J. Algebra Comb. Discrete Appl.
11(3) • 175–187

Received: 6 March 2023
Accepted: 26 November 2023

Journal of Algebra Combinatorics Discrete Structures and Applications

Determining Sidon polynomials on Sidon sets over finite fields*

Research Article

Muhammad Afifurrahman, Aleams Barra

Abstract: Let p be a prime, and $q = p^n$ be a prime power. In his works on Sidon sets over $\mathbb{F}_q \times \mathbb{F}_q$, Cilleruelo conjectured about polynomials that could generate q-element Sidon sets over $\mathbb{F}_q \times \mathbb{F}_q$. In this paper, we derive some criteria for determining polynomials that could generate q-element Sidon set over $\mathbb{F}_q \times \mathbb{F}_q$. Using these criteria, we prove that certain classes of monomials and cubic polynomials over $\mathbb{F}_p$ cannot be used to generate p-element Sidon set over $\mathbb{F}_p \times \mathbb{F}_p$. We also discover a connection between this class of polynomials and the class of planar polynomials.

2020 MSC: 11T06, 11B83, 05A20

Keywords: Sidon sets, Planar polynomial, Finite fields

1. Introduction

Sometimes we use some objects to satisfy some other means, but we do not know whether any other similar object exists.

1.1. Background

Let G be an abelian group, written additively. A subset $\mathcal{A} \subseteq G$ is a *Sidon set* if, for any $a_1, a_2, a_3, a_4 \in \mathcal{A}$ that satisfy $a_1 - a_2 = a_3 - a_4$, $\{a_1, a_4\} = \{a_2, a_3\}$.

Sidon sets have been studied extensively since the 1940s, and have appeared on subjects such as finite geometry, graph theory, and coding theory, to mention some instances.

* *This work was supported by PPMI ITB 2021.*
Muhammad Afifurrahman (Corresponding Author); School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia (email: m.afifurrahman@unsw.edu.au).
Muhammad Afifurrahman, Aleams Barra; Algebra Research Group, Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Indonesia (email: aleamsbarra@itb.ac.id).

In this paper, we focus on Sidon sets over the group $(\mathbb{F}_q \times \mathbb{F}_q, +)$, with $\mathbb{F}_q$ being a finite field with q being a power of a prime p. A precursor of the set first appeared in [11], by considering that the map $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ given as $(k, k^2) \to (2pk + (k^2 \pmod p))$ with $1 \leq k \leq p$ and $\mathbb{N} \times \mathbb{N} \to \mathbb{F}_p \times \mathbb{F}_p$ given as $(k, k^2) \to (k, k^2)$ both gives a Sidon set over the respective groups. The Sidon set over this group is resurgent in 2010s, with applications in additive number theory [5, 6] and extremal graph theory [1, 9, 16, 17].

It turns out that the Sidon sets over this group can be parametrized by two polynomials in $\mathbb{F}_q[x]$. We aim to give some criteria of polynomials that can (or cannot) parametrize a Sidon set over $(\mathbb{F}_q \times \mathbb{F}_q, +)$, and derive some results regarding the parametrization from them.

1.2. Maximum Sidon sets

Consider a Sidon set $\mathcal{A}$ over $(\mathbb{F}_q \times \mathbb{F}_q, +)$. We first notice that when $\mathbb{F}_q$ is of characteristic 2, there do not exist non-trivial Sidon sets over $(\mathbb{F}_q \times \mathbb{F}_q, +)$ based on our definition. This is true since $(a, b) - (c, d) = (c, d) - (a, b)$ for all $(a, b), (c, d) \in \mathbb{F}_q \times \mathbb{F}_q$. However, if we use another definition of Sidon sets, that is, there are no elements $a_1, a_2, a_3, a_4 \in \mathcal{A}$ with at least three of them different that satisfy $a_1 - a_2 = a_3 - a_4$, then some non-trivial Sidon sets over the set $(\mathbb{F}_q \times \mathbb{F}_q, +)$ may exist. In particular, this family of Sidon sets may be used to construct almost perfect nonlinear functions, see [4, Section 11.3]

We may now assume that $\mathrm{char}(\mathbb{F}_q) > 2$ in this paper. By a counting argument based on the set $\{a - a', a, a' \in \mathcal{A}\}$, we have that $|\mathcal{A}| \leq q$. If equality occurs, we say that $\mathcal{A}$ is a *maximum* Sidon set over $\mathbb{F}_q \times \mathbb{F}_q$.

Now, let $\mathbb{F}_q = \{x_1, x_2, \ldots, x_q\}$ be an indexing of $\mathbb{F}_q$. By Lagrange interpolation Theorem, for any q-element multiset

$$X = \{\{(a_1, b_1), (a_2, b_2), \ldots, (a_q, b_q)\}\} \subseteq \mathbb{F}_q \times \mathbb{F}_q,$$

one can always find $P, Q \in \mathbb{F}_q[x]$ with $\deg P, \deg Q \leq q-1$ such that $(P(x_i), Q(x_i)) = (a_i, b_i)$ for $1 \leq i \leq q$. We note that this representation of X is not unique.

By this observation, we see that any maximum Sidon sets over $\mathbb{F}_q \times \mathbb{F}_q$ can be written in the form

$$(P, Q) := \{(P(x), Q(x)) : x \in \mathbb{F}_q\}$$

where $P, Q \in \mathbb{F}_q[x]$. Furthermore, we can assume that all polynomials are taken modulo $x^q - x$. Hence, we assume $\deg P, \deg Q \leq q - 1$ from now on.

We now restate a family of maximum Sidon sets constructed by Cilleruelo.

Lemma 1.1. *[5] Let $P, Q \in \mathbb{F}_q[x]$ be non-constant polynomials with degree not more than two, such that for any $k \in \mathbb{F}_q$, $P - kQ$ is not constant. Then, (P, Q) is a maximum Sidon set over $\mathbb{F}_q \times \mathbb{F}_q$. In particular, (x, x^2) is a maximum Sidon set.*

It is conjectured in [3] that when $q = p$, these families are the only possible maximum Sidon sets over $\mathbb{F}_p \times \mathbb{F}_p$. The precise statement is as follows.

Conjecture 1.2. *[3] Let p be prime, and A be a maximum Sidon set over $\mathbb{F}_p \times \mathbb{F}_p$. Then, there exists $P, Q \in \mathbb{F}_p[x]$ with $1 \leq \deg(P), \deg(Q) \leq 2$ and $A = (P, Q)$.*

The only progress known to the authors regarding this conjecture is over subsets of the form (x, Q) over $\mathbb{F}_p \times \mathbb{F}_p$, which is stated without proof (albeit with typographical errors) in [3].

Lemma 1.3. *[3] If (x, Q) is a maximum Sidon set over $\mathbb{F}_p \times \mathbb{F}_p$, then Q is quadratic.*

We later see that the proof of this statement is immediate from Theorem 2.8. On the other hand, for the case $q \neq p$, a maximum Sidon set other than the family in Lemma 1.1 may exist. This can be seen from Theorem 2.8. However, it is also not known whether any other maximum Sidon set exists outside of these families.

2. Sidon polynomials

2.1. Definition of Sidon polynomials

In this paper, we consider a related question to Conjecture 1.2. First, we define a class of related polynomials as follows:

Definition 2.1. *A polynomial $P \in \mathbb{F}_q[x]$ is Sidon over $\mathbb{F}_q \times \mathbb{F}_q$ if there exists $Q \in \mathbb{F}_q[x]$ such that (P, Q) is a maximum Sidon set.*

From Cilleruelo's construction in Lemma 1.1, and considering that if (P, Q) is a (maximum) Sidon set, $(P, Q + aP)$ is also Sidon, we see that all linear and quadratic polynomials are Sidon polynomials over $\mathbb{F}_q \times \mathbb{F}_q$.

By using this definition, we are able to derive the equivalent form of Conjecture 1.2 in terms of Sidon polynomials. However, in order to do this, we first need an observation on the polynomials over $\mathbb{F}_q$, and a new definition that is related to them.

Let (P, Q) be a Sidon set over $\mathbb{F}_q \times \mathbb{F}_q$ and $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ be a bijection. It is easy to see that $(P \circ \sigma, Q \circ \sigma)$ and $(\sigma \circ P, \sigma \circ Q)$ are Sidon sets as well.

We note that for any bijective map $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ there exist a polynomial $R \in \mathbb{F}_q[x]$ such that $\sigma(r) = R(r)$ for any $r \in \mathbb{F}_q$. Based on this, we define a polynomial $R \in \mathbb{F}_q[x]$ as a *permutation polynomial* if R is a bijection over $\mathbb{F}_q$. From the observation in the preceding paragraph, we are motivated to define the following equivalence.

Definition 2.2. *Let $P, P' \in \mathbb{F}_q[x]$. The polynomials P and P' are permutation-equivalent over $\mathbb{F}_q[x]$, denoted by $P \sim P'$, if $P' = R \circ P \circ T$, for some permutation polynomials $R, T \in \mathbb{F}_q[x]$. When the context is clear, we may only say an equivalence when referring to a permutation equivalence over $\mathbb{F}_q[x]$.*

The following result is immediate from the observation and the definition of $\sim$.

Theorem 2.3. *The relation $\sim$ is an equivalence relation. Moreover, if $P \sim P'$ and P is a Sidon polynomial, then P' is also a Sidon polynomial.*

We now define two functions over $\mathbb{F}_q[x]$ that act as invariants under relation $\sim$. Both functions are related to the roots of the polynomial $P(x) - \gamma$ in $\mathbb{F}_q$.

Definition 2.4. *For $P \in \mathbb{F}_q[x]$ and nonnegative integer n, define $f(P, n)$ as the number of $\gamma \in \mathbb{F}_q$ such that the polynomial $P(x) - \gamma$ has a root in $\mathbb{F}_q$ with multiplicity at least n. Also, define $g(P, n)$ as the number of $\gamma \in \mathbb{F}_q$ such that the polynomial $P(x) - \gamma$ has exactly n distinct roots in $\mathbb{F}_q$.*

As stated before, these two functions are invariants over $\mathbb{F}_q[x]$ with respect to $\sim$. The proof of this statement is given in Section 5.

Theorem 2.5. *Let n be a positive integer and $P, P' \in \mathbb{F}_q[x]$ such that $P \sim P'$. Then, $f(P, n) = f(P', n)$ and $g(P, n) = g(P', n)$*

As the first application of these invariants, we first classify the equivalencies of linear and quadratic polynomials in $\mathbb{F}_q[x]$ over $\sim$.

Corollary 2.6. *Let $a_1, b_1, a_2, b_2, c \in \mathbb{F}_q$ with $a_1,\ a_2 \neq 0$ and $\mathrm{char}(\mathbb{F}_q) > 2$. Then,*

$$a_1 x + b_1 \sim x$$

and

$$a_2 x^2 + b_2 x + c \sim x^2.$$

However,

$$x \not\sim x^2.$$

Proof. The proofs of the first two statements are considered straightforward, hence we only provide the proof of the last statement. To do this, we observe that $g(x, 2) = 0$. However, because the equation $x^2 = 1$ has two solutions in $\mathbb{F}_q$, we have $g(x^2, 2) > 0$. We conclude the proof by applying Theorem 2.5. □

Using these notations and results that we have introduced, we can now restate Conjecture 1.2 in terms of $\sim$.

Conjecture 2.7. *Let p be a prime, and $P \in \mathbb{F}_p[x]$ be a Sidon polynomial. Then, either $P \sim x$ or $P \sim x^2$.*

We end this section with noting that the last conjecture may be proven by brute force for $p \leq 5$.

2.2. Connection with planar polynomials

A polynomial $P \in \mathbb{F}_q$ is *planar* if, for any nonzero $a \in \mathbb{F}_q$, the polynomial $P(x + a) - P(x)$ is a permutation polynomial. This polynomial family was first introduced by Dembowski and Ostrom in [10], with applications in finite geometry.

If $q = p$, it is known that the only planar polynomials are quadratic polynomials [12, 13, 15]. This fact may be used to give a short proof of Lemma 1.3, which goes as follows. Suppose that $A = (x, Q)$ is a maximum Sidon set over $\mathbb{F}_p \times \mathbb{F}_p$. Let k be a fixed nonzero element of $\mathbb{F}_p$. Consider the elements

$$(x + k, Q(x + k)) - (x, Q(x)) = (k, Q(x + k) - Q(x)) \in A - A$$

for all $x \in \mathbb{F}_p$. Since A is a Sidon set, by considering the above equality, we have that

$$Q(x + k) - Q(x) = Q(y + k) - Q(y) \iff x = y.$$

Therefore, the polynomial $Q_k(x) := Q(x+k)-Q(x)$ is a permutation polynomial in $\mathbb{F}_p$, for each nonzero $k \in \mathbb{F}_p$. This implies that Q itself is a planar polynomial over $\mathbb{F}_p$, which implies that Q itself is quadratic.

However, if q is not prime, another family of planar polynomials can be constructed [2, 7, 8]. We now state a connection between Sidon polynomials and planar polynomials.

Theorem 2.8. *Any planar polynomial is a Sidon polynomial.*

Proof. Let $P \in \mathbb{F}_q[x]$ be planar. We now prove that the set (x, P) is a Sidon set. Now let x_1, x_2, x_3, x_4 satisfy the equation

$$(x_1 - x_2, P(x_1) - P(x_2)) = (x_3 - x_4, P(x_3) - P(x_4)).$$

Suppose $x_1 \neq x_2$ (and $x_3 \neq x_4$). By letting $x_1 - x_2 = x_3 - x_4 = a$, we see that $P(x_2 + a) - P(x_2) = P(x_4 + a) - P(x_4)$. However, since P is planar, this implies $x_2 = x_4$, and $x_1 = x_3$. This proves the initial assertion. □

To end this section, we note that x is a Sidon polynomial over $\mathbb{F}_q \times \mathbb{F}_q$ for any q, however it is not a planar polynomial.

3. Criteria of Sidon polynomials

In this section, we prove some criteria for determining whether a polynomial in $\mathbb{F}_q[x]$ is Sidon. To do this, we first define some functions over $\mathbb{F}_q[x]$ as follows.

Definition 3.1. *For any $P \in \mathbb{F}_q[x]$ and $r \in \mathbb{F}_q$, let*

$$d_r(P) = |\{(a, b) \in \mathbb{F}_q \times \mathbb{F}_q \colon P(a) - P(b) = r\}|$$
$$v_r(P) = |\{x \in \mathbb{F}_q \colon P(x) = r\}|.$$

When the discussed polynomial is clear from the context, we simply write d_r and v_r instead of $d_r(P)$ and $v_r(P)$.

Now we are ready to state the criteria, as follows:

Theorem 3.2. *If $P \in \mathbb{F}_q[x]$ is a Sidon polynomial, then*

$$d_r(P) \leq \begin{cases} 2q-1, & r=0 \\ q, & r \neq 0, \end{cases}$$

and

$$\sum_{i \in \mathbb{F}_q} v_i v_{i+r} \leq \begin{cases} 2q-1, & r=0 \\ q, & r \neq 0. \end{cases}$$

Proof. We first bound $d_r(P)$. Let $H = (P, Q)$ be a maximum Sidon set, and

$$H - H = \{h_1 - h_2,\ h_1, h_2 \in H\}.$$

Suppose for a fixed $r \in \mathbb{F}_q$, $(r, w) \in H - H$ for a certain $w \in \mathbb{F}_q$. This implies that the system of equations

$$\begin{aligned} P(x) - P(y) &= r \\ Q(x) - Q(y) &= w \end{aligned} \tag{1}$$

has a solution in $\mathbb{F}_q \times \mathbb{F}_q$. Furthermore, since H is a Sidon set, this solution is unique if $(r, w) \neq (0, 0)$.

If $r \neq 0$, because H is a Sidon set, each $w \in \mathbb{F}_q$ generates at most one pair $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ that satisfy Equations (1). This implies

$$d_r(P) \leq q$$

for all nonzero r, which completes the proof in this case.

Next, we consider the case where $r = 0$, and bound $d_0(P)$. By the preceding argument, each nonzero $w \in \mathbb{F}_q$ contributes to at most one solution of Equations (1). Then, when $w = 0$, since H is a Sidon set, the only possible solutions of Equations (1) are when $x = y$. By these observations, we have

$$d_0(P) \leq q - 1 + q = 2q - 1,$$

which completes the proof of the first inequality.

We now prove the second inequality. To do this, we prove that the left-hand side of this inequality is equivalent to the first inequality. By the definition of v_i, the number of $x, y \in \mathbb{F}_q$ such that $P(x) = i + r$ and $P(y) = i$ is $v_i v_{i+r}$. Summing over all possible i, we have

$$d_r(P) = \sum_{i \in \mathbb{F}_q} v_i v_{i+r}.$$

This completes the proof of this theorem. □

We note that $P = x^2$ satisfies the equality case for both inequalities for $r = 0$. Also, $P = x$ satisfies the equality case for $r \neq 0$.

We note that Theorem 3.2 generalizes the observation in Remark 3 of Rónyai and Szönyi [15].

Before giving another criterion to determine a Sidon polynomial, we first prove a short lemma on the number of solutions of a linear equation over a Sidon set H. We recall that for a set H equipped with an addition operation, we define

$$H + H = \{h + h' \colon h, h' \in H\}.$$

Lemma 3.3. *Let H be a Sidon set. If $s \in H+H$, the equation $x+y=s$ has exactly one solution in H if and only if $s=2h$, for an $h \in H$. Otherwise, the equation has exactly two solutions in H.*

Proof. Since $s \in H+H$ there exist $(a,b) \in H \times H$ with $a+b=s$. Suppose $(c,d) \in H \times H$ with $c+d=s$ as well. Then,

$$a-c=d-b.$$

Since H is a Sidon set, we have $(a,b)=(c,d)$ or $(a,b)=(d,c)$. If $a=b$ then (a,a) is the only solution of the above equation, and if $a \neq b$ there are exactly two solutions, namely (a,b) and (b,a). This completes the proof □

We can now derive another criterion to determine a Sidon polynomial.

Theorem 3.4. *If $P \in \mathbb{F}_q[x]$ is a Sidon polynomial, then for all $r \in \mathbb{F}_q$,*

$$v_{2^{-1}r} + \sum_{i \in \mathbb{F}_q} v_i v_{r-i} \leq 2q.$$

Proof. Let $P \in \mathbb{F}_q[x]$ be a Sidon polynomial and $H=(P,Q)$ be a Sidon set. First, we prove that, for a fixed $r \in \mathbb{F}_q$

$$|\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \colon P(a)+P(b)=r\}| = \sum_{i \in \mathbb{F}_q} v_i v_{r-i}.$$

This is done by considering that, for an arbitrary $i \in \mathbb{F}_q$, there are $v_i v_{r-i}$ ways of choosing $a,b \in \mathbb{F}_q$ with $P(a)=i$ and $P(b)=r-i$.

Consider a map $\mathbb{F}_q \times \mathbb{F}_q \to H+H$ defined as

$$(x,y) \mapsto (P(x)+P(y), Q(x)+Q(y)).$$

By Lemma 3.3, this map is two-to-one, except when $x=y$.

Now, for a fixed $r \in \mathbb{F}_q$, we consider an element $(r,w) \in H+H$. By definition, there exist $a,b \in \mathbb{F}_q$ that satisfy the system of equations

$$\begin{aligned} P(a)+P(b) &= r \\ Q(a)+Q(b) &= w. \end{aligned}$$

By the observation in the preceding paragraph, and dividing the cases where $a \neq b$ and $a=b$, we have that there are exactly

$$\frac{1}{2}|\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q, a \neq b \colon P(a)+P(b)=r\}| + v_{2^{-1}r}$$

elements of the form (r,w) in $H+H$, for a fixed $r \in \mathbb{F}_q$. Since there are at most q distinct element of the form (r,w) for a fixed r, we have that

$$\frac{1}{2}|\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q, a \neq b \colon P(a)+P(b)=r\}| + v_{2^{-1}r} \leq q.$$

On the other hand,

$$\begin{aligned} \sum_{i \in \mathbb{F}_q} v_i v_{r-i} &= |\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \colon P(a)+P(b)=r\}| \\ &= |\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q, a \neq b \colon P(a)+P(b)=r\}| + v_{2^{-1}r}. \end{aligned}$$

From these two statements, we may get

$$v_{2^{-1}r} + \sum_{i \in \mathbb{F}_q} v_i v_{r-i} \leq 2q,$$

which proves the theorem. □

We also notice that when $r = 0$, $P = x^2$ and $q \equiv 1 \pmod 4$, equality occurs in Theorem 3.4.

4. Classifying Sidon polynomials

As the first application of the criteria in the previous section, we classify a class of Sidon and non-Sidon monomials.

Proposition 4.1. *Let $r > 2$ be a natural number, $p > 3$ be a prime and q be a prime power of p. Then,*

(i) $P(x) = x^r \in \mathbb{F}_q[x]$ is not a Sidon polynomial in $\mathbb{F}_q \times \mathbb{F}_q$ if $r \mid q - 1$.

(ii) $P(x) = x^r \in \mathbb{F}_q[x]$ is a Sidon polynomial in $\mathbb{F}_q \times \mathbb{F}_q$ if $(r, q - 1) = 1$.

(iii) In $\mathbb{F}_p \times \mathbb{F}_p$, the set (x^r, Q) is a Sidon set if and only if $Q(x^k)$ is a quadratic polynomial (modulo $x^p - x$), where k is taken to satisfy $p - 1 \mid kr - 1$.

Proof. We first prove the first statement. Let $P = x^r \in \mathbb{F}_q[x]$ with $r \mid q-1$ and $r > 2$. For an arbitrary nonzero $i \in \mathbb{F}_q$ we notice that the equation $x^r = i$ has exactly zero or r solutions in $\mathbb{F}_q$. Furthermore, there are exactly $\dfrac{q-1}{r}$ values of i such that this equation has r solutions. By counting, we may get

$$d_0(P) = |\{(a, b) \in \mathbb{F}_q \times \mathbb{F}_q \colon a^r = b^r\}| = 1 + r^2 \cdot \frac{q-1}{r} > 2q.$$

This violates Theorem 3.2, therefore, this polynomial is not a Sidon polynomial.

Now we prove the other statements. Firstly, since $(r, q-1) = 1$, there exists k such that $q-1 \mid kr-1$. Since $(r, q-1) = (k, q-1) = 1$, that (from [14], for example) x^r and x^k are permutation polynomials over $\mathbb{F}_q$.

Hence, since composition with permutation polynomial (modulo $x^q - x$) preserves the Sidon property of a set, we see that (x^r, Q) is a Sidon set if and only if $((x^k)^r, Q(x^k)) = (x, Q(x^k))$ is also Sidon. Picking $Q = x^{2r}$, we have that x^r is a Sidon polynomial. And, from Lemma 1.3, we see that $Q(x^k) \pmod{x^q - x}$ must be quadratic, which proves the last statement. □

We then proceed with classifying cubic Sidon polynomials. We prove that all cubic polynomials in $\mathbb{F}_q[x]$ are classified, with regards to $\sim$, in one of three equivalence classes.

Theorem 4.2. *Let q be a prime power with $\mathrm{char}(\mathbb{F}_q) > 3$, $P \in \mathbb{F}_q[x]$ be a cubic polynomial, and k be a nonsquare in $\mathbb{F}_q$. Then, P is equivalent to one of x^3, $x^3 - x$, and $x^3 - kx$. Additionally, these three polynomials are not permutation-equivalent with each other.*

Proof. We first prove that for any cubic $P \in \mathbb{F}_q[x]$, there exists a $w \in \mathbb{F}_q$ with

$$P \sim x^3 - wx.$$

Let $P = ax^3 + bx^2 + cx + d$, and $ba^{-1} = e$, $ca^{-1} = f$. We get

$$\begin{aligned} P &\sim x^3 + ba^{-1}x^2 + ca^{-1}x + da^{-1} \\ &\sim x^3 + ex^2 + fx \sim \left(x - \frac{e}{3}\right)^3 + e\left(x - \frac{e}{3}\right)^2 + f\left(x - \frac{e}{3}\right) \\ &\sim x^3 - \left(f - \frac{e^2}{3}\right)x = x^3 - wx, \end{aligned}$$

which proves the statement.

Next, we prove that

$$x^3 - k_1 x \sim x^3 - k_2 x,$$

where $k_1, k_2 \in \mathbb{F}_q$ are both nonzero squares in $\mathbb{F}_q$ or are both not squares in $\mathbb{F}_q$. Notice that in either cases, k_1/k_2 is a square in $\mathbb{F}_q$. Let $k_1/k_2 = r^2$. Then, we have that

$$x^3 - k_1 x = x^3 - k_2 r^2 x \sim (rx)^3 - k_2 r^2 rx = r^3(x^3 - k_2 x) \sim x^3 - k_2 x,$$

which proves the statement.

By this point, we see that any cubic polynomial $P \in \mathbb{F}_q$ is equivalent to either x^3, $x^3 - x$, or $x^3 - kx$, for a fixed nonsquare $k \in \mathbb{F}_q$. We now prove that these three polynomials are not equivalent over $\sim$.

We first prove that x^3 is equivalent to neither $x^3 - x$ nor $x^3 - kx$, with respect to $\sim$. By Theorem 2.5, it suffices to prove $f(x^3, 3) \neq f(x^3 - x, 3)$ and $f(x^3, 3) \neq f(x^3 - kx, 3)$. We can easily show that

$$f(x^3, 3) > 0,\ f(x^3 - x, 3) = f(x^3 - kx, 3) = 0,$$

which completes the proof.

Next, we prove that $x^3 - x$ and $x^3 - kx$ are not equivalent. We have that

$$f(x^3 - x, 2) > 0$$

Now we prove $x^3 - x$ and $x^3 - kx$ are not equivalent over $\sim$. By Theorem 2.5, it is sufficient to prove

$$f(x^3 - x, 2) \neq f(x^3 - kx, 2).$$

We recall that $f(x^3 - x, 3) = 0$. Therefore, $f(x^3 - x, 2) > 0$ if and only if there exists an $\alpha \in \mathbb{F}_q$ such that the polynomial $x^3 - x - \alpha$ has a double root $\gamma \in \mathbb{F}_q$. The last scenario is possible if and only if $3\gamma^2 - 1 = 0$, which implies $1/3$ is a square in $\mathbb{F}_q$. By the same reasoning, we have that $f(x^3 - kx, 2) > 0$ if and only if $k/3$ is a square.

Since k is a nonsquare, $1/3$ and $k/3$ cannot both be squares in $\mathbb{F}_q$. Hence, when $f(x^3 - x, 2) > 0$, we have $f(x^3 - kx, 2) = 0$ and vice versa. This completes the proof. □

We also prove that these classes are distinct from the equivalence classes of linear polynomials and quadratic polynomials, except at two special cases.

Theorem 4.3. *Let q be a prime power with $\mathrm{char}(\mathbb{F}_q) > 3$. The classes x^3, $x^3 - x$, and $x^3 - kx$ (where k is a nonsquare) are equivalent to neither x nor x^2 in $\mathbb{F}_q[x]$, except in the following cases:*

1. *$x^3 \sim x$ when $q \equiv -1 \pmod 6$*
2. *$x^3 - kx \sim x^2$ when $q = 5$.*

Proof. We first prove that x^3 is equivalent to neither x^2 nor x. We first see that if $6|q-1$, x^3 is not a Sidon polynomial by Proposition 4.1. Therefore, in this case, this polynomial is equivalent to neither x^2 nor x^2. Next, we see that when $6|q+1$, x^3 is a permutation polynomial over $\mathbb{F}_q$. Therefore, we have $x^3 \sim x$ in this case. This completes the proof of the initial statement.

Next, we prove that $x^3 - x$ is equivalent to neither x nor x^2. From Theorem 2.5, it is sufficient to prove $g(x^3 - x, 3)$ is equal to neither $g(x, 3)$ nor $g(x^2, 3)$. We see that

$$g(x, 3) = g(x^2, 3) = 0.$$

However, since $x^3 - x = 0$ has three roots in $\mathbb{F}_q$, we have

$$g(x^3 - x, 3) > 0.$$

This implies that $x^3 - x \not\sim x^3$ and $x^3 - x \not\sim x^2$, which completes the proof.

Now we prove that $x^3 - kx$ (where k is a nonsquare) is not equivalent to x. Using the normalized permutation polynomial table in [14, Table (7.1)], we see that the only possible normalized permutation polynomials with degree 3 on this case is x^3 (if $q \equiv 1 \pmod 6$). However, since we already see that $x^3 \not\sim x^3 - kx$, it is not possible for $x^3 - kx$ to be a permutation polynomial. Hence, $x^3 - kx \not\sim x$.

Lastly, we prove that $x^3 - kx$ is not equivalent to x^2 when $q \neq 5$. To prove this, we compare $g(x^2, 2)$ and $g(x^3 - kx, 2)$. Firstly, since there are exactly $\dfrac{q-1}{2}$ nonzero squares in $\mathbb{F}_q$, we have

$$g(x^2, 2) = \frac{q-1}{2}.$$

We now calculate $g(x^3 - kx, 2)$. We notice that the polynomial $x^3 - kx - \alpha$ has exactly two roots in $\mathbb{F}_q$ if and only if this polynomial has double root. Suppose that the root is $\gamma \in \mathbb{F}_q$. We then have

$$3\gamma^2 - k = 0.$$

This equation has exactly zero or two solutions over $\mathbb{F}_q$. Since each solution of the equation corresponds to a different α, we have

$$g(x^3 - kx, 2) \leq 2.$$

Now suppose that $x^2 \sim x^3 - kx$. Then, $g(x^2, 2) = g(x^3 - kx, 2)$. Hence,

$$\frac{q-1}{2} \leq 2.$$

This implies that $q = 5$, since $\mathrm{char}(\mathbb{F}_q) > 3$.

It remains to prove that $x^2 \sim x^3 - kx$ in $\mathbb{F}_5$. To do this, we observe that

$$(x^3 - 3x, x^3 - 2x^2 + 3x) = \{(0,0), (3,2), (2,1), (3,3), (2,4)\} = (2x^2, x).$$

Since 3 is not a square in $\mathbb{F}_5$, this completes the proof of the theorem. □

After classifying all classes of cubic polynomials over $\mathbb{F}_q[x]$, we now apply the criteria of Sidon polynomials that we have to the three polynomials. First, we see that the following statement follows directly from Proposition 4.1 and Theorem 4.3.

Corollary 4.4. *Let q be a prime power with $\mathrm{char}(\mathbb{F}_q) > 3$. Then, the polynomial $P(x) = x^3 \in \mathbb{F}_q[x]$ is a Sidon polynomial over $\mathbb{F}_q \times \mathbb{F}_q$ if and only if $q \equiv -1 \pmod 6$.*

For other classes of cubic polynomials, we have the following classifications when $q = p$ is a prime. The proof of this proposition is given in Section 6.

Proposition 4.5. *Let $p > 3$ be a prime. Then, any polynomials that are equivalent to one of these polynomials are not Sidon polynomials in $\mathbb{F}_p \times \mathbb{F}_p$:*

(i) $P(x) = x^3 - kx$, *if k is a nonsquare in $\mathbb{F}_p$ and $12 \mid p+1$.*

(ii) $P(x) = x^3 - x$, *if $12 \nmid p-1$.*

The other cases are still open, as per the authors' knowledge. However, the authors believe further criteria on Sidon polynomials are needed.

5. Proof of Theorem 2.5

5.1. The invariant f

We first prove that $f(P,n) = f(R \circ P \circ T, n)$ for any positive integer n and permutation polynomials $R, T \in \mathbb{F}_q[x]$. For this purpose, we define

$$\mathcal{F}_n(Q) = \{\alpha \in \mathbb{F}_q \colon Q(x) - \alpha \text{ has a root of multiplicity at least } n\},$$

for a $Q \in \mathbb{F}_q[x]$.

By definition, we have $|\mathcal{F}_n(Q)| = f(Q,n)$. Hence, in order to prove the original statement, it is sufficient to exhibit a bijection between $\mathcal{F}_n(P)$ and $\mathcal{F}_n(R \circ P \circ T)$. We now prove that the map $\phi(\alpha) = R(\alpha)$ for all $\alpha \in \mathcal{F}_n(Q)$ satisfies this criterion.

First, we observe that since R is a permutation polynomial, the map ϕ is a bijection between $\mathcal{F}_n(P)$ and $\phi(\mathcal{F}_n(P))$. It remains to prove that the range of ϕ is $\mathcal{F}_n(R \circ P \circ T)$.

We now prove that $R(\alpha) \in \mathcal{F}_n(R \circ P \circ T)$ for each $\alpha \in \mathcal{F}_n(P)$. We first prove that $\alpha \in \mathcal{F}_n(P \circ T)$. Since $\alpha \in \mathcal{F}_n(P)$, there exist $\gamma \in \mathbb{F}_q$ and $Q_1 \in \mathbb{F}_q[x]$ with

$$P(x) - \alpha = (x - \gamma)^n Q_1(x).$$

Substituting $x \to T(x)$, we have

$$P(T(x)) - \alpha = (T(x) - \gamma)^n Q_1(T(x)).$$

Since T is a permutation polynomial, we see that $T^{-1}(\gamma)$ is a root of $T(x) - \gamma$. Hence, $x - T^{-1}(\gamma) \mid T(x) - \gamma$, and

$$(x - T^{-1}(\gamma))^n \mid P(T(x)) - \alpha.$$

This implies $T^{-1}(\gamma)$ is a root of $P(T(x)) - \alpha$ with order at least n, which completes the proof.

We now prove that $R(\alpha) \in \mathcal{F}_n(R \circ P \circ T)$. We observe that

$$P(T(x)) - \alpha \mid R(P(T(x))) - R(\alpha).$$

Hence, by the relations above, $R(P(T(x))) - R(\alpha)$ has a root of multiplicity at least n as well (namely, $T^{-1}(\gamma)$). This proves the initial assertion, and hence the original statement.

5.2. The invariant g

We aim to prove that $g(P,n) = g(R \circ P \circ T, n)$ for any positive integer n and permutation polynomials $R, T \in \mathbb{F}_q[x]$. For this purpose, we define

$$\mathcal{G}_n(Q) = \{\alpha \in \mathbb{F}_q \colon Q(x) - \alpha \text{ has exactly } n \text{ distinct roots in } \mathbb{F}_q\}$$

for a $Q \in \mathbb{F}_q[x]$.

By definition, we have $|\mathcal{G}_n(Q)| = g(Q,n)$. Hence, in order to prove the original statement, it is sufficient to exhibit a bijection between $\mathcal{G}_n(P)$ and $\mathcal{G}_n(R\circ P\circ T)$. We now prove that the map $\psi(\alpha) = R(\alpha)$ for all $\alpha \in \mathcal{G}_n(Q)$ satisfies this criterion.

We first observe that since R is a permutation polynomial, the map ψ is a bijection between $\mathcal{G}_n(P)$ and $\psi(\mathcal{G}_n(P))$. It remains to prove that the range of ψ is $\mathcal{G}_n(R \circ P \circ T)$.

We now prove that $R(\alpha) \in \mathcal{G}_n(R \circ P \circ T)$ for each $\alpha \in \mathcal{G}_n(P)$. Because $\alpha \in \mathcal{G}_n(P)$, the equation $P(x) = \alpha$ has exactly n different solutions in $\mathbb{F}_q$. Because T is a permutation polynomial, the equation

$$P(T(y)) = \alpha$$

also has exactly n solutions in $\mathbb{F}_q$, by letting $y = T^{-1}(x)$.

Then, because R is a permutation polynomial, the equation

$$R(P(T(y))) = R(\alpha)$$

has exactly n solutions in $\mathbb{F}_q$. Hence, $R(\alpha) \in \mathcal{G}_n(R \circ P \circ T)$, which completes the proof of the initial assertion.

6. Proof of Proposition 4.5

By Theorem 3.2, we may count the solution of $P(x) = P(y)$ in $\mathbb{F}_p$ to determine whether a polynomial is a Sidon polynomial over $\mathbb{F}_p \times \mathbb{F}_p$. In the case of $P = x^3 - cx$, the equation $P(x) = P(y)$ is equivalent to

$$x = y \text{ or } x^2 + xy + y^2 = c.$$

We now calculate the solutions of $x^2 + xy + y^2 = c$, where $c \in \mathbb{F}_p$ is nonzero.

Proposition 6.1. *Let $c \in \mathbb{F}_p$, $c \neq 0$. Then,*

$$|\{(a,b) \in \mathbb{F}_p \times \mathbb{F}_p \colon a^2 + ab + b^2 = c\}| = \begin{cases} p+1, & \text{if } p \equiv -1 \pmod 6 \\ p-1, & \text{if } p \equiv 1 \pmod 6. \end{cases}$$

Proof. Let $h(a,b) = a^2 + ab + b^2$. We notice that

$$h(a,b) = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 1 & 2^{-1} \\ 2^{-1} & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

and

$$\det\left(\begin{pmatrix} 1 & 2^{-1} \\ 2^{-1} & 1 \end{pmatrix}\right) = 2^{-2} \cdot 3.$$

By [14, Theorem 6.26], the number of solutions of $a^2 + ab + b^2 = c$ over $\mathbb{F}_p \times \mathbb{F}_p$, where $c \neq 0$, is

$$p - \eta(-2^{-2} \cdot 3) = p - \eta(-3),$$

where η is the quadratic character of $\mathbb{F}_p$. Since

$$\eta(-3) = \begin{cases} -1, & \text{if } p \equiv -1 \pmod 6 \\ 1, & \text{if } p \equiv 1 \pmod 6, \end{cases}$$

this completes the proof of the proposition. □

We proceed to count the number of solutions of the equation $P(a) = P(b)$, where $P = x^3 - cx \in \mathbb{F}_p[x]$. We recall that this quantity is denoted by $d_0(P)$.

Proposition 6.2. *Let $P(x) = x^3 - cx$ with $c \neq 0$. Then,*

$$d_0(P) = \begin{cases} 2p-3, & p \equiv 1 \pmod 6,\ c/3 \text{ is a square,} \\ 2p-1, & p \equiv 1 \pmod 6,\ c/3 \text{ is a nonsquare,} \\ 2p-1, & p \equiv -1 \pmod 6,\ c/3 \text{ is a square,} \\ 2p+1, & p \equiv -1 \pmod 6,\ c/3 \text{ is a nonsquare.} \end{cases}$$

Proof. By the algebraic manipulation done before, we only need to calculate the number of solutions of

$$a^2 + ab + b^2 = c$$

over $\mathbb{F}_q \times \mathbb{F}_q$, with $a \neq b$.

Without the restriction $a \neq b$, we see that the problem is equivalent to Proposition 6.1. Now, we proceed to count the number of solutions in the case $a = b$. We see that the equation

$$3a^2 = c$$

has exactly two solutions if and only if $c/3$ is a square; else, there are no solutions. Adding the p solutions of $P(x) = P(y)$ where $x = y$, the proof can now be completed by careful case division. □

We recall that, from Theorem 3.2, if P is a Sidon polynomial, $d_0(P) \leq 2p - 1$. Hence, by Proposition 6.2, we see that when $p \equiv -1 \pmod 6$ and $c/3$ is a nonsquare, $P(x) = x^3 - cx$ is not a Sidon polynomial in $\mathbb{F}_p \times \mathbb{F}_p$. Now, notice that 3 is a square in $\mathbb{F}_p$ if and only if $12 \mid p \pm 1$. By using quadratic reciprocity, we have the following results:

(i) If $p \equiv -1 \pmod{12}$ and k is a nonsquare in $\mathbb{F}_p$, $P(x) = x^3 - kx$ is not a Sidon polynomial.

(ii) If $p \equiv 5 \pmod{12}$ and c is a square in $\mathbb{F}_p$, $P(x) = x^3 - cx$ is not a Sidon polynomial.

The first result implies the first part of Proposition 4.5, and the second result implies the second part of Proposition 4.5, for the case $p \equiv 5 \pmod{12}$. We now to prove the second statement of Proposition 4.5. Namely, we prove

$$P(x) = x^3 - x$$

is not a Sidon polynomial in $\mathbb{F}_p \times \mathbb{F}_p$ for $p \equiv -1 \pmod{12}$ or $p \equiv -5 \pmod{12}$. We use the criterion in Theorem 3.4. We first notice that $v_i = v_{-i}$. Therefore, by substituting $r = 0$ in the left-hand side of Theorem 3.4, we have

$$\begin{aligned} v_{2^{-1}\cdot 0} + \sum_{i \in \mathbb{F}_q} v_i v_{0-i} &= v_0 + \sum_{i \in \mathbb{F}_q} v_i^2 \\ &= v_0 + d_0(P) \\ &= d_0(P) + 3, \end{aligned}$$

where the last equation can be deduced from the fact that $x^3 - x = 0$ has three distinct solutions in $\mathbb{F}_p$.

We first let $p \equiv -1 \pmod{12}$. This implies that $p \equiv -1 \pmod 6$. Since $1/3$ is a square in $\mathbb{F}_p$, we have that

$$d_0(P) + 3 = 2p + 2$$

from Proposition 6.2. By Theorem 3.4, P is not a Sidon polynomial.

Next, let $p \equiv -5 \pmod{12}$. This implies that $p \equiv 1 \pmod{6}$. Since $1/3$ is not a square in $\mathbb{F}_p$, we have that

$$d_0(P) + 3 = 2p + 2$$

from Proposition 6.2. Hence, P is not a Sidon polynomial from Theorem 3.4. This completes the proof of the theorem.

Acknowledgment: We would like to thank anonymous reviewers for constructive feedbacks, especially on giving additional references and simplifying the proof of Proposition 6.1. This research is supported by PPMI ITB 2021.

References

[1] P. Allen, P. Keevash, B. Sudakov, J. Verstraëte, Turán numbers of bipartite graphs plus an odd cycle, J. Combin. Theory Ser. B. 106 (2014) 134–162.
[2] E. Bergman, R. S. Coulter, I. Villa, Classifying planar monomials over fields of order a prime cubed, Finite Fields Their Appl. 78 (2022) 101959.
[3] P. Candela, J. Rué, O. Serra, Memorial to Javier Cilleruelo: a problem list, Integers, 18(A28) (2018) 9 pp.
[4] C. Carlet, Boolean functions for cryptography and coding theory, Cambridge University Press (2021).
[5] J. Cilleruelo, Combinatorial problems in finite fields and Sidon sets, Combinatorica, 32 (2012) 497–511.
[6] J. Cilleruelo, I. Ruzsa, C. Vinuesa, Generalized Sidon sets, Adv Math. 225(5) (2010) 2786–2807.
[7] R. S. Coulter, F. Lazebnik, On the classification of planar monomials over fields of square order, Finite Fields Their Appl. 18(2) (2012) 316–336.
[8] R. S. Coulter, R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.
[9] R. S. Coulter, R. W. Matthews, C. Timmons, Planar polynomials and an extremal problem of Fischer and Matoušek, J. Comb. Theory, Ser. B. 128 (2018) 96–103.
[10] P. Dembowski, T. G. Ostrom, Planes of order n with collineation groups of order n^2, Math. Z. 103 (1968) 239–258.
[11] P. Erdös, P. Turán, On a problem of Sidon in additive number theory, and some related problems, J. London Math. Soc. 16(4) (1941) 212–215.
[12] D. Gluck, A note on permutation polynomials and discrete geometries, Discrete Math. 80(1) (1990) 97–100.
[13] Y. Hiramine, A conjecture on affine planes of prime order, J. Comb. Theory Ser. A. 52(1) (1989) 44–50.
[14] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press (2000).
[15] L. Rónyai, L. Szönyi, Planar function over finite fields, Combinatorica, 9 (1989) 315–320.
[16] J. Solymosi, Incidences and the spectra of graphs, In: Combinatorial number theory and additive group theory. Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, (2009) 299–314.
[17] C. Timmons, J. Verstraëte, A counterexample to sparse removal, Eur. J. Comb. 44(A) (2015) 77–86.