Trace of products in finite fields and additive double character sums

Cathy Swaenepoel

IMJ-PRG, Université de Paris.

Carleton Finite Fields eSeminar,
April 28, 2021.

Plan

1. "Distribution" of the trace of products in $\mathbb{F}_q$:

$$\mathrm{Tr}(cd), \quad (c,d) \in C \times D.$$

2. Additive double character sums over some structured sets and applications:

$$\sum_{c\in C}\sum_{d\in D}\psi(cd).$$

Joint work with Arne Winterhof.

Plan

1. "Distribution" of the trace of products in $\mathbb{F}_q$:

$$\mathrm{Tr}(cd), \quad (c,d) \in C \times D.$$

2. Additive double character sums over some structured sets and applications:

$$\sum_{c \in C} \sum_{d \in D} \psi(cd).$$

Joint work with Arne Winterhof.

Trace

$q = p^r$, p prime, $r \geq 2$.

Trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$:

$$\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p, \qquad \mathrm{Tr}(x) = \sum_{j=0}^{r-1} x^{p^j}.$$

Tr is a **linear transformation** of basic importance in finite fields.

- For any linear transformation $L : \mathbb{F}_q \to \mathbb{F}_p$, there is a unique $b \in \mathbb{F}_q$ such that:

$$\forall x \in \mathbb{F}_q, \; L(x) = \mathrm{Tr}(bx).$$

- For any additive character ψ of $\mathbb{F}_q$, there is a unique $b \in \mathbb{F}_q$ such that:

$$\forall x \in \mathbb{F}_q, \; \psi(x) = \exp\left(\frac{2\pi i \, \mathrm{Tr}(bx)}{p}\right).$$

Products in $\mathbb{F}_q$

Let $C \subseteq \mathbb{F}_q^*$ and $D \subseteq \mathbb{F}_q^*$. We study the products:

$$cd, \quad (c, d) \in C \times D.$$

If C and D are large enough then these products are expected to be "well distributed".

Challenge: find a lower bound on $|C|$ and $|D|$ to ensure this behavior for a given randomness criterion.

Sárközy and co-authors have studied many problems in this spirit.

Given $A \subseteq \mathbb{F}_p$, let

$$\mathcal{E} = \{(c,d) \in C \times D : \mathrm{Tr}(cd) \in A\}.$$

Problem (Sárközy): Find a sharp lower bound on $|C|$ and $|D|$ to ensure that $\mathcal{E} \neq \emptyset$.

Interesting subsets A of $\mathbb{F}_p$ include:

- $\{s\}$ for $s \in \mathbb{F}_p$,
- subgroups of $\mathbb{F}_p^*$ (for instance squares),
- set of all generators of $\mathbb{F}_p^*$.

Recall that $\mathcal{E} = \{(c,d) \in C \times D : \mathrm{Tr}(cd) \in A\}$ and assume that $A \subseteq \mathbb{F}_p^*$.

Observe first that:

- for any $s \in \mathbb{F}_p^*$, $|\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = s\}| = p^{r-1} = q/p$,
- the proportion of $x \in \mathbb{F}_q^*$ such that $\mathrm{Tr}(x) \in A$ is

$$\frac{1}{q-1} \cdot |A| \cdot q/p = \frac{|A|}{p} \frac{q}{q-1}.$$

If the products cd were reasonably well distributed in $\mathbb{F}_q^*$ then we would expect:

$$|\mathcal{E}| \approx |C||D| \frac{|A|}{p} \frac{q}{q-1}.$$

Products cd with $\mathrm{Tr}(cd) = s \neq 0$

$$\mathcal{E} = \{(c,d) \in C \times D : \mathrm{Tr}(cd) = s\}$$

Proposition

If $s \in \mathbb{F}_p^*$ then

$$\left| |\mathcal{E}| - \frac{|C||D|q}{(q-1)p} \right| \leq \left(\frac{|C||D|q}{p} \right)^{1/2}.$$

Theorem 1 (S. 2018)

If $s \in \mathbb{F}_p^*$ and $|C||D| \geq pq$ then there exists $(c,d) \in C \times D$ such that $\mathrm{Tr}(cd) = s$.

Remark: This result is *optimal up to a constant factor*.
There are explicit sets C and D such that $pq/16 < |C||D| < pq$ and $\mathcal{E} = \emptyset$.
If $p \geq 3$ and s is a square, take for instance

$$C = \left\{ x \in \mathbb{F}_q^* : \mathrm{Tr}(x) \in (\mathbb{F}_p^*)^2 \right\} \quad \text{and} \quad D = \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2.$$

Products cd with $\mathrm{Tr}(cd) = 0$

$$\mathcal{E} = \{(c,d) \in C \times D : \mathrm{Tr}(cd) = 0\}$$

Proposition (simplified form)

$$\left| |\mathcal{E}| - \frac{|C||D|}{q-1}\left(\frac{q}{p} - 1\right) \right| \leq \frac{p-1}{p}\left(|C||D|q\right)^{1/2}.$$

Theorem 2 (S. 2018)

If $|C||D| \geq p^2 q$ *then there exists* $(c,d) \in C \times D$ *such that* $\mathrm{Tr}(cd) = 0$.

Remark: This result is *optimal up to a constant factor*.
There are explicit sets C and D such that $p^2 q/128 < |C||D| < p^2 q$ and $\mathcal{E} = \emptyset$.

Remark: If $\displaystyle\lim_{q \to +\infty} \frac{|C||D|}{p^2 q} = +\infty$, the traces $\mathrm{Tr}(cd)$ are well distributed in $\mathbb{F}_p$.

Products cd with $\mathrm{Tr}(cd) \in A$ (A subgroup)

Let A be a nontrivial subgroup of $\mathbb{F}_p^*$ and $m = |A|$.

Remark: By Theorem 1, if $|C||D| \geq pq$ then there exists $(c, d) \in C \times D$ such that $\mathrm{Tr}(cd) \in A$. This is optimal (up to constants).

Theorem 3 (S. 2018)

If C and D satisfy the two conditions:

(1) $|C||D| \geq 4pq/m^2$

(2) $\Delta_A(C) \leq 1/m$ *and* $\Delta_A(D) \leq 1/m$

then there exists $(c, d) \in C \times D$ such that $\mathrm{Tr}(cd) \in A$.

The technical condition (2) is true with a probability close to 1 (see below).

Remark: This result is *optimal up to a constant factor*:
there are sets C and D satisfying (2) such that $pq/(16m^2) < |C||D| < pq/m^2$ and $\mathcal{E} = \emptyset$.

Products cd with $\mathrm{Tr}(cd) \in A$ (A set of squares in $\mathbb{F}_p^*$)

If $p \geq 3$ and A is the set of squares in $\mathbb{F}_p^*$ (thus $m = |A| = \frac{p-1}{2}$), this implies:

Corollary (S.)

If C and D satisfy the two conditions:

(1) $|C||D| \geq \dfrac{16p}{(p-1)^2}\, q$

(2) $\Delta_A(C) \leq 1/m$ *and* $\Delta_A(D) \leq 1/m$

then, there exists $(c,d) \in C \times D$ such that $\mathrm{Tr}(cd)$ is a square in $\mathbb{F}_p^*$.

If $|C| = |D|$, it suffices to suppose $|C| \geq \dfrac{4\sqrt{p}}{p-1}\sqrt{q}$ to ensure that (1) is satisfied.

Notice that this lower bound may be substantially below $\sqrt{q}$.

Study of the condition (2)

For any nonempty subset $C \subseteq \mathbb{F}_q^*$, let

$$T_A(C) = \frac{1}{m} \sum_{t \in A \setminus \{1\}} \frac{|C \cap tC|}{|C|}$$

and

$$\Delta_A(C) = T_A(C) - \left(\frac{m-1}{m}\right) \frac{|C|-1}{q-2}.$$

Recall condition (2)**:** $\Delta_A(C) \le 1/m$ and $\Delta_A(D) \le 1/m$.

Condition (2) **is true "on average":**

Lemma (S.)

For any $1 \le d \le q-1$, the mean value of $\Delta_A(C)$ over all $C \subseteq \mathbb{F}_q^*$ with $|C| = d$ is 0.

Study of the condition (2)

Recall condition (2): $\Delta_A(C) \leq 1/m$ and $\Delta_A(D) \leq 1/m$.

Lemma (S.)

For any $1 \leq d \leq q-1$*, the variance of* $\Delta_A(C)$ *over all* $C \subseteq \mathbb{F}_q^*$ *with* $|C| = d$ *satisfies*

$$\frac{1}{\binom{q-1}{d}} \sum_{|C|=d} (\Delta_A(C))^2 = O\left(\frac{1}{mq}\right).$$

The probability that condition (2) is true is close to 1:
$\mathbb{P}\left(\Delta_A(C) \leq \frac{1}{m}\right) = 1 - O\left(\frac{m}{q}\right)$ with $\frac{m}{q} \to 0$ as $q \to +\infty$.

Examples of subsets C such that $\Delta_A(C) \leq 1/m$:
all subsets of affine hyperplanes of the form $\{x \in \mathbb{F}_q : f(x) = s\}$ where f is an $\mathbb{F}_p$-linear form and $s \in \mathbb{F}_p^*$.

The study of the quantity $|C \cap tC|$ is of independent interest.

Green and Konyagin (2009): if C is a subset of a group G of prime order with $|C| = \gamma|G|$ then there exists $x \in G$ such that

$$\Big||C \cap xC| - \gamma^2|G|\Big| = O(|G|(\log\log|G|/\log|G|)^{1/3}).$$

Notice that a similar statement with $G = \mathbb{F}_q^*$ does not hold:
if C is the set of squares then $|C| = \gamma|G|$ with $\gamma = 1/2$ and $C \cap xC = \emptyset$ or C.

Question: for $G = \mathbb{F}_q^*$ and C such that $|C| = \gamma|G|$,
give natural conditions on C so that $|C \cap xC|$ is "close" to $\gamma^2|G|$ for at least one $x \in G$.

Main arguments to estimate $|\mathcal{E}|$

Recall $\mathcal{E} = \{(c,d) \in C \times D : \mathrm{Tr}(cd) \in A\}$. Assume $A \subseteq \mathbb{F}_p^*$.

$$|\mathcal{E}| = \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x) \in A}} \sum_{(c,d) \in C \times D} \underbrace{\frac{1}{q-1} \sum_{\chi} \chi(cd)\overline{\chi(x)}}_{\mathbb{1}_{cd=x}} = \frac{1}{q-1} \sum_{\chi} \underbrace{\sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x) \in A}} \overline{\chi(x)}}_{U_A(\chi)} \underbrace{\sum_{c \in C} \chi(c)}_{S_C(\chi)} \underbrace{\sum_{d \in D} \chi(d)}_{S_D(\chi)}$$

Contribution of $\chi = \chi_0$: $|C||D| \frac{|A|}{p} \frac{q}{q-1}$.

For the sum over $\chi \neq \chi_0$:

- rewrite $U_A(\chi)$ as a product of two Gaussian sums and a character sum over A and deduce a sharp upper bound,
- apply Cauchy–Schwarz inequality,
- in the case where A is a subgroup, compute $\displaystyle\sum_{\substack{\chi \neq \chi_0 \\ \chi_{|A} = 1}} |S_C(\chi)|^2$

  (this makes appear $|C \cap tC|$).

Conclusion

- We provide (almost) optimal answers to Sárközy's question.
- For instance, we prove that if $p \geq 3$ and if C and D satisfy the two conditions:

  (1) $|C||D| \geq \dfrac{16p}{(p-1)^2}\, q$

  (2) technical condition (true with probability close to 1)

  then there exists $(c, d) \in C \times D$ such that $\mathrm{Tr}(cd)$ is a square in $\mathbb{F}_p^*$.
- If $L : \mathbb{F}_q \to \mathbb{F}_p$ is a linear transformation with $L \neq 0$ then the previous results can be reformulated with L in place of Tr (use $L(x) = \mathrm{Tr}(bx)$ for some $b \in \mathbb{F}_q^*$).

Remark: Mattheus (2019) uses an approach based on spectral graph theory with no reference to character theory to estimate $|\mathcal{E}|$. In particular, he extends some of the previous results to trace functions $\mathrm{Tr} : \mathbb{F}_{q^h} \to \mathbb{F}_q$.

1. "Distribution" of the trace of products in $\mathbb{F}_q$:

$$\mathrm{Tr}(cd), \quad (c,d) \in C \times D.$$

2. Additive double character sums over some structured sets and applications:

$$\sum_{c \in C} \sum_{d \in D} \psi(cd).$$

Joint work with Arne Winterhof.

Additive double character sums

$q = p^r$, p prime, $r \geq 1$.

We consider character sums of the form

$$\sum_{c \in C} \sum_{d \in D} \psi(cd)$$

where $C, D \subseteq \mathbb{F}_q$ and ψ is a non-trivial additive character of $\mathbb{F}_q$.

Many results on this type of character sums (with some variants) and many applications: Bourgain, Fouvry, Garaev, Glibichuk, Gyarmati, Konyagin, Michel, Niederreiter, Roche-Newton, Sárközy, Shparlinski, Vinogradov, Winterhof, ...

Classical bound

For any non-trivial additive character ψ of $\mathbb{F}_q$ and any subsets $C, D \subseteq \mathbb{F}_q$,

$$\left|\sum_{c\in C}\sum_{d\in D}\psi(cd)\right| \leq (|C||D|q)^{1/2}. \tag{1}$$

Proof: Cauchy–Schwarz inequality and orthogonality relations for characters.

- Non-trivial if $|C||D| > q$.
- Tight in general:
  for instance, if q is a square, if $C = D = \mathbb{F}_{q^{1/2}}$ and ψ is any non-trivial additive character of $\mathbb{F}_q$ which is trivial on the subfield $\mathbb{F}_{q^{1/2}}$ then (1) is an equality.

With structured sets such as additive or multiplicative subgroups, we know better bounds.

- Winterhof (2001): If D is an additive subgroup of $\mathbb{F}_q$ then

$$\sum_{c\in\mathbb{F}_q}\left|\sum_{d\in D}\psi(cd)\right|\leq q.$$

$\Rightarrow |\sum_{c\in C}\sum_{d\in D}\psi(cd)|\leq q$ for any $C\subseteq\mathbb{F}_q$. This is better than the classical bound.

- Bourgain, Glibichuk, Konyagin (2006): If $q=p$ then for any multiplicative subgroup D of $\mathbb{F}_p^*$ with $|D|\gg p^{\varepsilon}$ and for any $c\in\mathbb{F}_p^*$,

$$\left|\sum_{d\in D}\psi(cd)\right|\leq\frac{|D|}{p^{\gamma_\varepsilon}}\qquad(\gamma_\varepsilon>0).$$

$\Rightarrow$ non-trivial bound on $|\sum_{c\in C}\sum_{d\in D}\psi(cd)|$ for arbitrary $C\subseteq\mathbb{F}_p^*$ and very small subgroups D of $\mathbb{F}_p^*$.

Required structure for D

We will assume that there is a rational function $f(X) \in \mathbb{F}_q(X)$ satisfying a certain property of nonlinearity:

$$(2) \qquad f(X) \notin \{a(g(X)^p - g(X)) + bX + c : g(X) \in \mathbb{F}_q(X), a, b, c \in \mathbb{F}_q\}$$

such that

$$f(D) \subseteq D.$$

Examples of $f(X) \in \mathbb{F}_q(X)$ satisfying (2) are $f(X) = X^{-1}$ and $f(X) = X^2$ for odd q.

Examples of sets D with the required structure are $D = S \cup S^{-1}$ for $S \subseteq \mathbb{F}_q^*$.

Result

Theorem 1 (S. and Winterhof, 2021)

Let $D \subseteq \mathbb{F}_q$ and assume that there exists $f(X) \in \mathbb{F}_q(X)$ of degree k satisfying (2) *such that $f(D) \subseteq D$. Then there exists $U \subseteq D$ with*

$$|U| \geq \frac{|D|}{k+1}$$

such that for any $C \subseteq \mathbb{F}_q$ and any non-trivial additive character ψ of $\mathbb{F}_q$,

(3) $$\left| \sum_{c \in C} \sum_{u \in U} \psi(cu) \right| \ll_k \left(\frac{|C|^3 |D|^3 q}{M(|D|)} \right)^{1/4}$$

where

(4) $$M(|D|) = \min \left\{ \frac{q^{1/2}}{|D|^{1/2} (\log |D|)^{11/4}}, \frac{|D|^{4/5}}{q^{2/5} (\log |D|)^{31/10}} \right\}.$$

Strength of (3)

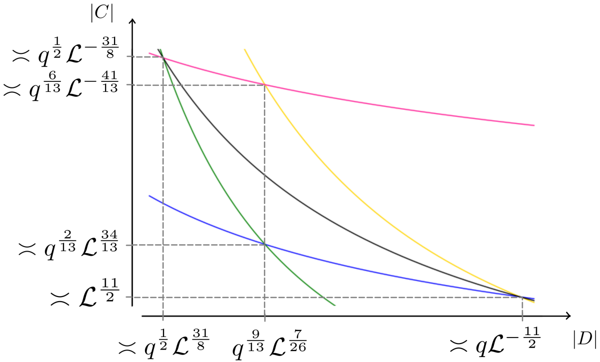
There exists a constant $\lambda > 0$ (depending only on k) such that (3) is non-trivial and improves the classical bound if

$$\lambda \max\left\{ \frac{q^{\frac{1}{2}}(\log q)^{\frac{11}{4}}}{|D|^{\frac{1}{2}}}, \frac{q^{\frac{7}{5}}(\log q)^{\frac{31}{10}}}{|D|^{\frac{9}{5}}} \right\} < |C| < \lambda^{-1} \min\left\{ \frac{q^{\frac{3}{2}}}{|D|^{\frac{3}{2}}(\log q)^{\frac{11}{4}}}, \frac{q^{\frac{3}{5}}}{|D|^{\frac{1}{5}}(\log q)^{\frac{31}{10}}} \right\}$$

(see next slide).

- If $|D| \asymp q^{\frac{9}{13}+\varepsilon}$ and $|C| \asymp q^{\frac{2}{13}}$ then (3) is non-trivial (while the classical bound is trivial).
- If $|D| \asymp q^{\frac{9}{13}}$ and $|C| \asymp q/|D|$ then (3) improves the classical bound by a factor $q^{-\frac{1}{26}}$ (up to logarithmic factors).

(3) is non-trivial and improves the classical bound if the point $(|D|, |C|)$ is in the surface bounded by the four colored curves:



Here $\mathcal{L} = \log q$ and the black curve corresponds to $|C||D| = q$.

Condition (2) of $f(X)$ cannot be removed from Theorem 1.

Without this condition, we could take

$$C = \left\{0, 1, 2, \ldots, \lfloor 0.1 p^{1/2} \rfloor\right\}, \; D = \{x \in \mathbb{F}_q : \mathrm{Tr}(x) \in C\}, \; f(X) = X, \; \psi(x) = \exp\left(\frac{2\pi i \, \mathrm{Tr}(x)}{p}\right).$$

Then for any $U \subseteq D$,

$$\left| \sum_{c \in C} \sum_{u \in U} \psi(cu) \right| \geq |C||U| \cos(0.02\pi) \geq 0.99|C||U|.$$

Moreover, there exist absolute constants $\lambda_1, \lambda_2 > 0$ such that if

$$\lambda_1 (\log q)^{11} < p < \lambda_2 q (\log q)^{-31/4}$$

then the right-hand side of (3) is $< 0.99|C||D|/2$.

Therefore, (3) holds for no U with $|U| \geq |D|/2$.

Proof of Theorem 1

Additive energy of $S \subseteq \mathbb{F}_q$:

$$E(S) = |\{(s_1, s_2, s_3, s_4) \in S^4 : s_1 + s_2 = s_3 + s_4\}|.$$

The proof is a combination of:

1. a bound on additive double character sums in terms of additive energy,
2. an existence result of a large subset of small additive energy.

Lemma 1

For any $C, U \subseteq \mathbb{F}_q$ and any non-trivial additive character ψ of $\mathbb{F}_q$,

$$\left| \sum_{c \in C} \sum_{u \in U} \psi(cu) \right| \le \left(|C|^3 E(U) q \right)^{1/4}.$$

Non-trivial and better than the classical bound if $\dfrac{qE(U)}{|U[^4} < |C| < \dfrac{q|U|^2}{E(U)}$.

Proof:

$$\left| \sum_{c \in C} \sum_{u \in U} \psi(cu) \right|^4 \le \left(\sum_{c \in C} \left| \sum_{u \in U} \psi(cu) \right| \right)^4 \le |C|^3 \sum_{c \in \mathbb{F}_q} \left| \sum_{u \in U} \psi(cu) \right|^4 \quad \text{(by Hölder's inequality)}$$

$$= |C|^3 \sum_{u_1, u_2, u_3, u_4 \in U} \sum_{c \in \mathbb{F}_q} \psi(c(u_1 + u_2 - u_3 - u_4)) = |C|^3 E(U) q.$$

Existence of a large subset of small additive energy

Goal: If D is as in Theorem 1 then there is a large $U \subseteq D$ of small additive energy.
To prove this, we use:

Theorem (Roche-Newton, Shparlinski, Winterhof, 2019)

For any $D \subseteq \mathbb{F}_q$ and any rational function $f(X) \in \mathbb{F}_q(X)$ of degree k satisfying (2), there exist disjoint sets $S, T \subseteq D$ such that $D = S \cup T$ and

$$\max\{E(S), E(f(T))\} \ll_k \frac{|D|^3}{M(|D|)}$$

where $M(|D|)$ is defined by (4).

- If $|S| \geq \frac{|D|}{k+1}$ then we take $U = S$. Otherwise, $|T| \geq \frac{k|D|}{k+1}$ and we take $U = f(T)$.
- In both cases, $|U| \geq \frac{|D|}{k+1}$ and $E(U) \ll_k \frac{|D|^3}{M(|D|)}$.
- Moreover, if $f(D) \subseteq D$ then $U \subseteq D$.

Existence of a large subset of small additive energy

To sum up, we have proved:

Lemma 2

Let $D \subseteq \mathbb{F}_q$ and assume that there exists $f(X) \in \mathbb{F}_q(X)$ of degree k satisfying (2) *such that $f(D) \subseteq D$. Then there exists $U \subseteq D$ such that*

$$|U| \geq \frac{|D|}{k+1}$$

and

$$E(U) \ll_k \frac{|D|^3}{M(|D|)}. \tag{5}$$

Remark: There are sets D with the required structure such that $E(D) \gg |D|^3$ and $M(|D|) \geq \log q$.

Theorem 1 follows from Lemmas 1 and 2.

Remarks

- Mohammadi and Stevens recently improved the decomposition theorem of Roche-Newton, Shparlinski and Winterhof (2019) by obtaining a larger $M(|D|)$.
- As they noted, this automatically leads to an improvement of Theorem 1.

First application of Theorem 1

We apply Theorem 1 to the following problem:

for $C, D \subseteq \mathbb{F}_q$, find conditions on $|C|$ and $|D|$ such that $\mathrm{Tr}(CD) = \mathbb{F}_p$.

First application of Theorem 1

For arbitrary sets (according to the first part of the talk):

Theorem (S. 2018)

Let $C, D \subseteq \mathbb{F}_q^*$. *If* $|C||D| \geq p^2 q$ *then* $\mathrm{Tr}(CD) = \mathbb{F}_p$.

In general, the condition $|C||D| \geq p^2 q$ is optimal up to an absolute constant factor.

For (mildly) structured sets:

Theorem 2 (S. and Winterhof, 2021)

Let $C, D \subseteq \mathbb{F}_q$ *and assume that there exists* $f(X) \in \mathbb{F}_q(X)$ *of degree* k *satisfying* (2) *such that* $f(D) \subseteq D$. *There exists a constant* $\lambda > 0$ *depending only on* k *such that if*

$$|C||D|M(|D|) > \lambda p^4 q \tag{6}$$

then $\mathrm{Tr}(CD) = \mathbb{F}_p$.

The condition (2) on $f(X)$ cannot be removed from Theorem 2.

If
$$\lambda^{5/4}p^{5/2}q^{1/2}(\log q)^{31/8} < |D| < \frac{q}{\lambda^2 p^4(\log q)^{11/2}}$$
(with λ as in Theorem 2) then the lower bound (6) defines a larger range of $|C|$ with $\mathrm{Tr}(CD) = \mathbb{F}_p$ than the lower bound for arbitrary sets.

This range for $|D|$ is non-trivial if $q = p^r$ with $r \geq 14$ and q is sufficiently large (provided that λ is bounded by an absolute constant)

It follows from Theorem 2 that $\mathrm{Tr}(CD) = \mathbb{F}_p$ for any D with $|D| \asymp q^{9/13+\varepsilon}$ such that D is closed under inversion and for any C with $|C| \gg p^4 q^{2/13}$.
Notice that we can choose $|C|$ such that $|C||D| \asymp p^4 q^{11/13+\varepsilon}$ which may be much smaller than $p^2 q$.

Proof of Theorem 2

Let U be as in Theorem 1. For $s \in \mathbb{F}_p$, let $N_s = |\{(c,u) \in C \times U : \mathrm{Tr}(cu) = s\}|$.
For any $s \in \mathbb{F}_p$,

$$N_s = \frac{1}{p} \sum_{j=0}^{p-1} \mathrm{e}_p(-js) \sum_{(c,u) \in C \times U} \mathrm{e}_p(j\,\mathrm{Tr}(cu)) \qquad \text{where } \mathrm{e}_p(x) = \exp(2i\pi x/p)$$

hence

$$\left| N_s - \frac{|C||U|}{p} \right| \leq \max_{1 \leq j \leq p-1} \left| \sum_{(c,u) \in C \times U} \mathrm{e}_p(j\,\mathrm{Tr}(cu)) \right| \leq \lambda_k \left(\frac{|C|^3 |D|^3 q}{M(|D|)} \right)^{1/4}.$$

If $\frac{|C||D|}{(k+1)p} > \lambda_k \left(\frac{|C|^3|D|^3 q}{M(|D|)} \right)^{\frac{1}{4}}$ then, since $|U| \geq \frac{|D|}{k+1}$, we have $N_s \neq 0$ for any $s \in \mathbb{F}_p$, thus

$$\mathbb{F}_p = \mathrm{Tr}(CU) \subseteq \mathrm{Tr}(CD).$$

We apply Theorem 1 to the following problem:

for $A, B, C, D \subseteq \mathbb{F}_q$, find conditions on $|A|, |B|, |C|, |D|$ such that there is a solution $(a, b, c, d) \in A \times B \times C \times D$ of the sum-product equation

$$a + b = cd.$$

Second application of Theorem 1

Let $A, B, C, D \subseteq \mathbb{F}_q$ and denote $N = \{(a,b,c,d) \in A \times B \times C \times D : a + b = cd\}$.
For arbitrary sets:

Theorem (Gyarmati and Sárközy, 2008)

If $|A||B||C||D| > q^3$ *then* $N > 0$.

In general, this condition is optimal up to an absolute constant factor.

For (mildly) structured sets:

Theorem 3 (S. and Winterhof, 2021)

Assume that there exists $f(X) \in \mathbb{F}_q(X)$ *of degree* k *satisfying* (2) *such that* $f(D) \subseteq D$. *Then there exists a constant* $\lambda > 0$ *depending only on* k *such that if*

$$|A|^2|B|^2|C||D|M(|D|) > \lambda q^5$$

then $N > 0$.

Conclusion

- We give (almost optimal) conditions on C and D to ensure that $\mathrm{Tr}(CD) \cap A \neq \emptyset$ for some interesting subsets A of $\mathbb{F}_p$.
- We prove that if D has some desirable structure then there is a large subset U of D for which the classical upper bound on $|\sum_{c \in C} \sum_{u \in U} \psi(cu)|$ can be improved.
- We apply this new bound to trace products and sum-product equations and improve previous results (provided that one of the involved sets has some structure).

Conclusion

- We give (almost optimal) conditions on C and D to ensure that $\mathrm{Tr}(CD) \cap A \neq \emptyset$ for some interesting subsets A of $\mathbb{F}_p$.
- We prove that if D has some desirable structure then there is a large subset U of D for which the classical upper bound on $|\sum_{c\in C}\sum_{u\in U}\psi(cu)|$ can be improved.
- We apply this new bound to trace products and sum-product equations and improve previous results (provided that one of the involved sets has some structure).

Thank you for your attention!