Questions about the divisibility of exponential sums, Fourier coefficients and weight of codes

YACC 2014

Régis Blache

LAMIA, ÉSPÉ de Guadeloupe

10 juin 2014

rblache@iufm.univ-ag.fr

The problem

In the following, we fix

- a prime p;
- a finite subset $D \subset \mathbb{N}_{>0}$

For any $m \geq 1$, we consider the set $E_{D,p}(m) \subset \{0, \ldots, p^m - 1\}^{|D|}$ consisting of the solutions of a modular equation

$$U = (u_d)_{d \in D} \; s.t. \left\{ \begin{array}{rcl} \sum_D du_d & \equiv & 0 \mod p^m - 1 \\ \sum_D du_d & > & 0 \\ 0 \leq & u_d & \leq p^m - 1 \end{array} \right.$$

The problem

In the following, we fix

- a prime p;
- a finite subset $D \subset \mathbb{N}_{>0}$

For any $m \geq 1$, we consider the set $E_{D,p}(m) \subset \{0, \ldots, p^m - 1\}^{|D|}$ consisting of the solutions of a modular equation

$$U = (u_d)_{d \in D} \; s.t. \left\{ \begin{array}{rcl} \sum_D du_d & \equiv & 0 \mod p^m - 1 \\ \sum_D du_d & > & 0 \\ 0 \leq & u_d & \leq p^m - 1 \end{array} \right.$$

For any integer, we define its *p-weight* as the sum of its p-ary digits

$$n = n_0 + \cdots + p^{m-1} n_{m-1} \to s_p(n) = \sum n_i$$

For $U \in E_{D,p}(m)$, let $s_p(U) = \sum_D s_p(u_d)$.

The problem

In the following, we fix

- a prime p;
- a finite subset $D \subset \mathbb{N}_{>0}$

For any $m \geq 1$, we consider the set $E_{D,p}(m) \subset \{0, \ldots, p^m - 1\}^{|D|}$ consisting of the solutions of a modular equation

$$U = (u_d)_{d \in D} \; s.t. \; \begin{cases} \sum_D du_d & \equiv & 0 \mod p^m - 1 \\ \sum_D du_d & > & 0 \\ 0 \leq & u_d & \leq p^m - 1 \end{cases}$$

For any integer, we define its *p-weight* as the sum of its p-ary digits

$$n = n_0 + \cdots + p^{m-1} n_{m-1} \to s_p(n) = \sum n_i$$

For $U \in E_{D,p}(m)$, let $s_p(U) = \sum_D s_p(u_d)$.

Problem

Find

$$\sigma_{D,p}(m) := \min\{s_p(U),\ U \in E_{D,p}(m)\}$$

Why ?

We now give three results in order to motivate our problem; we denote by $\mathbb{F}_{p^m}$ the finite field with p^m elements.

The first one is about exponential sums; let $f(x) = \sum_D a_d x^d \in \mathbb{F}_q[x]_D$ denote a polynomial *having its exponents in D*; we define the exponential sum

$$S_m(f) := \sum_{x \in \mathbb{F}_q} \psi(f(x)).$$

where ψ is a non trivial additive character of $\mathbb{F}_{p^m}$.

Why ?

We now give three results in order to motivate our problem; we denote by $\mathbb{F}_{p^m}$ the finite field with p^m elements.

The first one is about exponential sums; let $f(x) = \sum_D a_d x^d \in \mathbb{F}_q[x]_D$ denote a polynomial *having its exponents in D*; we define the exponential sum

$$S_m(f) := \sum_{x \in \mathbb{F}_q} \psi(f(x)).$$

where ψ is a non trivial additive character of $\mathbb{F}_{p^m}$.

If we fix a root π of $X^{p-1} + p = 0$, we have

Theorem (Moreno et al.)

Let $f(x) \in \mathbb{F}_q[x]_D$,

- *the exponential sum $S_m(f)$ is divisible by $\pi^{\sigma_{D,p}(m)}$*
- *there exists $f \in \mathbb{F}_q[x]_D$ such that $S_m(f)$ is not divisible by $\pi^{\sigma_{D,p}(m)+1}$.*

Codes, and boolean functions

We consider binary cyclic codes of length n. Such a code C can be seen as an ideal in the group algebra $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$, defined by its zero set $Z(C)$, which is closed under multiplication by 2 in $\mathbb{Z}/n\mathbb{Z}$.
If we set $D = Z(C)$ here, McEliece theorem on the divisibility of cyclic codes can be written

Theorem

Let C be the code described above, with $n = 2^m - 1$. Then the Hamming weight of any codeword is divisible by $2^{\sigma_{D,2}(m)-1}$, and there exists a word whose Hamming weight is not divisible by $2^{\sigma_{D,2}(m)}$.

Codes, and boolean functions

We consider binary cyclic codes of length n. Such a code C can be seen as an ideal in the group algebra $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$, defined by its zero set $Z(C)$, which is closed under multiplication by 2 in $\mathbb{Z}/n\mathbb{Z}$.
If we set $D = Z(C)$ here, McEliece theorem on the divisibility of cyclic codes can be written

Theorem

Let C be the code described above, with $n = 2^m - 1$. Then the Hamming weight of any codeword is divisible by $2^{\sigma_{D,2}(m)-1}$, and there exists a word whose Hamming weight is not divisible by $2^{\sigma_{D,2}(m)}$.

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a boolean function. Its *Walsh transform* $W_f : \mathbb{F}_{2^m} \to \mathbb{Z}$ is

$$W_f(a) := S_m(f + \ell_a) = \sum_{x \in \mathbb{F}_q} \psi(f(x) + ax).$$

Many properties of boolean functions depend on the divisibility of its Walsh spectrum. For instance, if $f(x) = x^d$ is a power function, the divisibility of its Walsh spectrum is exactly $\sigma_{D,2}(m)$ for $D = \{1, d\}$.

Study of the minimal weight: let the length vary

A first bound: if $s_p(D) = \max\{s_p(D),\ d \in D\}$, we have

$$\sigma_{D,p}(m) \geq \frac{m(p-1)}{s_p(D)}$$

Study of the minimal weight: let the length vary

A first bound: if $s_p(D) = \max\{s_p(D),\ d \in D\}$, we have

$$\sigma_{D,p}(m) \geq \frac{m(p-1)}{s_p(D)}$$

Given a solution $U = (u_d)_{d \in D} \in E_{D,p}(m)$, we define

- its *length* as $\ell(U) = m$;
- its *weight* as $s_p(U)$;
- its *absolute value* by $\sum_D du_d = (p^m - 1)|U| \in \{1, \cdots, \sum_D d\}$.

Study of the minimal weight: let the length vary

A first bound: if $s_p(D) = \max\{s_p(D),\ d \in D\}$, we have

$$\sigma_{D,p}(m) \geq \frac{m(p-1)}{s_p(D)}$$

Given a solution $U = (u_d)_{d \in D} \in E_{D,p}(m)$, we define

- its *length* as $\ell(U) = m$;
- its *weight* as $s_p(U)$;
- its *absolute value* by $\sum_D du_d = (p^m - 1)|U| \in \{1, \cdots, \sum_D d\}$.

Remark

Let $U \in E_{D,p}(m)$, $V \in E_{D,p}(n)$ be such that $|U| = |V|$. Then the |D|-uple

$$W = U \oplus V \text{ defined by } \left(w_d = p^n u_d + v_d\right)_{d \in D}$$

is an element in $E_{D,p}(m+n)$, satisfying

$$\ell(W) = \ell(U) + \ell(V),\ s_p(W) = s_p(U) + s_p(V) \textit{ and } |W| = |U| = |V|$$

Shifting the solutions

Denote by δ_m the map from $\{0, \ldots, p^m - 1\}$ to itself that sends

- any $i < p^m - 1$ to the remainder of pi modulo $p^m - 1$;
- $p^m - 1$ to itself.

Shifting the solutions

Denote by δ_m the map from $\{0, \ldots, p^m - 1\}$ to itself that sends

- any $i < p^m - 1$ to the remainder of pi modulo $p^m - 1$;
- $p^m - 1$ to itself.

Then δ_m *shifts the base p digits*. Actually we get

$$\delta_m(i) = pi - (p^m - 1)i_{m-1}$$

where i_{m-1} is the $m-1$-th digit of i.
In particular the map δ *preserves the p-weight*.

Shifting the solutions

Denote by δ_m the map from $\{0, \ldots, p^m - 1\}$ to itself that sends

- any $i < p^m - 1$ to the remainder of pi modulo $p^m - 1$;
- $p^m - 1$ to itself.

Then δ_m *shifts the base p digits*. Actually we get

$$\delta_m(i) = pi - (p^m - 1)i_{m-1}$$

where i_{m-1} is the $m-1$-th digit of i.
In particular the map δ *preserves the p-weight*.

For $U = (u_d)_{d \in D} \in E_{D,p}(m)$, we define $\delta_m U := (\delta_m(u_d))_{d \in D}$.

Lemma

We have:

- $\delta_m U \in E_{D,p}(m)$
- $\delta_m U$ *has the same weight than* U

Moreover we get

$$|\delta_m U| = p|U| - \sum_D d u_{d,m-1}$$

Irreducible solutions

In the same way, we get

Lemma

Let $U \in E_{D,p}(m)$. Choose an integer $1 \leq t \leq m-1$, and for any $d \in D$ let $u_d = p^t w_d + v_d$ be the euclidean division of u_d by p^t.
We have the equalities :

$$\sum_{d \in D} dv_d = p^t |\delta_m^{-t} U| - |U| \ ; \ \sum_{d \in D} dw_d = p^{m-t} |U| - |\delta_m^{-t} U|.$$

As a consequence, if $|\delta_m^{-t} U| = |U|$ for some $1 \leq t \leq m-1$, we get

$$U = V \oplus W$$

Thus we can construct all solutions from the ones such that $|U|, \ldots, |\delta_m^{m-1} U|$ are pairwise distinct (and then $m \leq \sum_D d$).

Irreducible solutions

In the same way, we get

Lemma

Let $U \in E_{D,p}(m)$. Choose an integer $1 \leq t \leq m-1$, and for any $d \in D$ let $u_d = p^t w_d + v_d$ be the euclidean division of u_d by p^t.
We have the equalities :

$$\sum_{d \in D} d v_d = p^t |\delta_m^{-t} U| - |U| \ ; \ \sum_{d \in D} d w_d = p^{m-t} |U| - |\delta_m^{-t} U|.$$

As a consequence, if $|\delta_m^{-t} U| = |U|$ for some $1 \leq t \leq m-1$, we get

$$U = V \oplus W$$

Thus we can construct all solutions from the ones such that $|U|, \ldots, |\delta_m^{m-1} U|$ are pairwise distinct (and then $m \leq \sum_D d$).

Definition

We call such a solution an irreducible *solution.*

A linear lower bound for the minimal weights

Definition

We define the density *of the set D with respect to p by*

$$\delta_{D,p} := \min\left\{\frac{\sigma_{D,p}(m)}{m(p-1)},\ 1 \leq m \leq \sum_{D} d\right\}$$

A linear lower bound for the minimal weights

Definition

We define the density *of the set D with respect to p by*

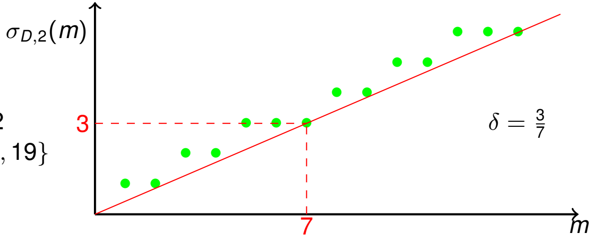
$$\delta_{D,p} := \min\left\{\frac{\sigma_{D,p}(m)}{m(p-1)},\ 1 \le m \le \sum_D d\right\}$$

Then we have

Proposition

For any $m \geq 1$, we have $\sigma_{D,p}(m) \geq m(p-1)\delta_{D,p}$.

$p = 2$
$D = \{1, 9, 19\}$



The case of complete sets

We fix some d_0, and consider $D := \{1 \leq i \leq d_0,\ (p, i) = 1\}$.

When $p = 2$, we have $\delta_2(D) = \frac{1}{n}$ for any $2^n - 1 \leq d_0 \leq 2^{n+1} - 3$.

The case of complete sets

We fix some d_0, and consider $D := \{1 \leq i \leq d_0,\ (p, i) = 1\}$.

When $p = 2$, we have $\delta_2(D) = \frac{1}{n}$ for any $2^n - 1 \leq d_0 \leq 2^{n+1} - 3$.

When p is odd, we have

- $\delta_p(D) = \frac{1}{p-1} \lceil \frac{p-1}{d} \rceil$ when $d_0 < p - 1$
- $\delta_p(D) = \frac{1}{n(p-1)}$ when $p^n - 1 \leq d_0 \leq p^{n+1} - p - 1$
- $\delta_p(D) = \frac{2}{(2n+1)(p-1)}$ when $p^{n+1} - p - 1 \leq d_0 \leq p^{n+1} - 2$

The case of complete sets

We fix some d_0, and consider $D := \{1 \leq i \leq d_0,\ (p, i) = 1\}$.

When $p = 2$, we have $\delta_2(D) = \frac{1}{n}$ for any $2^n - 1 \leq d_0 \leq 2^{n+1} - 3$.

When p is odd, we have

- $\delta_p(D) = \frac{1}{p-1}\lceil \frac{p-1}{d} \rceil$ when $d_0 < p - 1$
- $\delta_p(D) = \frac{1}{n(p-1)}$ when $p^n - 1 \leq d_0 \leq p^{n+1} - p - 1$
- $\delta_p(D) = \frac{2}{(2n+1)(p-1)}$ when $p^{n+1} - p - 1 \leq d_0 \leq p^{n+1} - 2$

Remark

One can look for almost complete sets D, in order to increase the density; for instance, for $p = 2$, $d_0 = 2^{n+1} - 3$, *if we remove the integers* $2^n - 1$ *and* $3 \cdot 2^{n-1} - 1$ *from D, we get*

$$\delta_2\left(D \setminus \{2^n - 1, 3 \cdot 2^{n-1} - 1\}\right) = \frac{2}{2n - 1}$$

Back to the minimal weights; how far are we ?

In the case of *complete sets of exponents*, the linear bound is optimal

$$\sigma_{D,p}(m) = \lceil m(p-1)\delta_{D,p}(m) \rceil .$$

Back to the minimal weights; how far are we ?

In the case of *complete sets of exponents*, the linear bound is optimal

$$\sigma_{D,p}(m) = \lceil m(p-1)\delta_{D,p}(m) \rceil .$$

In general we can be as far from the linear bound as possible

Example

Let $D = \{1, 2^n + 3\}$, $p = 2$ and assume $n \equiv 2 \mod 3$; then we have $\delta_{D,2} = \frac{1}{3}$, and

$$\sigma_{D,2}(2n+1) = n$$

We consider the difference

$$\epsilon_{D,p}(m) := \sigma_{D,p}(m) - m(p-1)\delta_{D,p}$$

Bounding the difference

Let us give some (very) partial results

Proposition

There exists infinitely many m such that $\epsilon_{D,p}(m) = 0$.

Assume that D generates $\mathbb{Z}$. There exists a constant $C(D,p)$ such that for all $m \geq 1$

$$\epsilon_{D,p}(m) \leq C(D,p)$$

Bounding the difference

Let us give some (very) partial results

Proposition

There exists infinitely many m such that $\epsilon_{D,p}(m) = 0$.

Assume that D generates $\mathbb{Z}$. *There exists a constant* $C(D, p)$ *such that for all* $m \geq 1$

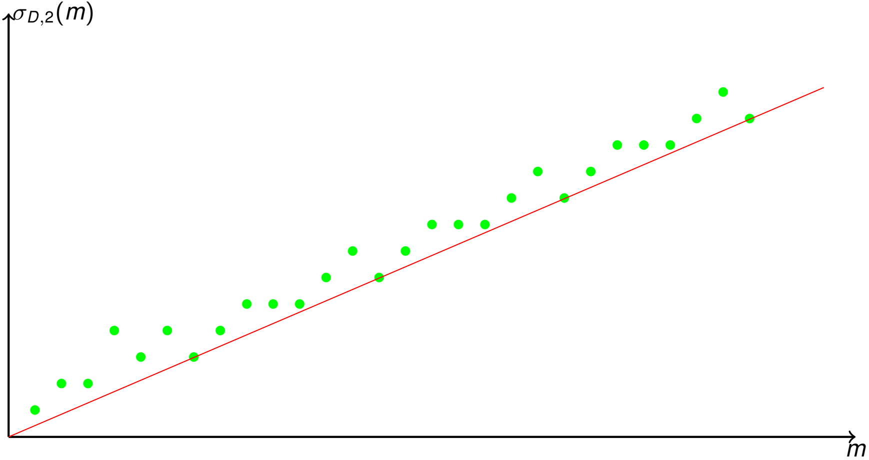
$$\epsilon_{D,p}(m) \leq C(D, p)$$

Under a stronger hypothesis, we can be more precise

Proposition

Assume moreover that all solutions of minimal density have the same length ℓ.
Then the function $\epsilon_{D,p}(m)$ *is* ℓ*-periodic for m large enough.*

$p = 2,\ D = \{1, 19\}$



$p = 2, \ D = \{1, 19\}$