On Kloosterman Sums Divisible by 3

SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Kseniya Garaschuk, Petr Lisoněk

{kgarasch,plisonek}@sfu.ca

MITACS

One nice property of the trace function

Let $\mathbb{F}_{2^m}^* := \mathbb{F}_{2^m} \setminus \{0\}$ and let $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ denote the trace mapping given by:

$$\mathrm{Tr}(x) = \sum_{i=0}^{2^{m-1}} x^{2^i} = x + x^2 + \cdots + x^{2^{m-1}}.$$

Lemma 1 (KG-PL, 2007). *Let $m > 1$ and let k be such that $\gcd(2^k - 1, 2^m - 1) = 1$. Then for each $a \in \mathbb{F}_{2^m}$ we have $\mathrm{Tr}(a^{1/(2^k-1)}) = 0$ if and only if $a = t^{2^k} + t^{2^k-1}$ for some $t \in \mathbb{F}_{2^m}$.*

Kloosterman sums divisible by 3

Definition 1. *The* **Kloosterman map** *is the mapping $K : \mathbb{F}_{2^m} \to \mathbb{Z}$ defined by*

$$K(a) := \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)}.$$

Theorem 1 (KG-PL, 2007). *Let $m \geq 3$ be odd, and let $a \in \mathbb{F}_{2^m}^*$. Then $K(a)$ is divisible by 3 if and only if $a = t^4 + t^3$ for some $t \in \mathbb{F}_{2^m}$.*

Proof. Let $t \in \mathbb{F}_{2^m}$, $t \notin \{0,1\}$, and consider the elliptic curve

$$\mathcal{E}_t : \quad y^2 + xy = x^3 + a_2 x^2 + (t^8 + t^6),$$

where

$$a_2 = \begin{cases} 0 & \text{if } \mathrm{Tr}(t) = 0, \\ 1 & \text{if } \mathrm{Tr}(t) = 1. \end{cases}$$

"$\Leftarrow$" (Proved first by Helleseth and Zinoviev, 1999.)

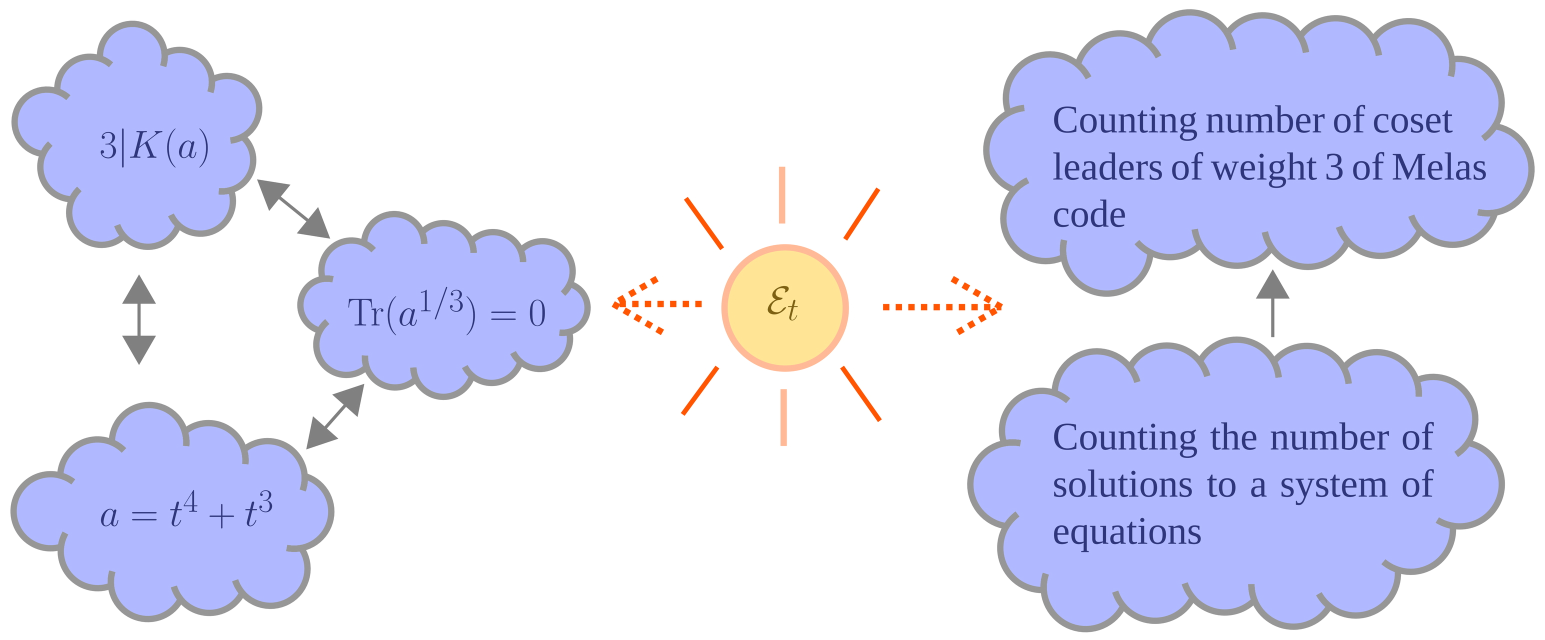
- Using (Lachaud and Wolfmann, 1990) we get

$$\#\mathcal{E}_t = \begin{cases} 2^m + 1 + K(t^4+t^3) & \text{if } \mathrm{Tr}(t) = 0, \\ 2^m + 1 - K(t^4+t^3) & \text{if } \mathrm{Tr}(t) = 1. \end{cases}$$

- The order of $(t^2 + t \,:\, t^4 + t^3 \,:\, 1)$ in $\mathcal{E}_t$ is 6, hence $6 | \#\mathcal{E}_t$.
- Since $3|(2^m+1)$, we get $3|K(t^4+t^3)$.

"$\Rightarrow$" ... in fact "$\Leftrightarrow$"

- Charpin, Helleseth and Zinoviev (2007) showed that $3|K(a) \Leftrightarrow \mathrm{Tr}(a^{1/3}) = 0$
- Set $k = 2$ in $\mathrm{Tr}(a^{1/(2^k-1)}) = 0 \Leftrightarrow a = t^{2^k} + t^{2^k-1}$. $\square$



Counting Coset Leaders for the Melas code

Definition 2. *H is called a parity check matrix for a linear code C if $x \in C \iff Hx^T = \mathbf{0}$. Hx^T is the syndrome of x.*

Note that $\mathbb{F}_{2^m} \simeq \mathbb{F}_2^m$, and let α a primitive element of $\mathbb{F}_{2^m}$, then the standard parity check matrix of the **Melas code** $\mathcal{M}_m$ is

$$\mathcal{H}_M = \begin{pmatrix} \alpha & \ldots & \alpha^i & \ldots & \alpha^{2^m-1} \\ \alpha^{-1} & \ldots & \alpha^{-i} & \ldots & \alpha^{-(2^m-1)} \end{pmatrix}.$$

Our goal: find the number of coset leaders for a coset of $\mathcal{M}_m$ of weight 3 corresponding to a given syndrome $(a,b)^T \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ produced by $\mathcal{H}_M$.

If $a \neq 0$, assume w.l.o.g. that $a = 1$ and we'll be led to counting the number of solutions to the following system of equations over $\mathbb{F}_{2^m}^*$:

$$\begin{cases} u + v + w = 1 \\ u^{-1} + v^{-1} + w^{-1} = r \end{cases} \qquad (*)$$

where $r \in \mathbb{F}_{2^m}$ is a fixed constant.

Theorem 2 (KG-PL, 2007). *Let $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$. The number of solutions over $\mathbb{F}_{2^m}^*$ of (*) is an integer T such that*

- *$T \in [2^m + 1 - 2^{m/2+1} - 6\,,\ 2^m + 1 + 2^{m/2+1} - 6]$*
- *6 divides T.*

Conversely, each T satisfying these two conditions occurs as the number of solutions for at least one $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$.

Idea for the proof. We eliminate w and homogenize as $u = U/Z$, $v = V/Z$. Next we apply the substitution

$$\begin{cases} r = 1 + \dfrac{1}{t}, \\ U = \dfrac{1}{t}x + (t+1)z, \\ V = \dfrac{1}{t^2}(y + sx) + (t^2+t)z, \\ Z = \dfrac{t+1}{t^2}x + (t+1)z. \end{cases}$$

Note: $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$ implies $t \in \mathbb{F}_{2^m} \setminus \{0,1\}$.

We obtain the same curve $\mathcal{E}_t$ as before!

Counting the points. A lot of technical calculations show that exactly 6 points on $\mathcal{E}_t$ do not produce a solution (u,v,w), thus the number of solutions to (*) is $\#\mathcal{E}_t - 6$.

The assumption $r \neq 1$ forces u, v, w to be distinct in any solution (u,v,w) to (*). Thus the number of solutions is divisible by $3! = 6$ for each $r \notin \{0,1\}$ and then so is $\#\mathcal{E}_t$.

By the Hasse Theorem for each $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$ the number of solutions to (*) is in

$$[2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6] \cap 6\mathbb{Z}.$$

The proof in the other direction relies heavily on Lachaud and Wolfmann resuls. $\square$

Theorem 3 (KG-PL, 2007). *Let $N(k)$ denote the number of those $r \in \mathbb{F}_{2^m} \setminus \{0,1\}$ for which the number of solutions to (*) is equal to k. Then for each $l \in \mathbb{N}$ we have $N(2^m - 5 + l) = N(2^m - 5 - l)$, that is, the values $N(k)$ are symmetric about $k = 2^m - 5$.*

Special cases. Cases $a = 0$ or $r \in \{0,1\}$ are easily doable but not interesting.

Applications in statistical experimental designs

Caps with many free pairs of points

- A cap in $\mathrm{PG}(n,2)$ is a set C of points such that no three of them are collinear.
- Points of C are columns of the parity check matrix H_C for a code of minimum distance 4.
- We say that $\{s,t\} \subset C$ is a free pair of points if $\{s,t\}$ is not contained in any coplanar quadruple of C.

Caps in statistics. In experimental design terminology caps and free pair of points are called fractional factorial designs and clear two-factor interactions, respectively. Given a coplanar quadruple of points in a cap, say $\{a,b,c,d\}$, in the analysis of an experiment it is impossible to distinguish between the two-factor interaction of $\{a,b\}$ and the two-factor interaction of $\{c,d\}$ and hence impossible to say which combination is effecting the outcome.

The goal: to maximize the number of free pairs of points in the cap given the size (number of points) of the cap and its projective dimension.

Observation. All pairs of points of C are free if and only if H_C defines a code of minimum distance 5 (or more).

Almost perfect nonlinear and almost bent functions

Theorem 4 (Carlet, Charpin and Zinoviev, 1998). *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $f(0) = 0$. Let C_f be the binary code defined be the parity check matrix*

$$\mathcal{H}_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-1} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^m-1}) \end{pmatrix}.$$

Then f is almost perfect nonlinear (APN) if and only if $d = 5$.

Theorem 5 (van Dam and Fon-Der-Flaass, 2003). *A function $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is almost bent (AB) if and only if the system*

$$\begin{cases} u + v + w = a \\ f(u) + f(v) + f(w) = b \end{cases}$$

has $q-2$ or $3q-2$ solutions (u,v,w) for every (a,b), where $q = 2^m$. If so, then the system has $3q-2$ solutions if $b = f(a)$ and $q-2$ solutions otherwise.

Construction based on linear codes of distance 5

- Start with the parity check matrix H^* of a binary linear code of distance 5 defined by an APN function and carefully add columns to it.
- If z is a newly added column and if a, b, c are three columns of H^* such that $a + b + c = z$, then the free pairs $\{a,b\}$, $\{a,c\}$ and $\{b,c\}$ are destroyed.
- Add to H^* syndromes z that correspond to cosets of weight 3 such that the number of coset leaders is minimized.
- In (Lisoněk, 2006) this was worked out for the Gold function $f(x) = x^3$ on $\mathbb{F}_{2^m}$ (BCH codes). When m is odd, Gold functions are AB and van Dam & Fon-Der-Flaass theorem applies: the number of solutions is always $2^m - 2$.
- On the other hand, $f(x) = x^{-1}$ is APN for m odd but not AB. Therefore the number of solutions can be as low as roughly $2^m - 2^{m/2+1}$, thus yielding a further improvement over the past result.