Equations in finite fields with restricted solution sets, II. (Algebraic equations)

by
K. Gyarmati
Alfréd Rényi Institute of Mathematics
H–1053 Budapest, Reáltanoda u. 13–15
Hungary
e-mail: gykati@cs.elte.hu
and
A. Sárközy
Eötvös Loránd University
Department of Algebra and Number Theory
H–1117 Budapest, Pázmány Péter sétány 1/C
Hungary
e-mail: sarkozy@cs.elte.hu

Abstract

Generalizing earlier results, it is shown that if $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ are "large" subsets of a finite field $\mathbb{F}_q$, then the equations

$$a+b=cd,$$

resp.

$$ab+1=cd$$

can be solved with $a\in\mathcal{A}$, $b\in\mathcal{B}$, $c\in\mathcal{C}$, $d\in\mathcal{D}$. Other algebraic equations with solutions restricted to "large" subsets of $\mathbb{F}_q$ are also studied. The proofs are based on character sum estimates proved in Part I of the paper.

2000 Mathematics Subject Classification: 11T24.
Key words and phrases: finite field, equation, character sum.
Research partially supported by the Hungarian National Foundation for Scientific Research, Grants No. T 043623, T 043631 and T 049693.

1 Introduction

In [4] and [5] Sárközy proved that if $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ are "large" (but otherwise unspecified) subsets of $\mathbb{Z}_p$, more precisely, $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| \gg p^3$, then the equations

$$a+b=cd, \tag{1.1}$$

resp.

$$ab+1=cd \tag{1.2}$$

can be solved with $a\in\mathcal{A}$, $b\in\mathcal{B}$, $c\in\mathcal{C}$, $d\in\mathcal{D}$, while in [1] Gyarmati studied the solvability of

$$a+b=f(x), \quad a\in\mathcal{A},\ b\in\mathcal{B}, \tag{1.3}$$

resp.

$$ab=f(x), \quad a\in\mathcal{A},\ b\in\mathcal{B} \tag{1.4}$$

for "large" subsets $\mathcal{A},\mathcal{B}\subset\mathbb{Z}_p$ and $f(x)\in\mathbb{Z}_p[x]$. In this paper we will generalize the results on the solvability of (1.1) and (1.2) to finite fields $\mathbb{F}_q$. We will also study the solvability of other algebraic equations with solutions restricted to "large" subsets of $\mathbb{F}_q$. The proofs will be based on the character sums estimates given in Part I [2]. (In Part III we will study "hybrid" problems which also involve special sets like equations (1.3) and (1.4).)

Throughout this paper we will use the following notations: We consider finite fields $\mathbb{F}_q$ with order $q=p^r$. We write $\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$. ψ denotes an additive, χ a multiplicative character of $\mathbb{F}_q$. We set $\chi(0)=0$. The trivial additive character is denoted by ψ_0, the trivial (principal) multiplicative character is denoted by χ_0. We write $e^{2\pi i\alpha}=e(\alpha)$ and $e\left(\frac{n}{p}\right)=e_p(n)$. $\mathbb{N}$ denotes the set of the positive integers and $\mathbb{Z}$ is the set of the integers.

We will need the following character sum estimates proved in [2]:

Theorem A. *If $\mathcal{A},\mathcal{B}\subset\mathbb{F}_q$ and ψ is a nontrivial additive character of $\mathbb{F}_q$, then we have*

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\psi(ab)\right|\le\left(|\mathcal{A}|\ |\mathcal{B}|q\right)^{1/2}.$$

Indeed, this is Corollary 1 in [2].

Theorem B. *If $\mathcal{A},\mathcal{B}\subset\mathbb{F}_q$ and χ is a nontrivial multiplicative character of $\mathbb{F}_q$, then we have*

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(ab+1)\right|\le\left(|\mathcal{A}|^{1/2}+1\right)\left(|\mathcal{B}|q\right)^{1/2}.$$

This is a special case of Theorem 3' and Corollary 5 in [2].

In the next two theorems the generalizations of the double sums in Theorems A and B are studied, but the price paid for the much greater generality is that the upper bounds obtained are weaker.

Theorem C. *Assume that $\alpha(x)$, $\beta(x)$ are complex valued functions on $\mathbb{F}_q$, ψ is a nontrivial additive character of $\mathbb{F}_q$, $f(x,y) \in \mathbb{F}_q[x,y]$, and $f(x,y)$ is not of the form $g(x)+h(y)$:*

$$f(x,y) \neq g(x)+h(y) \quad (\textit{with } g(x), h(x) \in \mathbb{F}_q[x]). \tag{1.5}$$

Write $f(x,y)$ in the form

$$f(x,y) = \sum_{k=0}^{n} g_k(y)x^k \tag{1.6}$$

(with $g_k(y) \in \mathbb{F}_q[y]$), and let K denote the greatest k value with the property that $g_k(y)$ is not identically constant: $g_K(y) \not\equiv c$ and either $K = n$ or $g_{K+1}(y), g_{K+2}(y), \ldots, g_n(y)$ are identically constant so that, by (1.5),

$$K > 0.$$

Denote the degree of the polynomial $g_K(y)$ by D so that

$$D > 0,$$

and assume that

$$(K,q) = 1. \tag{1.7}$$

Write

$$S = \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \alpha(x)\beta(y)\psi\big(f(x,y)\big),$$

$$X = \sum_{x \in \mathbb{F}_q} |\alpha(x)|^2 \quad \textit{and} \quad Y = \sum_{y \in \mathbb{F}_q} |\beta(y)|^2.$$

Then we have

$$|S| \leq \big(XYq\big(D + (K-1)q^{1/2}\big)\big)^{1/2}.$$

This is Theorem 4 in [2]. Note that, as we explained in [2], conditions (1.5) and (1.7) are necessary, however, in the important special case $r = 1$, i.e., $q = p^r = p =$ prime condition (1.7) can be dropped.

Before presenting the next theorem, we need some definitions from Part I.

Definition 1. A polynomial

$$F(x,y) = \sum_{i=0}^{n} G_i(y)x^i = \sum_{j=0}^{m} H_j(x)y^j \in \mathbb{F}_q[x,y]$$

is said to be *primitive in x* if $\big(G_0(y), \ldots, G_n(y)\big) = 1$, and it is said to be *primitive in y* if $\big(H_0(x), \ldots, H_m(x)\big) = 1$.

Definition 2. Every polynomial $f(x,y) \in \mathbb{F}_q[x,y]$ can be written in form

$$f(x,y) = F(x)G(y)H(x,y) \tag{1.8}$$

where $H(x,y) \in \mathbb{F}[x,y]$ is primitive in both x and y, and apart from constant factors, this representation is unique. The polynomial $H(x,y)$ (uniquely determined apart from a constant factor) is called the *primitive kernel* of $f(x,y)$.

Theorem D. *Assume that $\alpha(x)$, $\beta(x)$ are complex valued functions on $\mathbb{F}_q$, χ is a nontrivial multiplicative character of $\mathbb{F}_q$ of order d, $f(x,y) \in \mathbb{F}_q[x,y]$, the primitive kernel $H(x,y)$ of $f(x,y)$ is not of the form $c\big(K(x,y)\big)^d$:*

$$H(x,y) \neq c\big(K(x,y)\big)^d \quad \text{for} \quad c \in \mathbb{F}_q,\ K(x,y) \in \mathbb{F}_q[x,y], \tag{1.9}$$

and $f(x,y)$ is of degree n and m in x, resp. y. Then, writing

$$S = \sum_{x\in\mathbb{F}_q} \sum_{y\in\mathbb{F}_q} \alpha(x)\beta(y)\chi\big(f(x,y)\big),$$

$$X = \sum_{x\in\mathbb{F}_q} |\alpha(x)|^2, \qquad Y = \sum_{y\in\mathbb{F}_q} |\beta(y)|^2$$

and

$$B = \max_{y\in\mathbb{F}_q} |\beta(y)|,$$

we have

$$|S| \le \big(X(2nYq^{3/2} + 5B^2nmq^2)\big)^{1/2}.$$

This is Theorem 5 in [2].

2 Sums and products

First we will study equation (1.1):

Theorem 1. *If q is a prime power, $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{F}_q$, and the number of solutions of*

$$a + b = cd, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{2.1}$$

is denoted by N, then we have

$$\left| N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} \right| \le \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2} q^{1/2}.$$

Corollary 1. *If q is a prime power, $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{F}_q$ and*

$$|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > q^3, \tag{2.2}$$

then (2.1) can be solved.

Note that the $q = p =$ prime special case of Theorem 1 and Corollary 1 above is Theorem 1 resp. Corollary 1 in [4]. These results above have similar consequences as Theorem 1 and Corollary 1 in [4]; e.g., it follows from Corollary 1 that for $k \in \mathbb{N}$ and large subsets $\mathcal{A}$, $\mathcal{B}$ of $\mathbb{F}_q$, the equation

$$a + b = x^k, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ x \in \mathbb{F}_q$$

can be solved, and for $m, n, k \in \mathbb{N}$, $q > q_0(m, n, k)$ the equation

$$x^m + y^n = z^k, \quad xyz \neq 0, \quad x, y, z \in \mathbb{F}_q,$$

in particular,

$$x^k + y^k = z^k, \quad xyz \neq 0, \quad x, y, z \in \mathbb{F}_q$$

is also solvable (the latter is, of course, the generalization of Schur's theorem [6]).

Proof of Theorem 1. For every $a, b, c, d \in \mathbb{F}_q$ we have

$$\frac{1}{q}\sum_{\psi} \psi(a + b - cd) = \begin{cases} 1 & \text{if } a + b = cd \\ 0 & \text{if } a + b \neq cd \end{cases}$$

(where ψ runs over the additive characters of $\mathbb{F}_q$) so that

$$N = \frac{1}{q}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{\psi}\psi(a + b - cd).$$

Separating the $\psi = \psi_0$ term we obtain

$$\begin{aligned} N &= \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} + \frac{1}{q}\sum_{\psi\neq\psi_0}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\psi(a + b - cd) = \\ &= \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} + \frac{1}{q}\sum_{\psi\neq\psi_0}\Big(\sum_{a\in\mathcal{A}}\psi(a)\Big)\Big(\sum_{b\in\mathcal{B}}\psi(b)\Big)\Big(\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\psi(-cd)\Big) \end{aligned}$$

whence

(2.3)

$$\begin{aligned} \left|N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| &= \frac{1}{q}\left|\sum_{\psi\neq\psi_0}\Big(\sum_{a\in\mathcal{A}}\psi(a)\Big)\Big(\sum_{b\in\mathcal{B}}\psi(b)\Big)\Big(\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\overline{\psi}(cd)\Big)\right| \leq \\ &\leq \frac{1}{q}\sum_{\psi\neq\psi_0}\left|\sum_{a\in\mathcal{A}}\psi(a)\right|\,\left|\sum_{b\in\mathcal{B}}\psi(b)\right|\,\left|\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\overline{\psi}(cd)\right|. \end{aligned}$$

By using Theorem A and Cauchy's inequality, it follows that

$$\left|N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| \leq \frac{1}{q}\sum_{\psi\neq\psi_0}\left|\sum_{a\in\mathcal{A}}\psi(a)\right|\,\left|\sum_{b\in\mathcal{B}}\psi(b)\right|\big(|\mathcal{C}|\,|\mathcal{D}|q\big)^{1/2} =$$

$$= \left(\frac{|\mathcal{C}|\,|\mathcal{D}|}{q}\right)^{1/2} \sum_{\psi\neq\psi_0} \left|\sum_{a\in\mathcal{A}} \psi(a)\right| \left|\sum_{b\in\mathcal{B}} \psi(b)\right| \leq$$

$$\leq \left(\frac{|\mathcal{C}|\,|\mathcal{D}|}{q}\right)^{1/2} \left(\sum_{\psi} \left|\sum_{a\in\mathcal{A}} \psi(a)\right|^2\right)^{1/2} \left(\sum_{\psi} \left|\sum_{b\in\mathcal{A}} \psi(b)\right|^2\right)^{1/2}$$

whence, by the identity

$$\sum_{\psi} \left|\sum_{h\in\mathbb{F}_q} z_h \psi(h)\right|^2 = q \sum_{h\in\mathbb{F}_q} |z_h|^2 \tag{2.4}$$

(for any complex numbers $z_h \in \mathbb{C}$),

$$\left|N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| \leq \left(\frac{|\mathcal{C}|\,|\mathcal{D}|}{q}\right)^{1/2} \big(q|\mathcal{A}|\big)^{1/2} \big(q|\mathcal{B}|\big)^{1/2} = \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|q\big)^{1/2}$$

which completes the proof of Theorem 1. □

Proof of Corollary 1. By Theorem 1, it follows from (2.2) that

$$N \geq \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} - \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2} q^{1/2} =$$

$$= \frac{\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}}{q} \Big(\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2} - q^{3/2}\Big) > 0.$$

3 Products and shifted products

We will generalize Theorem 1 and Corollary 1 in [5] by proving:

Theorem 2. *If q is a prime power, $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{F}_q$, and the number of solutions of the equation*

$$ab + 1 = cd, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{3.1}$$

is denoted by N, then we have

$$\left|N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| \leq 8\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2} q^{1/2} + 4q^2. \tag{3.2}$$

Corollary 2. *If q is a prime power, $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{Z}_q$ and*

$$|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > 100q^3, \tag{3.3}$$

then (3.1) can be solved.

Proof of Theorem 2. Write

$$N_1 = \big|\big\{(a,b,c,d) : ab+1 = cd \neq 0,\ a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}\big\}\big|$$

and

$$N_2 = \big|\big\{(a,b,c,d) : ab+1 = cd = 0,\ a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}\big\}\big|$$

so that

$$N = N_1 + N_2. \tag{3.4}$$

Then, by $\chi(0) = 0$, we have

$$\begin{aligned} N_1 &= \frac{1}{q-1}\sum_{\chi}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\chi(ab+1)\overline{\chi}(cd) = \\ &= \frac{1}{q-1}\Big(\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\chi_0\big((ab+1)cd\big) + \\ &\qquad + \sum_{\chi\neq\chi_0}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\chi(ab+1)\overline{\chi}(cd)\Big) = \\ &= \frac{1}{q-1}(N_3+N_4) \end{aligned} \tag{3.5}$$

where

$$\begin{aligned} N_3 &= \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\chi_0\big((ab+1)cd\big) = \\ &= \big|\big\{(a,b,c,d) :\ a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}\big\}\big| - \\ &\quad - \big|\big\{(a,b,c,d) :\ (ab+1)cd = 0,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}\big\}\big| = \\ &= \big|\mathcal{A}\big|\,\big|\mathcal{B}\big|\,\big|\mathcal{C}\big|\,\big|\mathcal{D}\big| - N_5 \end{aligned} \tag{3.6}$$

with

$$N_5 = \big|\big\{(a,b,c,d) :\ (ab+1)cd = 0,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}\big\}\big|$$

and

$$N_4 = \sum_{\chi\neq\chi_0}\Big(\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(ab+1)\Big)\Big(\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\overline{\chi}(cd)\Big).$$

It remains to estimate N_2, N_4 and N_5. N_2 and N_5 can be estimated easily in exactly the same way as in [5], and we obtain

$$|N_2| \leq |\mathcal{A}|\big(|\mathcal{C}| + |\mathcal{D}|\big) \leq 2q^2 \tag{3.7}$$

and

$$|N_5| \leq |\mathcal{A}|\,|\mathcal{C}|\,|\mathcal{D}| + |\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{D}| + |\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}| \leq 3\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}q^{3/2}. \tag{3.8}$$

The crucial part of the proof is the estimate of N_4 which will be based on Theorem B. Indeed, by Theorem B and Cauchy's inequality we have

$$\begin{aligned}
|N_4| &\le \sum_{\chi\neq\chi_0}\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(ab+1)\right|\left|\sum_{c\in\mathcal{C}}\chi(c)\right|\left|\sum_{d\in\mathcal{D}}\chi(d)\right| \le \\
&\le \big(|\mathcal{A}|^{1/2}+1\big)\big(|\mathcal{B}|q\big)^{1/2}\sum_{\chi\neq\chi_0}\left|\sum_{c\in\mathcal{C}}\chi(c)\right|\left|\sum_{d\in\mathcal{D}}\chi(d)\right| \le \\
&\le \big(|\mathcal{A}|^{1/2}+1\big)\big(|\mathcal{B}|q\big)^{1/2}\left(\sum_{\chi}\left|\sum_{c\in\mathcal{C}}\chi(c)\right|^2\right)^{1/2}\left(\sum_{\chi}\left|\sum_{d\in\mathcal{D}}\chi(d)\right|^2\right)^{1/2}
\end{aligned}$$

whence, by the identity

$$\sum_{\chi}\left|\sum_{h\in\mathbb{F}_q^*}z_h\chi(h)\right|^2=(q-1)\sum_{h\in\mathbb{F}_q^*}|z_h|^2 \tag{3.9}$$

(for any complex numbers $z_h\in\mathbb{C}$),

$$\begin{aligned}
|N_4| &\le \big(|\mathcal{A}|^{1/2}+1\big)\big(|\mathcal{B}|q\big)^{1/2}\big((q-1)|\mathcal{C}|\big)^{1/2}\big((q-1)|\mathcal{D}|\big)^{1/2}= \\
&= (q-1)\big(|\mathcal{A}|^{1/2}+1\big)\big(|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|q\big)^{1/2}.
\end{aligned} \tag{3.10}$$

It follows from (3.4), (3.5), (3.6), (3.7), (3.8) and (3.10) that

$$\begin{aligned}
&\left|N-\frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| = \\
&= \left|\left(\frac{1}{q-1}\big(\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|-N_5\big)+N_4\big)+N_2\right)-\frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| \le \\
&\le |\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\left|\frac{1}{q-1}-\frac{1}{q}\right|+\frac{1}{q-1}\big(|N_5|+|N_4|\big)+|N_2| \le \\
&\le \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{(q-1)q}+\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}\big(6q^{1/2}+2q^{1/2}\big)+2q^2 \le \\
&\le 8\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|q\big)^{1/2}+4q^2
\end{aligned}$$

which completes the proof of Theorem 2. □

Proof of Corollary 2. By Theorem 2, it follows from (3.3) that

$$\begin{aligned}
N &\ge \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}-8\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}q^{1/2}-4q^2= \\
&= \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}\left(\frac{\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}}{q}-8q^{1/2}\right)-4q^2> \\
&> \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}(10q^{1/2}-8q^{1/2})-4q^2> \\
&> 10q^{3/2}\cdot 2q^{1/2}-4q^2=16q^2>0
\end{aligned}$$

whence the result follows. □

4 General equations involving sums

Now we will show that Theorem 1 can be generalized considerably at the expense of replacing the upper bound in the inequality by a much weaker one. Besides the proof of Theorem 1 was based on Theorem A which is elementary, while here we will apply Theorem C whose proof uses Weil's deep theorem [7].

Theorem 3. *Assume that q is a prime power, $f(x,y) \in \mathbb{F}_q[x,y]$, $f(x,y)$ is not of the form $g(x)+h(y)$, i.e., (1.5) holds. Define K and D as in Theorem C, and assume that (1.7) also holds. If $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$, and the number of solutions of*

$$a + b = f(c,d), \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{4.1}$$

is denoted by N, then we have

$$\left| N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} \right| \le \Big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| q\big(D + (K-1)q^{1/2}\big) \Big)^{1/2}. \tag{4.2}$$

Corollary 3. *If $q, f(x,y), K$ and D are defined as above, and $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$ satisfy*

$$|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > q^3\big(D + (K-1)q^{1/2}\big), \tag{4.3}$$

then equation (4.1) can be solved.

Note that in the $f(x,y) = xy$ special case we have $D = K = 1$ so that we obtain exactly Theorem 1, resp. Corollary 1 (but there we proved the result elementarily, without using Weil's theorem in the proof). On the other hand, if D, K are fixed and $K > 1$, then the lower bound in Corollary 3 is $\asymp q^{7/2}$ which is worse than the one in Corollary 1 by a factor $q^{1/2}$.

Proof of Theorem 3. We start in the same way as in the proof of Theorem 1 (with $f(c,d)$ in place of cd), and as in (2.3), we obtain that

$$\left| N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} \right| \le \frac{1}{q} \sum_{\psi \neq \psi_0} \left| \sum_{a \in \mathcal{A}} \psi(a) \right| \left| \sum_{b \in \mathcal{B}} \psi(b) \right| \left| \sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{D}} \overline{\psi}\big(f(c,d)\big) \right|.$$

Now we use Theorem C and Cauchy's inequality:

$$\begin{aligned}
&\left| N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} \right| \le \\
&\le \frac{1}{q} \sum_{\psi \neq \psi_0} \left| \sum_{a \in \mathcal{A}} \psi(a) \right| \left| \sum_{b \in \mathcal{B}} \psi(b) \right| \big(|\mathcal{C}|\,|\mathcal{D}| q\big(D + (K-1)q^{1/2}\big) \big)^{1/2} \le \\
&\le \frac{1}{q} \big(|\mathcal{C}|\,|\mathcal{D}| q\big(D + (K-1)q^{1/2}\big) \big)^{1/2} \left(\sum_{\psi} \left| \sum_{a \in \mathcal{A}} \psi(a) \right|^2 \right)^{1/2} \left(\sum_{\psi} \left| \sum_{b \in \mathcal{B}} \psi(b) \right|^2 \right)^{1/2}
\end{aligned}$$

whence, again by identity (2.4),

$$\left|N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| \le \frac{1}{q}\big(|\mathcal{C}|\,|\mathcal{D}|q(D+(k-1)q^{1/2})\big)^{1/2}\big(q|\mathcal{A}|\big)^{1/2}\big(q|\mathcal{B}|\big)^{1/2}$$

which proves (4.2) and this completes the proof of Theorem 3. □

Proof of Corollary 3. By Theorem 3, it follows from (4.3) that

$$N \ge \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q} - \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|q\big(D+(K-1)q^{1/2}\big)^{1/2} =$$

$$= \frac{\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}}{q}\Big(\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2} - q^{3/2}\big(D+(K-1)q^{1/2}\big)^{1/2}\Big) > 0$$

whence the result follows. □

5 General equations involving shifted products

We will prove the multiplicative analog of Theorem 3, i.e., we will generalize Theorem 2 considerably at the expense of giving a weaker estimate and using Theorem D whose proof is based on Weil's theorem.

Theorem 4. *Assume that q is a prime power, $f(x,y) \in \mathbb{F}_q[x,y]$, the primitive kernel $H(x,y)$ of $f(x,y)$ is not of the form $c\big(K(x,y)\big)^d$, i.e.* (1.8) *holds, and in representation* (1.8) *of $f(x,y)$, $F(x)$ is of degree r, $G(x)$ is of degree s, and $f(x,y)$ is of degree n and m in x, resp. y. If $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{F}_q$, and the number of solutions of*

$$ab = f(c,d), \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{5.1}$$

is denoted by N, then we have

$$\left|N - \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right| < \tag{5.2}$$

$$< 4n^{1/2}q^{3/4}\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2} + 7\left(r+s+n+(nm)^{1/2}\right)q^{5/2}.$$

Corollary 4. *If q, $f(x,y)$, n and m are defined as above, and $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{F}_q$ satisfy*

$$|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > 64\big(r+s+n+(nm)^{1/2}\big)q^{7/2}, \tag{5.3}$$

then equation (5.1) *can be solved.*

Note that while Theorem 4 and Corollary 4 are much more general than Theorem 2, resp. Corollary 2, the price paid for this greater generality is that inequality (5.2) in Theorem 4 is weaker and the lower bound in (5.3) in Corollary 4 is greater than in Theorem 2, resp. Corollary 2. Indeed, in the special

case $f(x,y) = xy - 1$ Corollary 4 gives Corollary 2 with a lower bound $\gg q^{7/2}$ for $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|$ which is worse by a factor $q^{1/2}$ than the one in Corollary 2. (Besides the proof of Theorem 2 is elementary, while the proof of Theorem 4 uses Theorem D whose proof is based on Weil's theorem.)

Proof of Theorem 4. As in the proof of Theorem 2 we have

$$N = \frac{1}{q-1}\big(\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| - N_5\big) + N_4\big) + N_2 \tag{5.4}$$

with

$$N_2 = \big|\{(a,b,c,d) : ab = f(c,d) = 0,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}\}\big|,$$

$$N_4 = \sum_{\chi \neq \chi_0} \Big(\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \chi(ab)\Big)\Big(\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}} \overline{\chi}(f(c,d))\Big)$$

and

$$N_5 = \big|\{(a,b,c,d) :\ abf(c,d) = 0,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}\}\big|.$$

First we will estimate N_2. If

$$ab = f(c,d) = 0,$$

then either a or b is 0, and then b, resp. a can be chosen in at most $|\mathcal{B}|$, resp. $|\mathcal{A}|$ ways, so that the pair (a,b) can be chosen in at most $|\mathcal{A}| + |\mathcal{B}|$ ways. If

$$f(c,d) = F(c)G(d)H(c,d) = 0, \tag{5.5}$$

then

$$F(c) = 0, \tag{5.6}$$

$$G(d) = 0 \tag{5.7}$$

or

$$H(c,d) = 0. \tag{5.8}$$

The number of pairs (c,d) satisfying (5.6) or (5.7) is at most $rq + sq$. Moreover, since $H(x,y)$ is primitive in x, thus $H(x,d)$ is never identically 0, so that for every $d \in \mathcal{D}$, c in (5.8) can be chosen in at most n ways. It follows that (5.5) has at most $rq + sq + n|\mathcal{D}|$ solutions so that

$$N_2 \le \big(|\mathcal{A}| + |\mathcal{B}|\big)\big(rq + sq + n|\mathcal{D}|\big) \le 2q(rq + sq + nq) = 2(r+s+n)q^2. \tag{5.9}$$

To estimate N_4 we use Theorem D, Cauchy's inequality and (3.9):

(5.10)

$$|N_4| \le \sum_{\chi\neq\chi_0} \Big|\sum_{a\in\mathcal{A}} \chi(a)\Big| \Big|\sum_{b\in\mathcal{B}} \chi(b)\Big| \big(|\mathcal{C}|\big(2n|\mathcal{D}|q^{3/2} + 5nmq^2\big)\big)^{1/2} \le$$

$$\leq \big(|\mathcal{C}|\big(2n|\mathcal{D}|q^{3/2}+5nmq^2\big)\big)^{1/2}\left(\sum_\chi\Big|\sum_{a\in\mathcal{A}}\chi(a)\Big|^2\right)^{1/2}\left(\sum_\chi\Big|\sum_{b\in\mathcal{B}}\chi(b)\Big|^2\right)^{1/2}<$$

$$<(q-1)\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\big(2n|\mathcal{D}|q^{3/2}+5nmq^2\big)\big)^{1/2}.$$

Finally, if (a,b,c,d) is counted in N_5 then

$$ab=0 \tag{5.11}$$

or

$$f(c,d)=0. \tag{5.12}$$

As the estimate of N_2 shows, the number of the quadruples (a,b,c,d) satisfying (5.11) and (5.12) is at most $\big(|\mathcal{A}|+|\mathcal{B}|\big)|\mathcal{C}|\,|\mathcal{D}|$, resp. $|\mathcal{A}|\,|\mathcal{B}|\big(rq+sq+n|\mathcal{D}|\big)\leq |\mathcal{A}|\,|\mathcal{B}|(r+s+n)q$, so that

$$|N_5|\leq \big(|\mathcal{A}|+|\mathcal{B}|\big)|\mathcal{C}|\,|\mathcal{D}|+|\mathcal{A}|\,|\mathcal{B}|(r+s+n)q. \tag{5.13}$$

It follows from (5.4), (5.9), (5.10) and (5.13) that

$$\left|N-\frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right|\leq$$

$$\leq|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\left|\frac{1}{q-1}-\frac{1}{q}\right|+\frac{1}{q-1}\big(|N_5|+|N_4|\big)+|N_2|<$$

$$<|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\frac{1}{(q-1)q}+\frac{\big(|\mathcal{A}|+|\mathcal{B}|\big)|\mathcal{C}|\,|\mathcal{D}|}{q-1}+\frac{q}{q-1}|\mathcal{A}|\,|\mathcal{B}|(r+s+n)+$$

$$+\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\big(2n|\mathcal{D}|q^{3/2}+5nmq^2\big)\big)^{1/2}+2(r+s+n)q^2$$

whence, by the inequality

$$(a+b)^{1/2}\leq a^{1/2}+b^{1/2}\qquad\text{for}\quad a,b\geq 0,$$

$$\left|N-\frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{q}\right|\leq$$

$$\leq\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}(q^4)^{1/2}\frac{2}{q^2}+\frac{2q^3}{q-1}+2q^2(r+s+n)+$$

$$+\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}(2n)^{1/2}q^{3/4}+\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\big)^{1/2}\cdot 3(nm)^{1/2}q+2(r+s+n)q^2\leq$$

$$\leq\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}\big(2+2n^{1/2}q^{3/4}\big)+q^2\big(4+4(r+s+n)\big)+(q^3)^{1/2}3(nm)^{1/2}q<$$

$$<4n^{1/2}q^{3/4}\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}+\big(4+4(r+s+n)+3(nm)^{1/2}\big)q^{5/2}<$$

$$<4n^{1/2}q^{3/4}\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}+7(r+s+n+(nm)^{1/2}\big)q^{5/2}$$

which completes the proof of Theorem 4. □

Proof of Corollary 4. By Theorem 4, it follows from (5.3) that

$$N > \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}\left(\frac{\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}}{q} - 4n^{1/2}q^{3/4}\right) - \\ - 7\big(r+s+n+(nm)^{1/2}\big)q^{5/2} > \\ > \big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}\cdot\frac{1}{2}\frac{\big(|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|\big)^{1/2}}{q} - 7\big(r+s+n+(nm)^{1/2}\big)q^{5/2} = \\ = \frac{|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|}{2q} - 7\big(r+s+n+(nm)^{1/2}\big)q^{5/2} > \\ > 25\big(r+s+n+(nm)^{1/2}\big)q^{5/2} > 0$$

which proves the result. □

6 "Good" polynomials and their size

Each of Theorems 1–4 can be formulated in the following way: a certain polynomial $f(x_1,x_2,x_3,x_4) \in \mathbb{F}_q[x_1,x_2,x_3,x_4]$ is given, and the conclusion of the theorem is that if $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D} \subset \mathbb{F}_q$ and $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|$ is "large", then the equation

$$f(a,b,c,d) = 0, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$$

can be solved. More generally, we may say that a polynomial $f(x_1,x_2,\dots,x_n) \in \mathbb{F}_q$ is "good" if for all "large" $\mathcal{A}_1,\mathcal{A}_2,\dots,\mathcal{A}_n \subset \mathbb{F}_q$ the equation

$$f(x_1,\dots,x_n) = 0, \quad x_1 \in \mathcal{A}_1,\dots,x_n \in \mathcal{A}_n$$

can be solved; here "large" means that for some *positive* absolute constants c_1, c_2 we have

$$|\mathcal{A}_1|\dots|\mathcal{A}_n| > c_1 q^{n-c_2}.$$

By Theorems 1–4, there are many "good" polynomials with $n = 4$. It is a natural question to ask what is the minimal number n of the variables of "good" polynomials? Trivially, n cannot be 1. We will also show that $n = 2$ is not possible either:

Theorem 5. *Let q be a prime, let $f(x,y) \in \mathbb{F}_q[x,y]$ be of degree u and v in x and y, resp., and assume that*

$$u, v < \frac{q}{2}. \tag{6.1}$$

Then there are $\mathcal{A},\mathcal{B} \subset \mathbb{F}_q$ with

$$|\mathcal{A}| \ge \frac{q}{2}, \qquad |\mathcal{B}| = \left[\frac{q}{2u}\right] \tag{6.2}$$

so that

$$f(a,b) = 0, \quad a \in \mathcal{A},\ b \in \mathcal{B}$$

cannot be solved.

Note that for fixed u, v and $q \to +\infty$, by (6.2) we have

$$|\mathcal{A}|\,|\mathcal{B}| = \left(\frac{1}{4u} + o(1)\right) q^2 \gg q^2.$$

Proof of Theorem 5. Write $f(x,y)$ in form

$$f(x,y) = g_0(y)x^u + g_1(y)x^{u-1} + \cdots + g_u(y) \text{ with } g_0(y), g_1(y), \ldots, g_u(y) \in \mathbb{F}_q[y].$$

Then by the definition of u and v the polynomial $g_0(y)$ is not identically 0 and its degree is at most v, thus it has at most v zeros in $\mathbb{F}_q$, so that writing $\mathcal{R} = \{r :\ r \in \mathbb{F}_q,\ g_0(r) \neq 0\}$, we have

$$|\mathcal{R}| = |\mathbb{F}_q \setminus \{r : r \in \mathbb{F}_q, g_0(r) = 0\}| \geq q - v$$

whence, by (6.1),

$$|\mathcal{R}| > \frac{q}{2}.$$

Now let $\mathcal{B}$ be any subset of $\mathcal{R}$ with

$$|\mathcal{B}| = \left[\frac{q}{2u}\right]. \tag{6.3}$$

For any $b \in \mathcal{B}$ write

$$\mathcal{S}(b) = \{s :\ s \in \mathbb{F}_q,\ f(s,b) = 0\}$$

so that, by $\mathcal{B} \subset \mathcal{R}$ and the definition of $\mathcal{R}$, we have

$$|\mathcal{S}(b)| \leq u \quad \text{for every} \quad b \in \mathcal{B}. \tag{6.4}$$

Define $\mathcal{A}$ by

$$\mathcal{A} = \mathbb{F}_q \setminus \bigcup_{b \in \mathcal{B}} \mathcal{S}(b). \tag{6.5}$$

Then clearly,

$$f(a,b) \neq 0 \quad \text{for} \quad a \in \mathcal{A},\ b \in \mathcal{B},$$

and it follows from (6.3), (6.4) and (6.5) that

$$|\mathcal{A}| \geq q - \sum_{b \in \mathcal{B}} |\mathcal{S}(b)| \geq q - \sum_{b \in \mathcal{B}} u = q - |\mathcal{B}|u = q - \left[\frac{q}{2u}\right] u \geq \frac{q}{2} \tag{6.6}$$

so that, by (6.3) and (6.6), (6.2) also holds and this completes the proof of Theorem 5. □

Thus a "good" polynomial must have at least 3 variables, and it can have 4 variables, but we have not been able to settle the following problem:

Problem 1. Are there "good" polynomials $f(x_1, x_2, x_3) \in \mathbb{F}_q[x_1, x_2, x_3]$ of 3 variables?

7 "Bad" polynomials with many variables

Perhaps, inspired by the discussion in the previous section, one may guess that if $n \in \mathbb{N}$ is large enough then every polynomial $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$ is "good". This is not so and, indeed, we will present two large families of "bad" polynomials with many variables. Note that there will be a close connection between the structure of these polynomials and conditions (1.5) and (1.9).

Theorem 6. *Let $n \in \mathbb{N}$, $n \geq 2$, $d_1, \dots, d_n \in \mathbb{N}$ and $\varepsilon > 0$. Then there is a $p_0 = p_0(n, d_1, \dots, d_n), \varepsilon$ so that if p is a prime with $p > p_0$ and $f_1(x) \in \mathbb{F}_p[x], \dots, f_n(x) \in \mathbb{F}_p[x]$ are polynomials of degree $d_1, \dots, d_n$, resp., then there are subsets $\mathcal{A}_1, \dots, \mathcal{A}_n$ of $\mathbb{F}_p$ so that*

$$|\mathcal{A}_i| > \left(\frac{1}{n} - \varepsilon\right) p \quad \text{for } i = 1, 2, \dots, n, \tag{7.1}$$

and

$$g(a_1, \dots, a_n) \stackrel{\text{def}}{=} f_1(a_1) + \cdots + f_n(a_n) = 0, \quad a_1 \in \mathcal{A}_1, \dots, a_n \in \mathcal{A}_n \tag{7.2}$$

has no solution.

We remark that this theorem could be extended from $\mathbb{F}_p$ to $\mathbb{F}_q$ (with $q = p^r$). However, in the $q = p$ special case there is a result (Lemma 1 below) at hand ready to use from which Theorem 6 can be deduced in a few lines, while in the general case one would need first the extension of Lemma 1 from $\mathbb{F}_p$ to $\mathbb{F}_q$; this can be done (we will return to this at the end of the proof of the theorem) but this would make the proof much longer, thus we present here only the $q = p$ special case.

Moreover, we remark that, e.g., in the special case $f_1(x) = \cdots = f_n(x) = x^k$ the equation

$$f_1(x_1) + \cdots + f_n(x_n) = 0$$

has nontrivial (nonzero) solution for $n > k$ by Chevalley's theorem which together with Theorem 6 shows that the solvability of an algebraic equation in general, resp. in large subsets can be very much different matters.

Proof of Theorem 6. The proof will be based on the following lemma:

Lemma 1. *Assume that p is a prime number, $f(x) \in \mathbb{F}_p[x]$ is of degree $d \geq 1$, let $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $s < p/2$. Define $\mathcal{R} \subset \{1, 2, \dots, p\}$ by*

$$m \in \mathcal{R} \text{ if } \exists\, h \in \{r, r+1, \dots, r+s-1\} \text{ with } f(m) \equiv h \pmod{p}$$

and

$$m \notin \mathcal{R} \text{ otherwise.}$$

Then we have

$$\big||\mathcal{R}| - s\big| < 1 + dp^{1/2}(1 + \log p).$$

Proof of Lemma 1. For $d = 1$ this is trivial (for $(a,p) = 1$, $f(m) = am + b \equiv h \pmod p$ has exactly one solution), while for $d \geq 2$ this is a part (see formula (2.1)) of Theorem 1 in [3] (which was proved there by using Weil's theorem [7]). Note that there $p > p_0$ is also assumed but this is needed only in the proofs of other parts of the theorem.

By using Lemma 1, we may complete the proof of Theorem 6 in the following way (we will identify the elements of $\mathbb{F}_p$ with the modulo p residue classes, and we will not distinguish between the integer a and the modulo p residue class represented by a): Define $\mathcal{A}_i$ by

$$\mathcal{A}_i = \left\{ m : \ 0 \leq m < p, \ \exists\, h \in \left\{ 1, 2, \ldots, \left[\frac{p}{n}\right] \right\} \text{ with } f_i(m) \equiv h \pmod p \right\}.$$

Then for $p > n$ we have

$$0 < f_i(m) \leq \left[\frac{p}{n}\right] < \frac{p}{n} \quad \text{for all } m \in \mathcal{A}_i$$

whence

$$0 < f_1(a_1) + \cdots + f_n(a_n) < n \cdot \frac{p}{n} = p \quad \text{for all } a_1 \in \mathcal{A}_1, \ldots, a_n \in \mathcal{A}_n$$

so that, indeed, (7.2) has no solution. Moreover, by Lemma 1 we have

$$|\mathcal{A}_i| > \left[\frac{p}{n}\right] - \left(1 + d_i p^{1/2}(1 + \log p)\right) > \left(\frac{1}{n} - \varepsilon\right) p$$

for all i and p large enough which proves (7.1) and this completes the proof of Theorem 6. □

To extend Theorem 6 from $\mathbb{F}_p$ to $\mathbb{F}_q$, one would need the generalization of the following type of Lemma 1:

Consider $\mathbb{F}_q$ (as always, $q = p^r$) as a linear vectorspace over $\mathbb{F}_p$. This can be written as the direct sum of its prime field, $\mathbb{F}_p$, and an $r - 1$ dimensional subspace, say $\mathcal{V}$:

$$\mathbb{F}_q = \mathbb{F}_p \oplus \mathcal{V}.$$

Then every $u \in \mathbb{F}_q$ has a unique representation in the form

$$u = w + v \quad \text{with } \ w \in \mathbb{F}_p, \ \ v \in \mathcal{V};$$

denote this w by $w(u)$, v by $v(u)$. Then

Lemma 1'. *Assume that q is a prime power, $f(x) \in \mathbb{F}_q[x]$ is of degree $d \geq 1$, let $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $s < p/2$. Define $\mathcal{R} \subset \mathbb{F}_q$ by*

$$m \in \mathcal{R} \text{ if } \exists\, h \in \{r, r+1, \ldots, r+s-1\} \text{ with } w\big(f(m)\big) \equiv h \pmod p$$

and

$m \notin \mathcal{R}$ *otherwise.*

Then we have

$$\big|\,|\mathcal{R}| - sp^{r-1}\big| = o(p^r)$$

for fixed d *and* $p \to +\infty$.

Such a lemma can be proved by using additive characters of $\mathbb{F}_q$ and Weil's theorem; see [8] for a related result.

Now we will prove the multiplicative analog of Theorem 6 (but this time with $\mathbb{F}_q$ in place of $\mathbb{F}_p$).

Theorem 7. *Let* $n \in \mathbb{N}$, $d_1, \dots, d_n \in \mathbb{N}$ *and* $\varepsilon > 0$. *Then there is a* $q_0 = q_0(n, d_1, \dots, d_n, \varepsilon)$ *so that if* q *is a prime power such that* $q > q_0$ *and* $d_1 \nmid q-1, \dots, d_n \nmid q-1$ *and* $f_1(x) \in \mathbb{F}_q[x], \dots, f_n(x) \in \mathbb{F}_q[x]$ *are polynomials of degree* $d_1, \dots, d_n$, *resp., then there are subsets* $\mathcal{A}_1, \dots, \mathcal{A}_n$ *of* $\mathbb{F}_q$ *so that*

$$|\mathcal{A}_i| > \left(\frac{1}{n} - \varepsilon\right) q \quad \textit{for} \quad i = 1, 2, \dots, n, \tag{7.3}$$

and

$$g(a_1, \dots, a_n) \stackrel{\text{def}}{=\!=} f_1(a_1) \dots f_n(a_n) - 1 = 0, \quad a_1 \in \mathcal{A}_1, \dots, a_n \in \mathcal{A}_n \tag{7.4}$$

has no solution.

Proof of Theorem 7. The proof will be based on the following lemma:

Lemma 2. *Assume that* q *is a prime power,* $f(x) \in \mathbb{F}_q[x]$ *is of degree* $d \geq 1$, *and, if* $d \mid q-1$, *then* $f(x)$ *is not of the form* $f(x) = c\big(g(x)\big)^d$ *with* $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_q[x]$. *Let* $r \in \mathbb{N}$, $s \in \mathbb{N}$, $s \leq (q-1)/2$, *and let* g *be a primitive element of* $\mathbb{F}_q$. *Define* $\mathcal{R} \subset \mathbb{F}_q$ *by*

$$m \in \mathcal{R} \text{ if } \exists\, h \in \{r, r+1, \dots, r+s-1\} \text{ with } f(m) = g^h$$

and

$$m \notin \mathcal{R} \text{ otherwise.}$$

Then we have

$$\big|\,|\mathcal{R}| - s\big| < 3dq^{1/2}(1 + \log q).$$

Proof of Lemma 2. We have

$$\frac{1}{q-1} \sum_{\chi} \chi\big(f(m)\big)\overline{\chi}(g^h) = \begin{cases} 1 & \text{if } f(m) = g^h \\ 0 & \text{otherwise} \end{cases}$$

(where $\sum_{\chi}$ denotes summation over the multiplicative characters of $\mathbb{F}_q$) so that

$$|\mathcal{R}| = \sum_{m \in \mathbb{F}_q} \sum_{h=r}^{r+s-1} \frac{1}{q-1} \sum_{\chi} \chi\big(f(m)\big)\overline{\chi}(g^h) =$$

$$= \frac{1}{q-1} \sum_{\chi} \sum_{m \in \mathbb{F}_q} \chi(f(m)) \sum_{h=r}^{r+s-1} (\overline{\chi}(g))^h$$

whence, separating the contribution of the trivial character,

(7.5)

$$\begin{aligned} \big||\mathcal{R}| - s\big| &= \left| \left(\frac{1}{q-1} \sum_{m \in \mathbb{F}_q} \chi_0(f(m)) \sum_{h=r}^{r+s-1} (\chi_0(g))^h - s \right) + \right. \\ &\quad \left. + \frac{1}{q-1} \sum_{\chi \neq \chi_0} \sum_{m \in \mathbb{F}_q} \chi(f(m)) \sum_{h=r}^{r+s-1} (\overline{\chi}(g))^h \right| \leq \\ &\leq \left| \frac{1}{q-1} \Big(\sum_{\substack{m \in \mathbb{F}_q \\ f(m) \neq 0}} 1 \Big) s - s \right| + \frac{1}{q-1} \sum_{\chi \neq \chi_0} \left| \sum_{m \in \mathbb{F}_q} \chi(f(m)) \right| \left| \sum_{h=r}^{r+s-1} (\chi(g))^h \right|. \end{aligned}$$

Now we use the following form of Weil's theorem [7]:

Lemma 3. *Suppose χ is a multiplicative character of order $D > 1$ of $\mathbb{F}_q$. Suppose $f(x) \in \mathbb{F}_q[x]$ has t distinct zeros over the algebraic closure of $\mathbb{F}_q$, and it is not the constant multiple of the D-th power of a polynomial over $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (t-1) q^{1/2}.$$

Using Lemma 2 (which can be used for every $\chi \neq \chi_0$ by our assumptions on $f(x)$) and the fact that if g is a primitive element of $\mathbb{F}_q$ and χ runs over the nontrivial characters of $\mathbb{F}_q$, then $\chi(g)$ runs over the $q-1$-st roots of unity, we obtain from (7.5) that

$$\begin{aligned} \big||\mathcal{R}| - s\big| &\leq \left| \frac{1}{q-1} \Big(q - \sum_{\substack{m \in \mathbb{F}_q \\ f(m)=0}} 1 \Big) s - s \right| + \\ &\quad + \frac{1}{q-1} \sum_{\chi \neq \chi_0} (d-1) q^{1/2} \frac{|1 - (\chi(g))^s|}{|1 - \chi(g)|} \leq \\ &\leq \frac{s}{q-1} + \frac{s}{q-1} \sum_{\substack{m \in \mathbb{F}_q \\ f(m)=0}} 1 + \frac{1}{q-1} (d-1) q^{1/2} \sum_{\chi \neq \chi_0} \frac{2}{|1 - \chi(g)|} \leq \\ &\leq \frac{s}{q-1} (d+1) + \frac{2}{q-1} (d-1) q^{1/2} \sum_{j=1}^{q-2} \frac{1}{|1 - e(j/(q-1))|} \end{aligned}$$

whence, by the inequality

$$|1 - e(\alpha)| \geq 4 \|\alpha\|$$

(where $\|\alpha\|$ denotes the distance of α from the nearest integer),

$$\big|\,|\mathcal{R}| - s\big| \le \frac{q/2}{q/2}(d+1) + \frac{2}{q-1}dq^{1/2}\cdot 2\sum_{j=1}^{\left[\frac{q-1}{2}\right]}\frac{1}{4j/(q-1)} \le$$
$$\le d\big(2 + q^{1/2}(1+\log q)\big) < 3dq^{1/2}(1+\log q)$$

which completes the proof of Lemma 2.

By using Lemma 2, the proof of Theorem 7 can be completed in the following way: Define $\mathcal{A}_i$ by

$$\mathcal{A}_i = \left\{m:\ m\in\mathbb{F}_q,\ \exists\, h\in\left\{1,2,\dots,\left[\frac{q-1}{n}\right]-1\right\}\ \text{with}\ f_i(m)=g^h\right\}.$$

Then for $a_1\in\mathcal{A}_1,\dots,a_n\in\mathcal{A}_n$ there exist $h_1,\dots,h_n\in\{1,2,\dots,[\frac{q-1}{n}]-1\}$ with $f_i(a_i)=g^{h_i}$ for $i=1,\dots,n$. Then we have

$$f_1(a_1)\dots f_n(a_n) = g^{h_1}\dots g^{h_n} = g^{h_1+\dots+h_n}$$

with

$$0 < h_1+\dots+h_n \le n\left(\left[\frac{q-1}{n}\right]-1\right) < n\cdot\frac{q-1}{n} = q-1$$

whence

$$f_1(a_1)\dots f_n(a_n) = g^{h_1+\dots+h_n} \ne g^0 = 1$$

which proves that, indeed, (7.4) has no solution. Moreover, by Lemma 2 we have

$$|\mathcal{A}_i| > \left(\left[\frac{q-1}{n}\right]-1\right) - 3d_iq^{1/2}(1+\log q) > \left(\frac{1}{n}-\varepsilon\right)q$$

for all i and q large enough which proves (7.3) and this completes the proof of Theorem 7. □

(We remark that in [5] two further examples were given for "bad" polynomials of $n=4$ variables.)

8 Unsolved problems

At the end of Section 6 we mentioned an unsolved problem (one of the most important ones that we have not been able to settle). In this section we will present some further open problems.

Problem 2. Find elementary-algebraic proofs for Theorems 1 and 2. Proofs of this type might help to understand these results better and to extend them in various directions.

Problem 3. In what other rings are the analogs of Theorems 1 and 2 true? (It was pointed out in [4] that the analog of Theorem 1 is not true in $\mathbb{Z}_m$ if m is composite, and it is easy to see that the analog of Theorem 2 is not true either in this case.)

Problem 4. Are there any infinite fields where theorems of similar flavour can be proved?

Problem 5. If $\mathcal{A} = \mathcal{B} = \mathcal{C} = \mathcal{D} = \{n : \ n \in \mathbb{N}, \ n \text{ is odd}\}$, then equations (1.1) and (1.2) are not solvable with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$. This shows that it is not enough to take large subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{N}$ to guarantee the solvability of (1.1), resp. (1.2) with elements belonging to the given sets. Does it help to consider k-colorings of $\mathbb{N}$ instead of large subsets of it? More exactly, does there exist a $k \in \mathbb{N}$ so that for any k-coloring of $\mathbb{N}$, (1.1) (to avoid trivialities, one should add the restriction $a \neq b$), resp. $ab + 8 = cd$ (modulo 8 discussion shows that 1 in (1.2) must be replaced by, say, 8) has a monochromatic solution? If yes, then what is the greatest k with this property? If the answer is negative, then what weaker statements can be proved on the coloring of the solutions of (1.1) and (1.2)?

Problem 6. Does it help if we have a lower bound for $\min\{|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}|\}$ instead of $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|$ when studying the solvability of (1.1), resp. (1.2)? More precisely, does there exist a $\delta > 0$ so that if $q > q_0$, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$ and $\min\{|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}|\} > q^{\frac{3}{4}-\delta}$, then (1.1), resp. (1.2) can be solved with a, b, c, d belonging to the given subsets?

Problem 7. Can one extend and sharpen Theorem 1 in the following way: for every $k \in \mathbb{N}$ there are $c = c(k) > 0$ and $q_0 = q_0(k)$ so that if $q > q_0$, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$, $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > q^{4-c}$ then there are $a_1, \dots, a_k \in \mathcal{A}$, $b_1, \dots, b_k \in \mathcal{B}$ with $a_i + b_j \in \mathcal{CD}$ (for $1 \leq i, j \leq k$)?

Problem 8. Can one extend and sharpen Theorem 2 in the following way: for every $k \in \mathbb{N}$ there are $c = c(k) > 0$ and $q_0 = q_0(k)$ so that if $q > q_0$, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$, $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > q^{4-c}$, then there are $a_1, \dots, a_k \in \mathcal{A}$, $b_1, \dots, b_k \in \mathcal{B}$ with $a_i b_j + 1 \in \mathcal{CD}$ (for $1 \leq i, j \leq k$)?

Problem 9. How large can a subset $\mathcal{A} \subset \mathbb{F}_p$ be so that there is no arithmetic progression of 3 terms in $\mathcal{A} \cdot \mathcal{A}$ $(= \{aa' : \ a \in \mathcal{A}, \ a' \in \mathcal{A}\})$?

Acknowledgement. We would like to thank the referee, Antal Balog for his valuable remarks.

References

[1] K. Gyarmati, On a problem of Diophantus, *Acta Arith.* **97** (2001), 53–65.

[2] K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets, I. (Character sums), *Acta Math. Hungar.*, submitted.

[3] C. Dartyge, E. Mosaki and A. Sárközy, On large families of subsets of the integers not exceeding N with strong pseudo-random properties, submitted.

[4] A. Sárközy, On sums and products of residues modulo p, *Acta Arith.* **118** (2005), 403–409.

[5] A. Sárközy, On products and shifted products of residues modulo p, *Integers:* EJCNT, to appear.

[6] I. Schur, Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, *Jahresber. Deutschen Math. Verein.* **25** (1916), 114–117.

[7] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, *Publ. Inst. Math. Univ. Strasbourg* **7** (1945), Hermann, Paris, 1948.

[8] A. Winterhof, Some estimates for character sums and applications, *Des. Codes Cryptogr.* **22** (2001), 123–131.