

On the number of irreducible polynomials

with prescribed trace and norm

Marko Moisio

Department of Mathematics and Statistics

University of Vaasa, Finland

Overview

- The goal(s)
- Earlier results
- Notations
- The main problem
- A formula for $N_t(a, b)$
- Case $a = 0$
- Case $a \neq 0$
- On Kloosterman sums, I
- On irreducible cubic polynomials
- On Kloosterman sums, II

The goal(s)

Notations:

| | |
|----------------|---|
| m, p, r | fixed positive integers, p a prime |
| \mathbb{F}_q | the finite field with $q = p^r$ elements |
| a, b | fixed elements in \mathbb{F}_q , $b \neq 0$ |
| $P_m(a, b)$ | the number of irreducibles $x^m - ax^{m-1} + \dots + (-1)^m b \in \mathbb{F}_q[x]$ |

The goal(s)

Notations:

| | |
|----------------|---|
| m, p, r | fixed positive integers, p a prime |
| \mathbb{F}_q | the finite field with $q = p^r$ elements |
| a, b | fixed elements in \mathbb{F}_q , $b \neq 0$ |
| $P_m(a, b)$ | the number of irreducibles $x^m - ax^{m-1} + \dots + (-1)^m b \in \mathbb{F}_q[x]$ |

Goal: Find an explicit expression for $P_m(a, b)$

The goal(s)

Notations:

| | |
|----------------|---|
| m, p, r | fixed positive integers, p a prime |
| \mathbb{F}_q | the finite field with $q = p^r$ elements |
| a, b | fixed elements in \mathbb{F}_q , $b \neq 0$ |
| $P_m(a, b)$ | the number of irreducibles $x^m - ax^{m-1} + \dots + (-1)^m b \in \mathbb{F}_q[x]$ |

Goal: Find an explicit expression for $P_m(a, b)$

This is very difficult in general, and so we also set an "easier"

Goal: Find good bounds for $P_m(a, b)$.

Earlier results

- An explicit expression for the number of irreducibles with a XOR b fixed was obtained by Carlitz (1952) (and more elementary by Yucas (2006))

Earlier results

- An explicit expression for the number of irreducibles with a XOR b fixed was obtained by Carlitz (1952) (and more elementary by Yucas (2006))
- An asymptotic bound for $P_m(a, b)$ was found by Carlitz (1952):

$$P_m(a, b) = \frac{q^m - 1}{mq(q-1)} + \mathcal{O}(q^{m/2}) \quad (m \rightarrow \infty)$$

Earlier results

- An explicit expression for the number of irreducibles with a XOR b fixed was obtained by Carlitz (1952) (and more elementary by Yucas (2006))
- An asymptotic bound for $P_m(a, b)$ was found by Carlitz (1952):

$$P_m(a, b) = \frac{q^m - 1}{mq(q-1)} + \mathcal{O}(q^{m/2}) \quad (m \rightarrow \infty)$$

- Wan (1997) obtained the bound

$$\left| P_m(a, b) - \frac{q^m - 1}{m(q-1)} \right| \leq \frac{3}{m} q^{m/2} \quad (1)$$

Notations

To state the main problem we fix some notations:

| | |
|------------------------------|--|
| t | a positive factor of m |
| $\text{tr}_t(x)$ | the trace function from \mathbb{F}_{q^t} onto \mathbb{F}_q |
| $\text{Norm}_t(x)$ | the norm function from \mathbb{F}_{q^t} onto \mathbb{F}_q |
| $N_t(a, b)$ | the number of elements x in $\mathbb{F}_{q^t}^*$ with $\text{tr}_m(x) = a$ and $\text{Norm}_m(x) = b$ |
| μ | the Möbius function |
| $p_1^{e_1} \cdots p_k^{e_k}$ | the c.p.d of m |

The main problem (1/2)

It is easily seen that

$$P_m(a, b) = \frac{1}{m} \sum_{t|m} \mu(t) N_{m/t}(a, b) \quad (2)$$

The main problem (1/2)

It is easily seen that

$$P_m(a, b) = \frac{1}{m} \sum_{t|m} \mu(t) N_{m/t}(a, b) \quad (2)$$

which implies the following

Lemma 1. *Let $m' = p_1 \cdots p_k$. Then*

$$N_m(a, b) - \frac{M_1 m'}{2} \leq m P_m(a, b) \leq N_m(a, b) + \frac{M_2 m'}{2}$$

*with $M_1 = \max_h \{N_{\frac{m}{h}}(a, b)\}$, $M_2 = \max_s \{N_{\frac{m}{s}}(a, b)\}$
where h (resp. $s > 1$) runs over the factors of m'
having odd (resp. even) number of prime factors.*

The main problem (2/2)

Hence, to achieve our goals we have to solve

The main problem: Evaluate $N_{m/s}(a, b)$ for all positive factors s of m'

The main problem (2/2)

Hence, to achieve our goals we have to solve

The main problem: Evaluate $N_{m/s}(a, b)$ for all positive factors s of m' or, at least, find good upper bounds for them.

The main problem (2/2)

Hence, to achieve our goals we have to solve

The main problem: Evaluate $N_{m/s}(a, b)$ for all positive factors s of m' or, at least, find good upper bounds for them.

A good estimate for $N_m(a, b)$ was obtained by Katz (1993) (using deep AG):

$$\left| N_m(a, b) - \frac{q^m - 1}{q(q-1)} \right| \leq mq^{\frac{m-2}{2}}. \quad (3)$$

A formula for $N_t(a, b)$

Notations:

d is the gcd of $\frac{m}{t}$ and $q - 1$

γ_t a primitive element of \mathbb{F}_{q^t}

e, χ the canonical additive characters of \mathbb{F}_{q^t} and \mathbb{F}_q

A formula for $N_t(a, b)$

Notations:

d is the gcd of $\frac{m}{t}$ and $q - 1$

γ_t a primitive element of \mathbb{F}_{q^t}

e, χ the canonical additive characters of \mathbb{F}_{q^t} and \mathbb{F}_q

Lemma 2. Assume $p \nmid \frac{m}{t}$ and $d \mid \text{ind}_g b$. Assume $t > 1$ if $a = 0$. Let i_0 be a solution of $\frac{m}{dt}i \equiv \frac{\text{ind}_g b}{d} \left(\frac{q-1}{d}\right)$ and let $a_0 = \frac{t}{m}a$. Then

$$N_t(a, b) = \frac{d}{q(q-1)}(q^t - 1 + \sigma_t(a, b))$$

where

$$\sigma_t(a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(-ca_0) \sum_{x \in \mathbb{F}_{q^t}^*} e(c\gamma_t^{i_0} x^{\frac{q-1}{d}}).$$

Case $a = 0$ (1/3)

Lemma 2 implies

Theorem 1. *If $p \nmid \frac{m}{t}$, $d \mid \text{ind}_g b$, and $t > 1$, then*

$$N_t(0, b) = d \left(\frac{q^{t-1} - 1}{q - 1} + \frac{1}{q} \sum_{x \in \mathbb{F}_{q^t}} e(\gamma_t^{i_0} x^s) \right)$$

where $s = \text{gcd}(t, \frac{q-1}{d})$.

Case $a = 0$ (1/3)

Lemma 2 implies

Theorem 1. *If $p \nmid \frac{m}{t}$, $d \mid \text{ind}_g b$, and $t > 1$, then*

$$N_t(0, b) = d \left(\frac{q^{t-1} - 1}{q - 1} + \frac{1}{q} \sum_{x \in \mathbb{F}_{q^t}} e(\gamma_t^{i_0} x^s) \right)$$

where $s = \text{gcd}(t, \frac{q-1}{d})$.

Corollary 1.

$$\left| N_m(0, b) - \frac{q^{m-1} - 1}{q - 1} \right| \leq (s - 1) q^{\frac{m-2}{2}},$$

where $s = \text{gcd}(m, q - 1)$.

Case $a = 0$ (1/3)

Lemma 2 implies

Theorem 1. *If $p \nmid \frac{m}{t}$, $d \mid \text{ind}_g b$, and $t > 1$, then*

$$N_t(0, b) = d \left(\frac{q^{t-1} - 1}{q - 1} + \frac{1}{q} \sum_{x \in \mathbb{F}_{q^t}} e(\gamma_t^{i_0} x^s) \right)$$

where $s = \text{gcd}(t, \frac{q-1}{d})$.

Corollary 1.

$$\left| N_m(0, b) - \frac{q^{m-1} - 1}{q - 1} \right| \leq (s - 1) q^{\frac{m-2}{2}},$$

where $s = \text{gcd}(m, q - 1)$.

Remark. This is an improvement of the Katz-bound (3).

Case $a = 0$ (2/3)

Corollary 2.

$$\begin{aligned} \left| P_m(0, b) - \frac{q^{m-1} - 1}{m(q-1)} \right| &\leq \frac{s-1}{m} q^{\frac{m-2}{2}} + \frac{q^{\frac{m}{2}} - 1}{q-1} \\ &< \frac{2}{q-1} q^{\frac{m}{2}} \end{aligned}$$

Case $a = 0$ (2/3)

Corollary 2.

$$\begin{aligned} \left| P_m(0, b) - \frac{q^{m-1} - 1}{m(q-1)} \right| &\leq \frac{s-1}{m} q^{\frac{m-2}{2}} + \frac{q^{\frac{m}{2}} - 1}{q-1} \\ &< \frac{2}{q-1} q^{\frac{m}{2}} \end{aligned}$$

Remark. This is an improvement of the Wan-bound (1) if $m < \frac{3}{2}(q-1)$.

Case $a = 0$ (2/3)

Corollary 2.

$$\begin{aligned} \left| P_m(0, b) - \frac{q^{m-1} - 1}{m(q-1)} \right| &\leq \frac{s-1}{m} q^{\frac{m-2}{2}} + \frac{q^{\frac{m}{2}} - 1}{q-1} \\ &< \frac{2}{q-1} q^{\frac{m}{2}} \end{aligned}$$

Remark. This is an improvement of the Wan-bound (1) if $m < \frac{3}{2}(q-1)$. Of course, it can even be improved assuming the knowledge of the factorization of m .

Case $a \neq 0$ (1/5)

Lemma 2 implies also the following

Theorem 2. *If $a \neq 0$ and $d \mid \text{ind}_g b$, then*

$$N_t(a, b) = \frac{d(q^t - 1)}{q(q - 1)} + (-1)^{t-1} \left(\sum_{i=0}^{d-1} N(c_i) - \frac{d(q-1)^t}{q(q-1)} \right),$$

where $N(c_i)$ is the number of solutions of

$$\begin{cases} x_1 + \cdots + x_t & = 1 \\ x_1 \cdots x_t & = c_i \end{cases} \quad (4)$$

in \mathbb{F}_q^t with $c_i = g^{\frac{q-1}{d}i + i_0} a_0^{-t}$.

Case $a \neq 0$ (2/5)

Combine Theorem 2 with the Katz-bound (3) to get

Lemma 3. *Let $c \in \mathbb{F}_q^*$. The number $N(c)$ of solutions of*

$$\begin{cases} x_1 + \cdots + x_n & = 1 \\ x_1 \cdots x_n & = c \end{cases}$$

in \mathbb{F}_q^n satisfies

$$\left| N(c) - \frac{(q-1)^n}{q(q-1)} \right| \leq nq^{\frac{n-2}{2}}.$$

Case $a \neq 0$ (3/5)

Corollary 3.

$$\begin{aligned} \left| P_m(a, b) - \frac{q^m - 1}{mq(q-1)} \right| &\leq q^{\frac{m-2}{2}} + \frac{q^{\frac{m}{2}} - 1}{q(q-1)} + mq^{\frac{m}{4}-1} \\ &< \left(\frac{1}{q-1} + \frac{m}{q^{m/4+1}} \right) q^{\frac{m}{2}} \\ &\leq \frac{2}{q-1} q^{\frac{m}{2}}. \end{aligned}$$

Case $a \neq 0$ (3/5)

Corollary 3.

$$\begin{aligned} \left| P_m(a, b) - \frac{q^m - 1}{mq(q-1)} \right| &\leq q^{\frac{m-2}{2}} + \frac{q^{\frac{m}{2}} - 1}{q(q-1)} + mq^{\frac{m}{4}-1} \\ &< \left(\frac{1}{q-1} + \frac{m}{q^{m/4+1}} \right) q^{\frac{m}{2}} \\ &\leq \frac{2}{q-1} q^{\frac{m}{2}}. \end{aligned}$$

Remark. Again we have an improvement of the Wan-bound (1) if $m < \frac{3}{2}(q-1)$.

Case $a \neq 0$ (4/5)

If $m = 3$, Theorem 2 and equation (2) imply

Corollary 4. *Let $c = b/a^3$, and let \mathcal{X} be the projective curve over \mathbb{F}_q defined by*

$$\mathcal{X} : y^2 + cy + xy = x^3.$$

Then, $N_3(a, b) = |\mathcal{X}(\mathbb{F}_q)|$ and

$$P_3(a, b) = \frac{1}{3}(|\mathcal{X}(\mathbb{F}_q)| - \epsilon),$$

where

$$\epsilon = \begin{cases} 1 & \text{if } p \neq 3 \text{ and } c = \frac{1}{27}, \\ 0 & \text{otherwise.} \end{cases}$$

Case $a \neq 0$ (5/5)

It can be shown that \mathcal{X} is singular iff $\epsilon = 1$.

Example. Assume $p \neq 3$, and let $b = \left(\frac{a}{3}\right)^3$. Then

$$P_3(a, b) = \frac{1}{3}(q \pm 1)$$

where the sign is plus if $p \equiv 2 \pmod{3}$ and $2 \nmid r$, and otherwise the sign is minus.

Case $a \neq 0$ (5/5)

It can be shown that \mathcal{X} is singular iff $\epsilon = 1$.

Example. Assume $p \neq 3$, and let $b = \left(\frac{a}{3}\right)^3$. Then

$$P_3(a, b) = \frac{1}{3}(q \pm 1)$$

where the sign is plus if $p \equiv 2 \pmod{3}$ and $2 \nmid r$, and otherwise the sign is minus.

The Hasse-Weil bound now implies sharp bounds

Corollary 5. Let $a, b \in \mathbb{F}_q$, $b \neq 0$. Then

$$3 \left\lceil \frac{q+1-2\sqrt{q}}{3} \right\rceil \leq N_3(a, b) \leq 3 \left\lfloor \frac{q+1+2\sqrt{q}}{3} \right\rfloor.$$

On Kloosterman sums, I (1/5)

Assume $m = t = p^k$ and use additive characters to count the number of solutions of (4)

Theorem 3. *If $a \neq 0$, then*

$$N_m(a, b) = mP_m(a, b) = \frac{q^{m-1}-1}{q-1} + (-1)^{m-1}k_{m-2}(c),$$

where $c = b/a^m$, and

$$k_{m-2}(c) = \sum_{x_i \in \mathbb{F}_q^*} \chi\left(x_1 + \cdots + x_{m-2} + \frac{c}{x_1 \cdots x_{m-2}}\right).$$

On Kloosterman sums, I (1/5)

Assume $m = t = p^k$ and use additive characters to count the number of solutions of (4)

Theorem 3. *If $a \neq 0$, then*

$$N_m(a, b) = mP_m(a, b) = \frac{q^{m-1}-1}{q-1} + (-1)^{m-1}k_{m-2}(c),$$

where $c = b/a^m$, and

$$k_{m-2}(c) = \sum_{x_i \in \mathbb{F}_q^*} \chi\left(x_1 + \cdots + x_{m-2} + \frac{c}{x_1 \cdots x_{m-2}}\right).$$

Let $k(c) := k_1(c)$, choose $p = m = t = 3$, and combine Theorem 3 with Corollary 4 to get

On Kloosterman sums, I (2/5)

Corollary 6. *Let $q = 3^r$, and let $c \in \mathbb{F}_q^*$. Let \mathcal{X}_c be the elliptic curve over \mathbb{F}_q defined by*

$$\mathcal{X}_c : y^2 + cy + xy = x^3.$$

Then

$$|\mathcal{X}_c(\mathbb{F}_q)| = q + 1 + k(c),$$

and

$$k(c) \equiv -1 \pmod{3}.$$

On Kloosterman sums, I (2/5)

Corollary 6. *Let $q = 3^r$, and let $c \in \mathbb{F}_q^*$. Let \mathcal{X}_c be the elliptic curve over \mathbb{F}_q defined by*

$$\mathcal{X}_c : y^2 + cy + xy = x^3.$$

Then

$$|\mathcal{X}_c(\mathbb{F}_q)| = q + 1 + k(c),$$

and

$$k(c) \equiv -1 \pmod{3}.$$

The following four claims are now easy to verify:

Claim 1. \mathcal{X}_c is isomorphic over \mathbb{F}_q to

$$\mathcal{X}'_c : y^2 = x^3 + x^2 - c.$$

On Kloosterman sums, I (3/5)

Let \mathcal{E} be an ordinary elliptic curve over \mathbb{F}_q .

On Kloosterman sums, I (3/5)

Let \mathcal{E} be an ordinary elliptic curve over \mathbb{F}_q .

Claim 2. \mathcal{E} is isomorphic over \mathbb{F}_q to

$\mathcal{E}' : y^2 = x^3 + dx^2 + e$, for some $d, e \in \mathbb{F}_q^*$.

On Kloosterman sums, I (3/5)

Let \mathcal{E} be an ordinary elliptic curve over \mathbb{F}_q .

Claim 2. \mathcal{E} is isomorphic over \mathbb{F}_q to

$$\mathcal{E}' : y^2 = x^3 + dx^2 + e, \text{ for some } d, e \in \mathbb{F}_q^*.$$

Claim 3. $|\mathcal{E}'(\mathbb{F}_q)| = q + 1 + t$ with $t \equiv -1 \pmod{3}$ if and only if d is a square in \mathbb{F}_q^* .

On Kloosterman sums, I (3/5)

Let \mathcal{E} be an ordinary elliptic curve over \mathbb{F}_q .

Claim 2. \mathcal{E} is isomorphic over \mathbb{F}_q to

$$\mathcal{E}' : y^2 = x^3 + dx^2 + e, \text{ for some } d, e \in \mathbb{F}_q^*.$$

Claim 3. $|\mathcal{E}'(\mathbb{F}_q)| = q + 1 + t$ with $t \equiv -1 \pmod{3}$ if and only if d is a square in \mathbb{F}_q^* .

Claim 4. If d is a square then \mathcal{E}' is isomorphic over \mathbb{F}_q to \mathcal{X}'_c with $c = -e/d^3$.

On Kloosterman sums, I (3/5)

Let \mathcal{E} be an ordinary elliptic curve over \mathbb{F}_q .

Claim 2. \mathcal{E} is isomorphic over \mathbb{F}_q to $\mathcal{E}' : y^2 = x^3 + dx^2 + e$, for some $d, e \in \mathbb{F}_q^*$.

Claim 3. $|\mathcal{E}'(\mathbb{F}_q)| = q + 1 + t$ with $t \equiv -1 \pmod{3}$ if and only if d is a square in \mathbb{F}_q^* .

Claim 4. If d is a square then \mathcal{E}' is isomorphic over \mathbb{F}_q to \mathcal{X}'_c with $c = -e/d^3$.

Therefore:

\mathcal{E} OEC with $|\mathcal{E}(\mathbb{F}_q)| = q + 1 + t, t \equiv -1 \pmod{3}$
 $\Rightarrow \mathcal{E}$ is isomorphic over \mathbb{F}_q to \mathcal{X}_c for some $c \in \mathbb{F}_q^*$.

On Kloosterman sums, I (4/5)

Moreover, we have an elementary fact (by which we may replace OEC with EC above):

Lemma 4. *Let $|\mathcal{E}(\mathbb{F}_q)| = q + 1 + t$. Then,*

\mathcal{E} is supersingular iff $3 \mid t$.

On Kloosterman sums, I (4/5)

Moreover, we have have an elementary fact (by which we may replace OEC with EC above):

Lemma 4. *Let $|\mathcal{E}(\mathbb{F}_q)| = q + 1 + t$. Then,*

\mathcal{E} is supersingular iff $3 \mid t$.

and a deeper fact:

Theorem 4 (Deuring (1941)). *The number $M(t)$ of isomorphism classes of elliptic curves over \mathbb{F}_q having $q + 1 + t$ points with $\gcd(q, t) = 1$ is given by*

$$M(t) = \begin{cases} H(t^2 - 4q) & \text{if } t^2 < 4q, \\ 0 & \text{otherwise.} \end{cases}$$

Here $H(d)$ is the Kronecker class number of d .

On Kloosterman sums, I (5/5)

Claims 1–4, Lemma 4, and Deuring imply

Theorem 5. *Let $q = 3^r$. The range R of $k(c)$, as c runs over \mathbb{F}_q^* , is given by*

$$R = \{t \in \mathbb{Z} : |t| < 2\sqrt{q} \text{ and } t \equiv -1 \pmod{3}\}.$$

Moreover, each value $t \in R$ is attained exactly $H(t^2 - 4q)$ times.

On Kloosterman sums, I (5/5)

Claims 1–4, Lemma 4, and Deuring imply

Theorem 5. *Let $q = 3^r$. The range R of $k(c)$, as c runs over \mathbb{F}_q^* , is given by*

$$R = \{t \in \mathbb{Z} : |t| < 2\sqrt{q} \text{ and } t \equiv -1 \pmod{3}\}.$$

Moreover, each value $t \in R$ is attained exactly $H(t^2 - 4q)$ times.

This was proved by Katz and Livne (1989), and by vds Geer and Vlught (1991), by using more advanced methods.

On the irreducible cubics ($p = 3$)

Combine Theorem 5 and Corollaries 4 and 6 to get

Corollary 7. *If $a \neq 0$, then $P_3(a, b) = (q + 1 + t)/3$ where t is an integer satisfying the following two conditions:*

- (i) $t \equiv -1 \pmod{3}$,
- (ii) $|t| < 2\sqrt{q}$.

On the irreducible cubics ($p = 3$)

Combine Theorem 5 and Corollaries 4 and 6 to get

Corollary 7. *If $a \neq 0$, then $P_3(a, b) = (q + 1 + t)/3$ where t is an integer satisfying the following two conditions:*

(i) $t \equiv -1 \pmod{3}$,

(ii) $|t| < 2\sqrt{q}$.

Conversely, for an integer t satisfying (i) and (ii), there are exactly $(q - 1)H(t^2 - 4q)$ pairs $(a, b) \in \mathbb{F}_q^2$ with $ab \neq 0$ and $P_3(a, b) = (q + 1 + t)/3$.

On Kloosterman sums, II (1/2)

Consider the divisibility modulo 3 of Kloosterman sums under the assumption $q = 2^r$.

On Kloosterman sums, II (1/2)

Consider the divisibility modulo 3 of Kloosterman sums under the assumption $q = 2^r$.

Notations:

- $\text{Tr}_{2^s}^q$ the trace function from \mathbb{F}_q onto \mathbb{F}_{2^s}
- A the set of elements $a \in \mathbb{F}_q$ with $\text{Tr}_2^q(a) = 0$
- $T_3(b)$ the number of irreducibles $x^3 + ax^2 + cx + b$ in $\mathbb{F}_q[x]$ with b fixed and a runs over the set A
- $N(b)$ the number of solutions of $x^3 = b$ in A

On Kloosterman sums, II (1/2)

Consider the divisibility modulo 3 of Kloosterman sums under the assumption $q = 2^r$.

Notations:

- $\text{Tr}_{2^s}^q$ the trace function from \mathbb{F}_q onto \mathbb{F}_{2^s}
- A the set of elements $a \in \mathbb{F}_q$ with $\text{Tr}_2^q(a) = 0$
- $T_3(b)$ the number of irreducibles $x^3 + ax^2 + cx + b$ in $\mathbb{F}_q[x]$ with b fixed and a runs over the set A
- $N(b)$ the number of solutions of $x^3 = b$ in A

Lemma 2 (and a few other results...) implies

Lemma 5. *Let $b \in \mathbb{F}_q^*$. Then,*

$$T_3(b) = \frac{1}{3} \left(\frac{1}{2} (q^2 + 1 + k(b)^2) - N(b) \right).$$

On Kloosterman sums, II (2/2)

Lemma 5 implies

Theorem 6. *Let $q = 2^r$, and let $b \in \mathbb{F}_q^*$. Then, 3 divides $k(b)$ if and only if one of the following condition holds*

1. *r is odd and $\text{Tr}_2^q(\sqrt[3]{b}) = 0$,*
2. *r is even, $b = a^3$ for some $a \in \mathbb{F}_q$, and $\text{Tr}_4^q(a) \neq 0$.*

On Kloosterman sums, II (2/2)

Lemma 5 implies

Theorem 6. *Let $q = 2^r$, and let $b \in \mathbb{F}_q^*$. Then, 3 divides $k(b)$ if and only if one of the following condition holds*

1. *r is odd and $\text{Tr}_2^q(\sqrt[3]{b}) = 0$,*
2. *r is even, $b = a^3$ for some $a \in \mathbb{F}_q$, and $\text{Tr}_4^q(a) \neq 0$.*

Remark. In the case r odd Theorem 6 was recently proved by Charpin, Helleseth and Zinoviev (using different methods).

Conclusions

- We didn't succeed too well in reaching the **Goal**

Conclusions

- We didn't succeed too well in reaching the Goal
- We succeeded not too bad in reaching the Goal

Conclusions

- We didn't succeed too well in reaching the **Goal**
- We succeeded not too bad in reaching the **Goal**
- We obtained some results on Kloosterman sums when trying to reach the **Goal**