Finite Fields and Their Applications 51 (2018) 93–129

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Trace of products in finite fields

Cathy Swaenepoel

Aix Marseille Université, CNRS, Centrale Marseille, I2M, Marseille, France
Institut de Mathématiques de Marseille UMR 7373 CNRS, 163 Avenue de Luminy, Case 907, 13288 Marseille cedex 9, France

ARTICLE INFO

Article history:
Received 14 April 2017
Received in revised form 16 January 2018
Accepted 18 January 2018
Available online xxxx
Communicated by Igor Shparlinski

MSC:
11T30
11T23
11A63

Keywords:
Finite fields
Trace function
Direct product of subsets
Character sums
Squares
Generators

ABSTRACT

Let p be a prime number and let $q = p^r$. If $\mathcal{C}$ and $\mathcal{D}$ are large subsets of $\mathbb{F}_q^*$ we study the trace of products cd with $c \in \mathcal{C}$ and $d \in \mathcal{D}$ and show that it is well distributed in $\mathbb{F}_p$. We give an optimal condition (up to an absolute constant factor) on the size of the subsets $\mathcal{C}$ and $\mathcal{D}$ to ensure that the trace of products cd takes any given value in $\mathbb{F}_p$. We also give a condition (optimal up to an absolute constant factor in most cases) on the size of the subsets $\mathcal{C}$ and $\mathcal{D}$ to ensure that the trace of cd meets the set of k-th powers for $k \geq 1$, respectively the set of generators. Our method will enable us to take sets $\mathcal{C}$ and $\mathcal{D}$ whose size is substantially below $\sqrt{q}$. Character sums and Gaussian sums over $\mathbb{F}_p$ and $\mathbb{F}_q$ will play an important role in the proofs. Some estimates lead to interesting combinatorial questions in finite fields.

E-mail address: cathy.swaenepoel@univ-amu.fr.

https://doi.org/10.1016/j.ffa.2018.01.005
1071-5797/

1. Introduction

1.1. Motivation

The study of the connection between the arithmetic properties of an integer and the properties of its digits in a given basis produces a lot of interesting questions and a lot of papers have been devoted to this topic. In particular, Gelfond [6] proved an asymptotic formula for the number of integers of an arithmetic progression whose sum of digits modulo m is fixed. More recently, Mauduit and Rivat [10,11] obtained an asymptotic formula for the number of prime numbers and also for the number of squares whose sum of digits modulo m is fixed. In another direction, Maynard [12] showed in a recent work that there are infinitely many prime numbers with one missing digit (e.g. no digit 9) in their decimal expansion.

In the context of finite fields, the algebraic structure permits to formulate and study new problems of interest which might be out of reach in the context of natural integers [9,13]. In [3], Dartyge and Sárközy initiated the study of the concept of digits in the context of finite fields. Let p be a prime number, let $q = p^r$ with $r \geq 2$ and consider the finite field $\mathbb{F}_q$. If $\mathcal{B} = \{e_1, \ldots, e_r\}$ is a basis of $\mathbb{F}_q$ viewed as a $\mathbb{F}_p$-vector space then every $x \in \mathbb{F}_q$ can be written uniquely in base $\mathcal{B}$:

$$x = \sum_{j=1}^{r} c_j e_j \tag{1}$$

with $c_1, \ldots, c_r \in \mathbb{F}_p$. In [3], $c_1, \ldots, c_r$ are called the "digits" of x and the function $s_{\mathcal{B}}$ defined on $\mathbb{F}_q$ by

$$s_{\mathcal{B}}(x) = \sum_{j=1}^{r} c_j \tag{2}$$

is called the "sum of digits" function. Dartyge and Sárközy estimated the number of squares in $\mathbb{F}_q$ whose sum of digits is fixed and also obtained results for polynomial values, resp. polynomial values with generator arguments whose sum of digits is fixed. Further problems on digits in finite fields have been studied by Dartyge, Mauduit, Sárközy [2], Dietmann, Elsholtz, Shparlinski [4] and Gabdullin [5]. In particular, an estimate of the number of squares in $\mathbb{F}_q$ with restricted digits has been proved in [2] and then improved in [4] and [5].

In [14], Rivat and Sárközy provided a "possibly complete" list of the papers written on arithmetic properties of products and showed that if $\mathcal{C}$ and $\mathcal{D}$ are large subsets of $\{1, \ldots, N\}$ then the sum of digits of the products cd with $c \in \mathcal{C}$ and $d \in \mathcal{D}$ is well distributed modulo m. We will study a local analog of this result in the context of finite fields. Instead of the sum of digits function $s_{\mathcal{B}}$, we will consider the trace function Tr from $\mathbb{F}_q$ to $\mathbb{F}_p$ which is of basic importance in finite fields (see [9,13]) and can be used