Finite Fields and Their Applications 23 (2013) 1–7

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Planarity of mappings $x(\mathrm{Tr}(x) - \frac{\alpha}{2}x)$ on finite fields

Minghui Yang [a,*], Shixin Zhu [a], Keqin Feng [b]

[a] School of Mathematics, Hefei University of Technology, Hefei 230009, PR China
[b] Department of Mathematical Sciences, Tsinghua University, Beijing 100084, PR China

ARTICLE INFO

Article history:
Received 16 October 2012
Revised 23 January 2013
Accepted 3 April 2013
Available online 17 April 2013
Communicated by Gary McGuire

MSC:
12E10
11G20
14G50

Keywords:
Planar mapping
Perfect nonlinear
Trace mapping
Finite field
Kloosterman sum

ABSTRACT

Let q be a power of an odd prime, $n \geqslant 3$ and $\mathrm{Tr}_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be the trace mapping. A mapping $f = f(x) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is called planar (or perfect nonlinear) on $\mathbb{F}_{q^n}$ if for any non-zero $a \in \mathbb{F}_{q^n}$, the difference mapping $D_{f,a} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a permutation where for $x \in \mathbb{F}_{q^n}$, $D_{f,a}(x) = f(x+a) - f(x)$. Kyureghyan and Özbudak (2012) [8] considered the planarity of mappings $f_{n,\alpha}(x) = x(\mathrm{Tr}_n(x) - \frac{\alpha}{2}x)$ on $\mathbb{F}_{q^n}$ for $\alpha \in \mathbb{F}_{q^n}$ and proved that there is no planar $f_{n,\alpha}$ for $n \geqslant 5$. For the case $n = 3$ and $n = 4$, they raised three conjectures. In this paper we prove the third conjecture which says that there is no planar $f_{n,\alpha}$ for $n = 4$, by using Kloosterman sums. Our proof also works for case $n \geqslant 5$, so we present a new proof of the Kyureghyan–Özbudak result. For case $n = 3$, we present an elementary proof of the first conjecture which says that there is no planar $f_{3,\alpha}$ for $\alpha \in \mathbb{F}_q \backslash \{2, 4\}$.

1. Introduction

Let q be a power of an odd prime, $n \geqslant 1$, $\mathbb{F}_{q^n}$ be the finite field with q^n elements and $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \backslash \{0\}$. A mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is called planar (or perfect nonlinear) if for each $a \in \mathbb{F}_{q^n}^*$, the difference function $D_{f,a} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $D_{f,a}(x) = f(x+a) - f(x)$ is a permutation on $\mathbb{F}_{q^n}$. Planar mappings were introduced in [3] as a tool to construct projective planes. In cryptology, such mappings provide optimal resistance to differential attacks [10]. They are also used to construct optimal constant-composition codes [5], signal sets with good correlation properties [4] and finite semifields [1].

* Corresponding author.
E-mail addresses: yangminghui6688@163.com (M. Yang), zhushixin@hfut.edu.cn (S. Zhu), kfeng@math.tsinghua.edu.cn (K. Feng).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.04.001

In the past twenty years, many papers have been devoted to existence and non-existence results for planar mappings. Many planar mappings have been constructed by a variety of methods, see [2,6–8] and the references therein.

Recently, Kyureghyan and Özbudak [8] investigated the planarity of products of two linearized polynomials. Particularly, they paid much attention to the planarity of mappings

$$f = f_{n,\alpha} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \qquad f_{n,\alpha} = x\left(\mathrm{Tr}_n(x) - \frac{\alpha}{2}x\right)$$

where $\alpha \in \mathbb{F}_{q^n}^*$ and $\mathrm{Tr}_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is the trace mapping. For $n = 1$, all quadratic mappings $f(x) = (1 - \frac{\alpha}{2})x^2$ $(\alpha \neq 0)$ are planar. For $n = 2$, the problem is also solved completely (see [8, Theorem 2]). On the other hand, it is proved in [8] that there is no planar mapping $f_{n,\alpha}(x)$ when $n \geqslant 5$ [8, Theorem 4]. When $n = 3$, $f_{3,\alpha}(x)$ is planar for $\alpha \in \{2, 4\}$ and is not planar for $\alpha \in \{0, 3, 6\}$ [8, Theorems 6 and 7]. Based on computer experiments, the following conjecture has been raised in [8]:

Conjecture. *Let q be a power of an odd prime.*

1. *There is no planar mapping $f_{3,\alpha}(x)$ on $\mathbb{F}_{q^3}$ for $\alpha \in \mathbb{F}_q \backslash \{0, 2, 3, 4, 6\}$.*
2. *There is no planar mapping $f_{3,\alpha}(x)$ on $\mathbb{F}_{q^3}$ for $\alpha \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$.*
3. *There is no planar mapping $f_{4,\alpha}(x)$ on $\mathbb{F}_{q^4}$ for $\alpha \in \mathbb{F}_{q^4}$.*

As named in [8], we will refer to these three subconjectures 1, 2 and 3 as Conjecture 1, Conjecture 2 and Conjecture 3.

These three conjectures have been checked to be true in [8] for $q \leqslant 997, 29$ and 11 respectively.

In this paper we prove Conjecture 3 by using Kloosterman sums in Section 2. Our proof works also for case $n \geqslant 5$, so we present a new proof of the result for $n \geqslant 5$ [8, Theorem 4]. In Section 3 we present an elementary proof of Conjecture 1.

As the starting point for this paper, we now introduce a result from [8] which gives criterion on the planarity of the mapping $f_{n,\alpha}$.

Lemma 1. *(See [8, Theorem 3].) Let q be a power of an odd prime, $n \geqslant 2$, $\alpha \in \mathbb{F}_{q^n}$ and $\mathrm{Tr}_n : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be the trace mapping. Then the mapping*

$$f_{n,\alpha} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \qquad f_{n,\alpha}(x) = x\left(\mathrm{Tr}_n(x) - \frac{\alpha}{2}x\right)$$

is planar on $\mathbb{F}_{q^n}$ if and only if the following three conditions are satisfied:

(i) $\alpha \neq 0$.
(ii) $\mathrm{Tr}_n(\frac{1}{\alpha}) \neq 1, \frac{1}{2}$.
(iii) *There is no $z \in \mathbb{F}_{q^n} \backslash \{0, -\frac{\alpha}{2}, -\alpha\}$ such that $\mathrm{Tr}_n(\frac{1}{z}) = -1$ and $\mathrm{Tr}_n(\frac{1}{z+\alpha}) = 1$.*

We end this section by stating several basic facts concerning Kloosterman sums which will be needed in Section 2, see [9].

We denote the group of additive characters on $\mathbb{F}_q$ by $\hat{\mathbb{F}}_q$. Let $q = p^m$, where p is a prime and $m \geqslant 1$. The group $\hat{\mathbb{F}}_q$ can be described as

$$\hat{\mathbb{F}}_q = \{\lambda_b : b \in \mathbb{F}_q\}$$

where, for $x \in \mathbb{F}_q$, $\lambda_b(x) = \zeta_p^{T_p^q(bx)}$, $T_p^q : \mathbb{F}_q \to \mathbb{F}_p$ is the trace mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$.