 2w)^2} \]
when \( q \to \infty \); precisely, if \( f \) is a test function on \([-1, +1]\) and if we set
\[ g_q(w) = f \left( \frac{q - 1 - 2w}{\sqrt{q}} \right) \]
for \( w \in [w_-, w_+] \),
then
\[ \frac{1}{q^2} \sum_{x \in \mathcal{X}_q(q)} g_q(w(x)) = \int_{w_-}^{w_+} g_q(w) q_q(w) \, dw + O \left( \frac{1}{\sqrt{q}} \right) \]
when \( q \to \infty \), where the hidden constant in the remainder depends only of \( f \).

References