ON GENERALIZATIONS OF \(p\)-SETS AND THEIR APPLICATIONS

HENG ZHOU AND ZHIQIANG XU

Abstract: The \(p\)-set, which is in a simple analytic form, is well distributed in unit cubes. The well-known Weil’s exponential sum theorem presents an upper bound of the exponential sum over the \(p\)-set. Based on the result, one shows that the \(p\)-set performs well in numerical integration, in compressed sensing as well as in UQ. However, \(p\)-set is somewhat rigid since the cardinality of the \(p\)-set is a prime \(p\) and the set only depends on the prime number \(p\). The purpose of this paper is to present generalizations of \(p\)-sets, say \(P_{a,\epsilon,d,p}\), which is more flexible. Particularly, when a prime number \(p\) is given, we have many different choices of the new \(p\)-sets. Under the assumption that Goldbach conjecture holds, for any even number \(m\), we present a point set, say \(L_{p,q}\), with cardinality \(m - 1\) by combining two different new \(p\)-sets, which overcomes a major bottleneck of the \(p\)-set. We also present the upper bounds of the exponential sums over \(P_{a,\epsilon,d,p}\) and \(L_{p,q}\), which imply these sets have many potential applications.

Key words and phrases \(p\)-set; Deterministic sampling; Numerical integral; Exponential sum

AMS Subject Classification 2000 11K38, 65C05, 11L05, 41A10, 65D32

1. Introduction

1.1. \(p\)-set. Let \(p\) be a prime number. We consider the point set

\[ P_{d,p} = \{x_0, \ldots, x_{p-1}\} \subset [0,1)^d \]

where

\[ x_j = \left( \left\{ \frac{j}{p} \right\}, \left\{ \frac{j^2}{p} \right\}, \ldots, \left\{ \frac{j^d}{p} \right\} \right) \in [0,1)^d, \quad j \in \mathbb{Z}_p, \]

\(\mathbb{Z}_p := \{0,1,\ldots,p-1\}\) and \(\{x\}\) is the fractional part of \(x\) for a nonnegative real number \(x\). The point set \(P_{d,p}\) is called \(p\)-set and was introduced by Korobov \[5\] and Hua-Wang \[4\]. Recently, \(p\)-set attracts much attention since its advantage in numerical integration \[1\], in the recovery of sparse trigonometric polynomials \[12\] and in the UQ \[13\]. In \[1\], Dick presents a numerical integration formula based on \(P_{d,p}\) with showing the error bound of the formula depends only polynomially on the dimension \(d\). In \[12\], Xu uses \(P_{d,p}\) to construct the deterministic sampling points of sparse trigonometric polynomials and show the sampling

---

Heng Zhou was supported by the National Natural Science Foundation of China (No. 61602341); Zhiqiang Xu was supported by NSFC grant (11422113, 91630203, 11331012) and by National Basic Research Program of China (973 Program 2015CB856000).
matrix corresponding to $\mathcal{P}_{d,p}$ has the almost optimal coherence. And hence, $\mathcal{P}_{d,p}$ has a good performance for the recovery of sparse trigonometric polynomials.

1.2. Extensions of $p$-set: $\mathcal{P}_{d,p}^{a,\epsilon}$ and $\mathcal{L}_{p,q}$. The $p$-set is in a simple analytic form and hence it is easy to be generated by computer. However, the $p$-set is somewhat rigid with the point set only depending on a prime number $p$. If the function values at some points in $p$-set are not easy to be obtained, one has to change the prime number $p$ to obtain a new point set which has the different cardinality with the previous one. Hence, in practical application, it will be better that one has many different choices. We next introduce a generalization of $p$-set.

Let
\[
Z_p^d := \{ a = (a_1, \ldots, a_d) \in \mathbb{Z}^d : a_j \in \mathbb{Z}_p, j = 1, \ldots, d \}. 
\]

Suppose that $a = (a_1, \ldots, a_d) \in Z_p^d$ and $\epsilon = (\epsilon_1, \ldots, \epsilon_{d-1}) \in \{0,1\}^{d-1}$. We set
\[
(1) \quad \mathcal{P}_{d,p}^{a,\epsilon} := \{ x_j^{a,\epsilon} : j \in \mathbb{Z}_p \}
\]
where
\[
x_j^{a,\epsilon} := \left\{ \left\{ \frac{a_1 j}{p} \right\}, \left\{ \frac{a_1 j + a_2 j^2}{p} \right\}, \ldots, \left\{ \frac{\sum_{h=1}^{d-1} a_h j^h + a_d j^d}{p} \right\} \right\} \in [0,1)^d
\]
and $a_k^j = \epsilon_k a_k, k = 1, \ldots, d - 1$. We call $\mathcal{P}_{d,p}^{a,\epsilon}$ as the $p$-set associating with the parameter $a$ and $\epsilon$. If we take $a = (1, \ldots, 1)$ and $\epsilon = (0, \ldots, 0)$, then $\mathcal{P}_{d,p}^{a,\epsilon}$ is reduced to the classical $p$-set.

The $p$-set $\mathcal{P}_{d,p}^{a,\epsilon}$ associating with the parameters $a, \epsilon$ is more flexible. Given the prime number $p$, one can generate various point sets by changing the parameters $a$ and $\epsilon$ with presenting an option set when the cardinality $p$ is given.

Note that the cardinality of both $\mathcal{P}_{d,p}^{a,\epsilon}$ and $\mathcal{P}_{d,p}$ is prime. Since the distance between adjacent prime can be very large, the cardinality of $p$-set does not change smoothly. Using the set $\mathcal{P}_{d,p}^{a,\epsilon}$, we next present a set with the cardinality being odd number. Suppose that $m \in 2\mathbb{Z}$ is given. The Goldbach conjecture, which is one of the best-known unsolved problem in number theory, says that $m$ can be written as the sum of two primes, i.e., $m = p + q$ where $p$ and $q$ are prime numbers. One has verified the conjecture up to $m \leq 4 \cdot 10^{14}$ which is enough for practical application. We next suppose that $m = p + q$ with $p$ and $q$ being prime numbers. We set
\[
(2) \quad \mathcal{L}_{p,q} := \left\{ \begin{array}{ll} 
\mathcal{P}_{d,p} \cup \mathcal{P}_{d,q}, & p \neq q \\
\mathcal{P}_{d,p}^{a,\epsilon} \cup \mathcal{P}_{d,q}^{a,\epsilon'}, & p = q, 
\end{array} \right.
\]
where $\mathcal{P}_{d,p}^{a,\epsilon'}$ and $\mathcal{P}_{d,q}^{a,\epsilon''}$ are the $p$-sets that we have defined above and $a, b \in \mathbb{Z}_p^d, \epsilon', \epsilon'' \in \{0,1\}^{d-1}$. We call $\mathcal{L}_{p,q}$ the $(p,q)$-set. As shown later, $\mathcal{P}_{d,p} \cap \mathcal{P}_{d,q} = \{(0, \ldots, 0)\}$ provided $p \neq q$. We can choose $a, b, \epsilon'$ and $\epsilon''$ so that $\mathcal{P}_{d,p}^{a,\epsilon'} \cap \mathcal{P}_{d,q}^{b,\epsilon''} = \{(0, \ldots, 0)\}$. Hence, under the assumption of Goldbach conjecture, for any odd number, says $m - 1$, there exist $p, q$ so that $|\mathcal{L}_{p,q}| = p + q - 1 = m - 1$.

We would like to mention the following point sets with cardinality $p^2$ [5, 4] :
\[
Q_{p^2,d} = \{ z_j : j = 0, \ldots, p^2 - 1 \}, \quad z_j = \left( \left\{ \frac{j}{p^2} \right\}, \left\{ \frac{j^2}{p^2} \right\}, \ldots, \left\{ \frac{j^d}{p^2} \right\} \right) \in [0,1)^d;
\]
\[
(3) \quad R_{p^2,d} = \{ z_{j,k} : j, k = 0, \ldots, p - 1 \}, \quad z_{j,k} = \left( \left\{ \frac{k}{p} \right\}, \left\{ \frac{jk}{p} \right\}, \ldots, \left\{ \frac{j^{d-1}k}{p} \right\} \right) \in [0,1)^d.
\]
The weighted star discrepancy of $Q_{p^2,d}$ and $R_{p^2,d}$ is given in [2]. Using a similar method with above, we can generalize $Q_{p^2,d}$ and $R_{p^2,d}$ to $Q_{p^2,d}$ and $R_{p^2,d}$, respectively. We will introduce it in Section 2.3 in detail.

1.3. Organization. In Section 2, we present the upper bounds of the exponential sums over $P_{d,p}$ and $L_{p,q}$. Particularly, we present the condition under which $|L_{p,q}| = p + q - 1$ and also prove that $P_{d,p} \cap P_{d,p} = \{0, \ldots, 0\}$ when $P_{d,p} \neq P_{d,p}$. We furthermore consider the generalization of the point sets $Q_{p^2,d}$ and $R_{p^2,d}$ and present the upper bounds of exponential sums over the new sets. The results in Section 2 show that the point sets presented in this paper have many potential applications in various areas. In Section 3, we choose $L_{p,q}$ as a deterministic sampling set for the recovery of sparse trigonometric polynomials and then show their performance.

2. THE EXPONENTIAL SUMS OVER $P_{d,p}$ AND $L_{p,q}$

The aim of this section is to present the exponential sums over $P_{d,p}$ and $L_{p,q}$. To this end, we first introduce the well-known Weil’s formula, which plays a key role in our proof.

Theorem 2.1. [11] Suppose that $p$ is a prime number. Suppose $f(x) = \sum_{h=1}^{d} m_h x^h$ with $m_h \in \mathbb{Z}$ $(h = 1, \ldots, d)$ and there is a $j \in \{1, 2, \ldots, d\}$, satisfying $p \nmid m_j$. Then

$$\left| \sum_{x=1}^{p} e^{\frac{2\pi i f(x)}{p}} \right| \leq (d - 1) \sqrt{p}.$$ 

2.1. THE EXPONENTIAL SUM OVER $P_{d,p}$. Recall that

$$P_{d,p} := \{ x^{a,\epsilon}_{j} : j \in \mathbb{Z}_p \}$$

and

$$x^{a,\epsilon}_{j} = \left( \left\{ \frac{a_1 j}{p} \right\}, \left\{ \frac{a_2 j + a_2 j^2}{p} \right\}, \ldots, \left\{ \frac{\sum_{h=1}^{d} a_h j^h + a_d j^d}{p} \right\} \right) \in [0,1)^d$$

where $a = (a_1, \ldots, a_d) \in [1, p - 1]^d \cap \mathbb{Z}^d$, $a_j' = \epsilon_j a_j$ and $\epsilon = (\epsilon_1, \ldots, \epsilon_{d-1}) \in \{0,1\}^{d-1}$. Note that $|P_{d,p}| = p$. We next show the exponential sum formula over $P_{d,p}$.

Theorem 2.2. For any $k \in [-p + 1, p - 1]^d \cap \mathbb{Z}^d$ and $k \neq 0$, we have

$$\left| \sum_{x \in P_{d,p}} \exp(2\pi ik \cdot x) \right| = \left| \sum_{j=0}^{p-1} \exp(2\pi ik \cdot x^{a,\epsilon}_{j}) \right| \leq (d - 1) \sqrt{p}.$$ 

Proof. Set

$$g(j) = \sum_{\ell=1}^{d} c_{\ell} j^\ell$$

where $c_\ell = k_\ell a_\ell + k_{\ell+1} a_\ell' + \cdots + k_d a_d'$. We set $j_0 := \max \{ \ell : k_\ell \neq 0 \}$. Then $c_{j_0} = k_{j_0} a_{j_0}$ and we have $p \nmid c_{j_0}$. According to Theorem 2.1, we obtain that

$$\left| \sum_{j=0}^{p-1} \exp(2\pi ik \cdot x^{a,\epsilon}_{j}) \right| = \left| \sum_{j=0}^{p-1} \exp \left( 2\pi i \frac{g(j)}{p} \right) \right| \leq (d - 1) \sqrt{p}.$$ 

□
2.2. The exponential sum over $\mathcal{L}_{p,q}$. To this end, we consider the cardinality of $\mathcal{L}_{p,q}$. A simple observation is that $|\mathcal{L}_{p,q}| \leq p + q - 1$. We would like to present the condition under which $|\mathcal{L}_{p,q}| = p + q - 1$. We first consider the case where $p \neq q$.

**Theorem 2.3.** Suppose that $p$ and $q$ are two distinct prime numbers. Then $|\mathcal{L}_{p,q}| = p + q - 1$.

**Proof.** According to (2), to this end, we just need show that 

$$\mathcal{P}_{d,p} \cap \mathcal{P}_{d,q} = \{0, \ldots, 0\}.$$ 

We prove it by contradiction. Assume that $\mathcal{P}_{d,p} \cap \mathcal{P}_{d,q} \neq \{0, \ldots, 0\}$, and then there exists $j \in \mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$ and $k \in \mathbb{Z}_q^*$ so that $\left\{\frac{j^i}{p}\right\} = \left\{\frac{k^j}{q}\right\}$, $i = 1, \ldots, d$. Particularly, we have $\frac{j}{p} = \frac{k}{q}$, which is equivalent to $jq = kp$. Since $p$ and $q$ are different prime numbers, $j \in \mathbb{Z}_p^*$ and $k \in \mathbb{Z}_q^*$, we have $j \mid k$ and hence $p = q$. A contradiction. \(\square\)

We next consider the case where $p = q$, i.e., $\mathcal{L}_{p,q} = \mathcal{P}_{d,p} \cup \mathcal{P}_{d,p}^{d,p}$. For the case where $c' = c''$, we have

**Theorem 2.4.** Suppose that $c \in \{0, 1\}^{d-1}$ is a fixed vector and $a = (a_1, \ldots, a_d) \in \mathbb{Z}_p^d$, $b = (b_1, \ldots, b_d) \in \mathbb{Z}_p^d$.

(1) $\mathcal{P}_{d,p}^{a,c} \subseteq \mathcal{P}_{d,p}^{b,c}$ if and only if there exists $c \in \mathbb{Z}_p^*$ such that $b_j c^j \equiv a_j \pmod{p}$ for $j = 1, \ldots, d$.

(2) If $\mathcal{P}_{d,p}^{a,c} \not\subseteq \mathcal{P}_{d,p}^{b,c}$, then $\mathcal{P}_{d,p}^{a,c} \cap \mathcal{P}_{d,p}^{b,c} = \{0, \ldots, 0\}$.

**Proof.** (1) We first suppose that there exists $c \in \mathbb{Z}_p^*$ such that $b_j c^j \equiv a_j \pmod{p}$ for $j \in \{1, \ldots, d\}$. Recall that 

$$\mathcal{P}_{d,p}^{a,c} = \left\{x_j^{a,c} : j \in \mathbb{Z}_p\right\},$$ 

where

$$x_j^{a,c} = \left(\frac{a_1 j}{p}, \frac{a_1' j + a_2 j^2}{p}, \ldots, \frac{\sum_{h=1}^{d-1} a_h' j^h + a_d j^d}{p}\right).$$

For any $j_0 \in \mathbb{Z}_p$, we take $k_0 \equiv c j_0 \pmod{p}$. Then

$$x_{j_0}^{a,c} = \left(\frac{a_1 j_0}{p}, \frac{a_1' j_0 + a_2 j_0^2}{p}, \ldots, \frac{\sum_{h=1}^{d-1} a_h' j_0^h + a_d j_0^d}{p}\right) = x_{k_0}^{b,c},$$

which implies that

$$\mathcal{P}_{d,p}^{a,c} \subseteq \mathcal{P}_{d,p}^{b,c}.$$ 

Here we use $b_j' c^j \equiv a_j' \pmod{p}$ which follows from $b_j c^j \equiv a_j \pmod{p}$.

Since $p$ is a prime number, there exists $c^{-1} \in \mathbb{Z}_p^*$ so that $c^{-1} c \equiv 1 \pmod{p}$. Then we have $b_j \equiv a_j c^{-j} \pmod{p}$, $j = 1, \ldots, d$. Then, similarly, for any $j_0 \in \mathbb{Z}_p$,

$$x_{j_0}^{b,c} = x_{c^{-1} j_0}^{a,c},$$

which implies that

$$\mathcal{P}_{d,p}^{b,c} \subseteq \mathcal{P}_{d,p}^{a,c}.$$
Theorem 2.5. Suppose that there exist \( a_1 j_0 \equiv b_1 k_0 \pmod{p} \), which implies that \( a_1 c \equiv 0 \), we set \( c \equiv a_1 c' \pmod{p} \). Then the followings hold.

(1) We assume that (7) holds. Take \( P \)

(2) We prove it by contradiction. Assume that \( P \)

(3) Assume that \( a_j \equiv b_j c'' \pmod{p} \)

(4) We prove it by contradiction. Assume that \( P \)

(5) \( \sum_{h=1}^{d-1} a_h j_0^h + a_d j_0^d \equiv \sum_{h=1}^{d-1} b_h j_0^h + b_d j_0^d \pmod{p} \).

We set \( c \equiv k_0 j_0^{-1} \pmod{p} \), where \( j_0^{-1} \in \mathbb{Z}_p \) so that \( x_0^a = x_0^b \). Similarly with the above proof, we can find a \( c \equiv k_0 j_0^{-1} \pmod{p} \) so that \( a_j \equiv b_j c'' \pmod{p} \) for \( j = 1, \ldots, d \). It leads to \( P_d = P_{d,p} \) by (1) of Theorem 2.4, which is impossible by the assumption in (2).

We next consider the case where \( c' \neq c'' \).

Theorem 2.5. Suppose that \( c', c'' \in \{0, 1\}^{d-1} \) with \( c' \neq c'' \). Set

\[ Z := \{ j : c'_j \neq c''_j \text{ and } a_j^2 + b_j^2 \neq 0, 1 \leq j \leq d - 1 \}, \]

and

\[ \ell_0 := \min \{ j : j \in Z \}. \]

Then the followings hold.

(1) \( P_d = P_{d,p} \) if and only if there exists a \( c \in \mathbb{Z}_p^d \) so that

\[ a_j \equiv b_j c \pmod{p} \]

(2) Assume that \( P_d \neq P_{d,p} \) where \( a, b \in \mathbb{Z}_p^d \). If \( Z = \emptyset \) then we have

\[ P_d \cap P_{d,p} = \{(0, \ldots, 0)\}. \]

If \( Z \neq \emptyset \), then \(|P_d \cap P_{d,p}| \leq r + 1\), where

\[ r = \min \{ j : a_j^2 + b_j^2 \neq 0 \}. \]

(3) Assume that \( Z \neq \emptyset \), and \( a_1 \neq 0 \). If \( a_1 b_{1+1} b_{2+1} \equiv a_1 b_{1+1} b_{2+1} \pmod{p} \), then

\[ P_d \cap P_{d,p} = \{(0, \ldots, 0)\}. \]

Proof. (1) We assume that (7) holds. Take

\[ \epsilon_j = \begin{cases} \epsilon'_j, & \text{if } \epsilon'_j = \epsilon''_j \\ 0, & \text{if } \epsilon'_j \neq \epsilon''_j \end{cases} \]

Noting that \( a_j = b_j = 0 \), we have \( P_d = P_{d,p} \) and \( P_d = P_{d,p} \). Theorem 2.4 implies that \( P_d = P_{d,p} \) and hence \( P_d = P_{d,p} \).
We next assume that $\mathcal{P}_{d,p}^{a,c'} = \mathcal{P}_{d,p}^{b,c''}$ which is equivalent to that there exists a permutation 
\{k_0, k_1, \ldots, k_{p-1}\} of \{0, 1, \ldots, p - 1\} so that
\[ x_j^{a,c'} = x_{k_j}^{b,c''}, \quad j = 0, 1, \ldots, p - 1. \]
(8)

This is equivalent to
\[ a_1 \equiv b_1 k_1 \pmod{p} \]
\[ 2a_1 \equiv b_1 k_2 \pmod{p} \]
(9)
\[ \vdots \]
\[ (p-1)a_1 \equiv b_1 k_{p-1} \pmod{p} \]
and
\[ \sum_{i=1}^{i-1} a'_i + a_i \equiv \sum_{h=1}^{i-1} b'_h k_1^h + b_1 k_1^i \pmod{p} \]
\[ \sum_{h=1}^{i-1} 2^h a'_h + a_i 2^i \equiv \sum_{h=1}^{i-1} b'_h k_2^h + b_1 k_2^i \pmod{p} \]
(10)
\[ \vdots \]
\[ \sum_{h=1}^{i-1} (p-1)^h a'_h + a_i (p-1)^i \equiv \sum_{h=1}^{i-1} b'_h k_{p-1}^h + b_1 k_{p-1}^i \pmod{p}, \]
for $i = 2, \ldots, d$. Since $a_1 \neq 0$, by (9) we have
\[ a_1 \equiv b_1 k_1 \pmod{p} \]
\[ k_2 \equiv 2k_1 \pmod{p} \]
(11)
\[ \vdots \]
\[ k_{p-1} \equiv (p-1)k_1 \pmod{p}. \]

Set $j_0 := \min \{ i : \epsilon'_i \neq \epsilon''_i \}$. Using the same argument with the one in Theorem 2.4 we have
\[ a_i \equiv b_i k_1^i \pmod{p}, i = 1, \ldots, j_0. \]
Combining (11) for $i = j_0 + 1$ and (11) we have
\[ a_{j_0} + a_{j_0+1} \equiv b_{j_0} k_1^{j_0} + b_{j_0+1} k_1^{j_0+1} \pmod{p} \]
\[ 2^{j_0} a_{j_0} + 2^{j_0+1} a_{j_0+1} \equiv b_{j_0} k_2^{j_0} + b_{j_0+1} k_2^{j_0+1} \pmod{p}. \]

Without loss of generality, we can assume $\epsilon'_i = 1$ and $\epsilon''_i = 0$ and then
\[ a_{j_0} + a_{j_0+1} \equiv b_{j_0+1} k_1^{j_0+1} \pmod{p} \]
\[ 2^{j_0} a_{j_0} + 2^{j_0+1} a_{j_0+1} \equiv b_{j_0+1} k_2^{j_0+1} \pmod{p}, \]
which implies $a_{j_0} = b_{j_0} = 0$ since $k_2 \equiv 2k_1 \pmod{p}$ and $a_{j_0} = b_{j_0} k_1^{j_0} \pmod{p}$.

(2) We first assume that $Z = \emptyset$ which implies $a_j = b_j = 0$ provided $\epsilon'_j \neq \epsilon''_j$. Take
\[ \epsilon_j = \begin{cases} \epsilon'_j, & \text{if } \epsilon'_j = \epsilon''_j \\ 0, & \text{if } \epsilon'_j \neq \epsilon''_j. \end{cases} \]
Noting that $a_j = b_j = 0$ provided $\epsilon'_j \neq \epsilon''_j$, we have $\mathcal{P}_{d,p}^{a,c} = \mathcal{P}_{d,p}^{a,c'}$ and $\mathcal{P}_{d,p}^{b,c} = \mathcal{P}_{d,p}^{b,c''}$. The (2) of Theorem 2.4 implies that $\mathcal{P}_{d,p}^{a,c',c''} \cap \mathcal{P}_{d,p}^{b,c',c''} = \{(0, \ldots, 0)\}$. We next consider the case where
Z \neq \emptyset$. Suppose that $\mathcal{P}_{d,p}^{a_e'}$ and $\mathcal{P}_{d,p}^{b_e''}$ have a common nonzero point. Then, there exist $j, k \in \mathbb{Z}_p$ so that

$$a_1j \equiv b_1k \pmod{p}$$

$$a_1'j + a_2j^2 \equiv b_1'k + b_2k^2 \pmod{p}$$

(12)

Note that $a_h = b_h = 0$ when $h \leq r - 1$ and $a_h' = b_h' = 0, h \leq r - 1$. The (12) implies that

$$a_hj^h \equiv b_hk^h \pmod{p}, \quad h = r, \ldots, \ell_0,$$

(13)

$$a_{\ell_0}j^{\ell_0} + a_{\ell_0 + 1}j^{\ell_0 + 1} \equiv b_{\ell_0}k^{\ell_0} + b_{\ell_0 + 1}k^{\ell_0 + 1} \pmod{p}.$$  

(14)

Without loss of generality, we can assume $\ell_0 = 1$ and $\ell_0'' = 0$. By (14), we have

$$a_{\ell_0}j^{\ell_0} + a_{\ell_0 + 1}j^{\ell_0 + 1} \equiv b_{\ell_0 + 1}k^{\ell_0 + 1} \pmod{p}.$$  

Taking $h = r$ in (13), we have $a_r = b_r(k^{-1}r) \pmod{p}$ where $j^{-1} \in \mathbb{Z}_p$ satisfies $j^{-1}j \equiv 1 \pmod{p}$. Since $a_r^2 + b_r^2 \neq 0$, we have $a_r \neq 0$. Set $x_0 = kj^{-1}$. Then $x_0$ satisfies

$$a_r \equiv b_r x_0^r \pmod{p}$$

$$a_{\ell_0}j^{\ell_0} + a_{\ell_0 + 1}j^{\ell_0 + 1} \equiv b_{\ell_0 + 1}k^{\ell_0 + 1} \pmod{p}.$$  

Each nonzero point in $\mathcal{P}_{d,p}^{a_e'} \cap \mathcal{P}_{d,p}^{b_e''}$ corresponds to a solution to

$$a_r \equiv b_r x^r \pmod{p}$$

$$a_{\ell_0}j^{\ell_0} + a_{\ell_0 + 1}j^{\ell_0 + 1} \equiv b_{\ell_0 + 1}k^{\ell_0 + 1} \pmod{p}.$$  

(15)

Note that $a_r \equiv b_r x^r \pmod{p}$ has at most $r$ solutions. Hence,

$$|\mathcal{P}_{d,p}^{a_e'} \cap \mathcal{P}_{d,p}^{b_e''}| \leq r + 1.$$  

(3) We prove it by contradiction. Assume that $\mathcal{P}_{d,p}^{a_e'} \cap \mathcal{P}_{d,q}^{a_e''} \neq \{(0, \ldots, 0)\}$, and then there exist $j_0, k_0 \in \mathbb{Z}_p$ so that $x_{j_0}^{a_e} = x_{k_0}^{b_e''.}$ Particularly, we have

$$a_{h,j_0^h} \equiv b_hk_0^h \pmod{p}, h = 1, \ldots, \ell_0,$$

(16)

$$a_{\ell_0,j_0^{\ell_0}} + a_{\ell_0 + 1,j_0^{\ell_0 + 1}} \equiv b_{\ell_0,k_0^{\ell_0}} + b_{\ell_0 + 1,k_0^{\ell_0 + 1}} \pmod{p}.$$  

(17)

Without loss of generality, we can assume $\ell_0 = 1$ and $\ell_0'' = 0$. By (17), we have

$$a_{\ell_0,j_0^{\ell_0}} + a_{\ell_0 + 1,j_0^{\ell_0 + 1}} \equiv b_{\ell_0 + 1,k_0^{\ell_0 + 1}} \pmod{p}.$$  

(18)

By (16) with $h = 1$, we have

$$a_{\ell_0 + 1,j_0^{\ell_0 + 1}} - b_{\ell_0 + 1,k_0^{\ell_0 + 1}} \equiv a_{\ell_0 + 1}(b_1k_0a_1^{-1})_{\ell_0 + 1} - b_{\ell_0 + 1}k_0^{\ell_0 + 1}$$

$$= k_0^{\ell_0 + 1}(a_{\ell_0 + 1}b_1^{\ell_0 + 1}a_1^{-\ell_0 - 1} - b_{\ell_0 + 1})$$

$$\equiv 0 \pmod{p},$$

according to $a_{\ell_0 + 1}b_1^{\ell_0 + 1} \equiv a_1^{\ell_0 + 1}b_{\ell_0 + 1} \pmod{p}$. By (18), we have $a_{\ell_0,j_0^{\ell_0}} \equiv 0 \pmod{p}$, which implies that $a_{\ell_0} \equiv 0 \pmod{p}$ or $j_0 \equiv 0 \pmod{p}$. This is impossible by the assumption.

□
In the following, we choose the appropriate vectors $a, b$ so that $|\mathcal{L}_{p,q}| = q + p - 1$. We now state the inequalities for exponential sums over $\mathcal{L}_{p,q}$, which is the main result of this subsection.

**Theorem 2.6.** Suppose $p$ and $q$ are odd prime numbers and set $m = p + q$. Recall that

$$
\mathcal{L}_{p,q} = \begin{cases}
p_{d,p} \cup p_{d,q}, & p \neq q \\
^{a,c}p_{d,p} \cup ^{b,c}p_{d,p}, & p = q.
\end{cases}
$$

We assume that $|\mathcal{L}_{p,q}| = p + q - 1$. Then, for any $k \in [-p + 1, p - 1]^d \cap [-q + 1, q - 1]^d \cap \mathbb{Z}^d$ and $k \neq 0$, we have

$$
| \sum_{x \in \mathcal{L}_{p,q}} \exp(2 \pi i k \cdot x) | \leq (d - 1) \sqrt{2m} + 1.
$$

**Proof.** We first consider the case where $p = q$. We have

$$
\mathcal{L}_{p,q} = p_{d,p}^{b,c} \cup p_{d,p}^{b,c}. 
$$

Recall that

$$
p_{d,p}^{a,c} \cap p_{d,p}^{b,c} = \{(0, \ldots, 0)\}.
$$

Then

$$
| \sum_{x \in \mathcal{L}_{p,q}} \exp(2 \pi i k \cdot x) | \leq \left| \sum_{x \in p_{d,p}^{a,c}} \exp(2 \pi i k \cdot x) \right| + \left| \sum_{x \in p_{d,p}^{b,c}} \exp(2 \pi i k \cdot x) \right| + 1
$$

$$
\leq (d - 1) \sqrt{p} + (d - 1) \sqrt{q} + 1 = (d - 1) \sqrt{2m} + 1.
$$

Here, in the last inequality, we use Theorem 2.2. We next consider the case where $p \neq q$. When $p \neq q$, $\mathcal{L}_{p,q} = p_{d,p} \cup p_{d,q}$. Then we have

$$
| \sum_{x \in \mathcal{L}_{p,q}} \exp(2 \pi i k \cdot x) | \leq \left| \sum_{x \in p_{d,p}} \exp(2 \pi i k \cdot x) \right| + \left| \sum_{x \in p_{d,q}} \exp(2 \pi i k \cdot x) \right| + 1
$$

$$
\leq (d - 1) \sqrt{p} + (d - 1) \sqrt{q} + 1
\leq (d - 1) \sqrt{2m} + 1.
$$

\[ \square \]

### 2.3. The exponential sums over $\mathcal{Q}^{a,c}_{p^2,d}$ and $\mathcal{R}^{a,c}_{p^2,d}$

Suppose that $a \in \mathbb{Z}_p^d$ and $\epsilon \in \{0,1\}^{d-1}$. We set

$$
\mathcal{Q}^{a,c}_{p^2,d} := \{ z^{a,c}_{j} : j = 0, \ldots, p^2 - 1 \},
$$

$$
z^{a,c}_{j} = \left( \left\{ \frac{a_{1,j}}{p^2} \right\}, \left\{ \frac{a_{1,j} + a_{2,j}}{p^2} \right\}, \ldots, \left\{ \frac{\sum_{h=1}^{d-1} a_{h,j} h + a_{d,j} d}{p^2} \right\} \right) \in [0,1)^d;
$$

and

$$
\mathcal{R}^{a,c}_{p^2,d} := \{ z^{a,c}_{j,k} : j, k = 0, \ldots, p - 1 \},
$$

$$
z^{a,c}_{j,k} = \left( \left\{ \frac{a_{1,k}}{p} \right\}, \left\{ \frac{(a_{1}^t + a_{2}) k}{p} \right\}, \ldots, \left\{ \frac{\sum_{h=1}^{d} a_{h,j} h + a_{d,j} d - 1}{p} \right\} \right) \in [0,1)^d.
$$

The $\mathcal{Q}^{a,c}_{p^2,d}$ and $\mathcal{R}^{a,c}_{p^2,d}$ can be considered as the generalization of the $p$-sets given in [3]. Based on the Lemma 5 and Lemma 6 in [2], we can obtain the following inequalities for exponential sums over $\mathcal{Q}^{a,c}_{p^2,d}$ and $\mathcal{R}^{a,c}_{p^2,d}$.
Theorem 2.7. Suppose that \( a \in \mathbb{Z}_p^n \) and \( \epsilon \in \{0,1\}^{d-1} \). Then, for any \( k = (k_1, \ldots, k_d) \in [-p+1, p-1]^d \cap \mathbb{Z}^d \) and \( k \neq 0 \), we have

\[
\left| \sum_{x \in \mathbb{Q}_{p^2}^n} \exp(2\pi i k \cdot x) \right| \leq (d-1)p.
\]

Proof. Set

\[
g(j) := \sum_{\ell=1}^{d} c_{\ell} j^\ell,
\]

where \( c_{\ell} = k_\ell a_{\ell} + k_{\ell+1} a'_{\ell+1} + \cdots + k_d a'_{d} \). We set \( j_0 := \max \{ \ell : k_\ell \neq 0 \} \). Then \( c_{j_0} = k_{j_0} a_{j_0} \) and we have \( p \nmid c_{j_0} \). According to Lemma 5 in [2], we have

\[
\left| \sum_{x \in \mathbb{Q}_{p^2}^n} \exp(2\pi i k \cdot x) \right| = \left| \sum_{j=0}^{p^2-1} \exp \left( 2\pi i \frac{g(j)}{p^2} \right) \right| \leq (d-1)p.
\]

\[ \square \]

Theorem 2.8. Suppose that \( a \in [1, p-1]^d \cap \mathbb{Z}^d \). Then, for any \( k \in [-p+1, p-1]^d \cap \mathbb{Z}^d \) and \( k \neq 0 \), we have

\[
\left| \sum_{x \in \mathbb{R}_{p^2}^n} \exp(2\pi i k \cdot x) \right| \leq (d-1)p.
\]

Proof. Set

\[
g(j) := \sum_{\ell=0}^{d-1} c_{\ell} j^\ell
\]

and \( c_{\ell} := k_{\ell+1} a_{\ell+1} + k_{\ell+2} a'_{\ell+1} + \cdots + k_d a'_{d} \). We set \( j_0 := \max \{ \ell : k_\ell \neq 0 \} \). Then \( c_{j_0-1} = k_{j_0} a_{j_0} \) and we have \( p \nmid c_{j_0-1} \). Using Lemma 6 in [2], we have

\[
\left| \sum_{x \in \mathbb{R}_{p^2}^n} \exp(2\pi i k \cdot x) \right| = \left| \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \exp \left( 2\pi i k \frac{g(j)}{p} \right) \right| \leq (d-1)p.
\]

\[ \square \]

3. The Applications of \( \mathcal{P}_{a,p}^s \) and \( \mathcal{L}_{p,q} \)

Based on the exponential sum formula in Section 2, the new point sets are useful in numerical integration [8, 1], in UQ [13] and in the recovery of sparse trigonometric polynomials [12]. We just state the results for the recovery of sparse trigonometric polynomials in detail.

We start with some notations which go back to [12]. Set

\[
\Pi_s^d := \left\{ f : f(x) = \sum_{k \in [-s, s]^d \cap \mathbb{Z}^d} c_k e^{2\pi i k \cdot x}, \ c_k \in \mathbb{C}, \ x \in [0,1]^d \right\}.
\]

Note that \( \Pi_s^d \) is a linear space with the dimension \( D := (2s+1)^d \). For

\[
f(x) = \sum_{k \in [-s, s]^d \cap \mathbb{Z}^d} c_k e^{2\pi i k \cdot x} \in \Pi_s^d,
\]

we set \( T := \{ k : c_k \neq 0 \} \) which is the support of the sequence of coefficients \( c_k \), and set

\[
\Pi_s^d(M) := \bigcup_{T \subseteq [-s, s]^d \cap \mathbb{Z}^d, |T| \leq M} \Pi_T.
\]
where $\Pi_T$ denotes the space of all trigonometric polynomials whose coefficients are supported on $T$. When $M \ll D$, we call the trigonometric polynomials in $\Pi_s^d(M)$ as $M$-sparse trigonometric polynomials.

The recovery of sparse trigonometric polynomials is an active topic recently. The main aim of this research topic is to design a sampling set $X = \{z_j\}_{j=1}^N$ so that one can recover $f \in \Pi_s^d(M)$ from $f(z_j), z_j \in X \setminus \{0\}$ [12, 9, 8]. We state the problem as follows. Assume the sampling set is $X = \{x_j \in [0,1]^d; j = 1, \ldots, N\}$. Then our aim is to solve the following programming:

$$\text{(19)} \quad \text{find } f \in \Pi_s^d(M) \text{ subject to } f(x_j) = y_j, \ j = 1, \ldots, N.$$ 

Denote by $F_X$ the $N \times D$ sampling matrix with entries

$$(F_X)_{j,k} = \exp(2\pi ik \cdot x_j), \ j = 1, \ldots, N, \ k \in [-s,s]^d \cap \mathbb{Z}^d.$$ 

Let $a_k = (\exp(2\pi ik \cdot x_j))_{j=1}^N$ denote a column of $F_X$ with $k \in [-s,s]^d \cap \mathbb{Z}^d$. A simple observation is that $\|a_k\|_2 = \sqrt{N}$. Set

$$\mu := \mu_X := \frac{1}{N} \max_{m,k \in [-s,s]^d \cap \mathbb{Z}^d, m \neq k} |\langle a_m, a_k \rangle|,$$ 

which is called the mutual incoherence of the matrix $F_X / \sqrt{N}$. Theorem 2.5 in [9] shows that if $\mu < 1/(2M - 1)$ then the Orthogonal Matching Pursuit Algorithm (OMP) and the Basis Pursuit Algorithm (BP) can recover any $M$-sparse trigonometric polynomials in $\Pi_s^d(M)$. Therefore, our aim is to choose the sampling set $X$ so that $\mu$ is small and hence OMP and BP can recover $M$-sparse trigonometric polynomials. Based on Theorem 2.2 and Theorem 2.6 respectively, the following results give upper bounds of $\mu$ with taking $X = \mathcal{P}_{a,p}^e$, and $X = \mathcal{L}_{p,q}$, respectively.

**Lemma 3.1.** (1) Suppose that $X = \mathcal{P}_{a,p}^e$ where $a \in [1, p - 1]^d \cap \mathbb{Z}^d$ and $p \geq 2s + 1$ is a prime number. Then

$$\mu_X \leq (d-1)/\sqrt{p}.$$ 

(2) Suppose that $p, q \geq 2s + 1$ are prime numbers and $a, b \in [1, p - 1]^d \cap \mathbb{Z}^d$. Recall that

$$L_{p,q} = \left\{ \begin{array}{l l} \mathcal{P}_{a,p} \cup \mathcal{P}_{d,q}, & p \neq q \\ \mathcal{P}_{a,p}^e \cup \mathcal{P}_{b,p}^e, & p = q. \end{array} \right.$$ 

Set $X = L_{p,q}$ and $m = p + q$. Then

$$\mu_X \leq \frac{(d-1)/2m + 1}{m - 1}.$$ 

As said before, if $\mu < 1/(2M - 1)$ then OMP (and also BP) can recover every $M$-sparse trigonometric polynomials. Then we have the following corollary:

**Theorem 3.2.** (1) Suppose that $p > \max\{2s + 1, (d-1)^2(2M - 1)^2 + 1\}$ is a prime number and $a \in [1, p - 1]^d \cap \mathbb{Z}^d$. Then OMP (and also BP) recovers every $M$-sparse trigonometric polynomial $f \in \Pi_s^d(M)$ exactly from the deterministic sampling $\mathcal{P}_{a,p}^e$.

(2) Under the condition in (2) of Lemma 3.1. Suppose that

$$m = p + q > \left( \frac{1}{\sqrt{2}} + \frac{1}{2} \right) (2M - 1)(d-1) + \sqrt{M}.$$ 

Then OMP (and also BP) recovers every $M$-sparse trigonometric polynomial $f \in \Pi_s^d(M)$ exactly from the deterministic sampling set $L_{p,q}$. 


Proof. We first consider (1). Note that $p \geq (d - 1)^2(2M - 1)^2 + 1$ implies that $(d - 1)/\sqrt{p} < 1/(2M - 1)$. According to (1) in Lemma 3.1, if $(d - 1)/\sqrt{p} < 1/(2M - 1)$ then $\mu < 1/(2M - 1)$ and hence the conclusion follows. Similarly, we can prove (2).

References

[1] J. Dick, Numerical integration of Hölder continuous, absolutely convergent Fourier-, Fourier cosine-, and Walsh series, J. Approx. Theory, 183, 14-30, 2014.
[2] J. Dick and F. Pillichshammer, The weighted star discrepancy of Korobov’s $p$-sets, Proceedings of the American Mathematical Society, 143(12), 5043-5057, 2015.
[3] Michael Drmota, Robert F. Tichy, Sequences, discrepancies and applications, Lecture Notes in Mathematics, vol. 1651, Springer-Verlag, Berlin, 1997.
[4] L. K. Hua and Y. Wang, Applications of number theory to numerical analysis. Springer-Verlag, Berlin-New York, 1981. Translated from the chinese edition, Science Press, Beijing, 1978.
[5] N. M. Korobov, Number-theoretic methods in approximate analysis. Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1963.
[6] S. Kunis, H. Rauhut, Random sampling of sparse trigonometric polynomials II- Orthogonal matching pursuit versus basis pursuit, Foundations of Computational Mathematics, 8(6), 1615-3375, 2008.
[7] Gunther Leobacher, Friedrich Pillichshammer, Introduction to quasi-Monte Carlo integration and applications, Compact Textbook in Mathematics, Birkhäuser/Springer, Cham, 2014.
[8] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, CBMS-NSF Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, 1992.
[9] H. Rauhut. Random sampling of sparse trigonometric polynomials, Appl. Comput. Harmon. Anal., 22, 16-42, 2007.
[10] Ian H. Sloan, Henryk Woźniakowski, When are quasi-Monte Carlo algorithms efficient for high-dimensional integrals?, J. Complexity, 14, 14(1), 1-33, 1998.
[11] A. Weil, On some exponential sums, PNAS, USA, 34, 204-207, 1948.
[12] Z. Xu, Deterministic sampling of sparse trigonometric polynomials, Journal of Complexity, 27(2), 133-140, 2011.
[13] T. Zhou, A. Narayan and Z. Xu, Multivariate discrete least-squares approximations with a new type of collocation grid, SIAM J. Sci. Comput., 36(5), A2401-A2422, 2014.

School of Sciences, Tianjin Polytechnic University, Tianjin 300160, China
E-mail address: zhouheng7590@sina.com.cn

LSEC, Institute of Computational Mathematics, Academy of Mathematics and System Sciences, Chinese Academy of Sciences, Beijing 100190, China
E-mail address: xuzq@lsec.cc.ac.cn