On Compressed Sensing Matrices Breaking the Square-Root Bottleneck

Shohei Satake
Faculty of Advanced Science and Technology
Kumamoto University
Kumamoto 860-8555, Japan
Email: shohei-satake@kumamoto-u.ac.jp

Yujie Gu
Faculty of Information Science and Electrical Engineering
Kyushu University
Fukuoka 819-0395, Japan
Email: gu@inf.kyushu-u.ac.jp

Abstract—Compressed sensing is a celebrated framework in signal processing and has many practical applications. One of the challenging problems in compressed sensing is to construct deterministic matrices having the restricted isometry property (RIP). So far, there are only a few publications providing deterministic RIP matrices beating the square-root bottleneck on the sparsity level. In this paper, we investigate RIP of certain matrices defined by higher power residues modulo primes. Moreover, we prove that the widely-believed generalized Paley graph conjecture implies that these matrices have RIP breaking the square-root bottleneck. Also the compression ratio realized by these RIP matrices is significantly larger than 2.

I. INTRODUCTION

Matrices with the restricted isometry property (RIP) have important applications to compressed processing. According to [8], by means of RIP matrices, it is possible to measure and recover sparse signals using significantly fewer measurements than the dimension of the signals.

Definition 1 (Restricted isometry property, RIP). Let $\Phi$ be a complex $M \times N$ matrix. Suppose that $K \leq M \leq N$ and $0 \leq \delta < 1$. Then $\Phi$ is said to have the $(K, \delta)$-restricted isometry property (RIP) if

$$
(1 - \delta)||x||^2 \leq ||\Phi x||^2 \leq (1 + \delta)||x||^2
$$

for every $N$-dimensional complex vector $x$ with at most $K$ non-zero entries. Here $|| \cdot ||$ denotes the $\ell_2$ norm.

According to Candès [8], for applications to signal processing, it suffices to investigate the $(K, \delta)$-RIP matrix for some $\delta < \sqrt{2} - 1$. In addition, the sparsity $K$ is expected to be as large as possible.

On the other hand, it is known ([3]) that the problem checking whether a given matrix has RIP is NP-hard. Thus many publications have attempted to look for deterministic constructions of matrices having RIP, for details and benefits of deterministic RIP matrices, see e.g. a recent survey [21].

Throughout this paper, we assume that all matrices have column vectors with unit $\ell_2$-norm. Most of known constructions for RIP matrices are investigated via the coherence $\mu(\Phi)$ of an $M \times N$ matrix $\Phi$ with column vectors $\psi_1, \ldots, \psi_N$, where

$$
\mu(\Phi) := \max_{1 \leq j \neq k \leq N} |\langle \psi_j, \psi_k \rangle|,
$$

and $\langle \cdot, \cdot \rangle$ denotes the standard inner product in the Hilbert space $\mathbb{C}^M$. It can be proved (e.g. [7]) that if $\mu(\Phi) = \mu$, then $\Phi$ has the $(K, (K-1)\mu)$-RIP, which implies the $(K, \delta)$-RIP with only $K = O(\sqrt{M})$, following from the well-known achievable Welch bound (3) in [27].

$$
\mu(\Phi) \geq \sqrt{\frac{N - M}{M(N - 1)}}.
$$

This barrier on the magnitude of the order of $K$ is popularly dubbed as the square-root bottleneck or quadratic bottleneck. Accordingly, the following problem arises.

Problem 2 ([7]). Construct an $M \times N$ matrix $\Phi$ having the $(K, \delta)$-RIP with $K = \Omega(M^\gamma)$ for some $\gamma > 1/2$ and $\delta < \sqrt{2} - 1$.

To our best knowledge, the first (unconditional) solution to this problem was given by Bourgain et al. [7], and later improved by Mixon [20]; see Table I.

On the other hand, in [4], Bandeira, Fickus, Mixon and Wong conjectured that the Paley matrix, a $(p+1)/2 \times (p+1)$ matrix defined by quadratic residues modulo an odd prime $p$, satisfies the $(K, \delta)$-RIP with $K \geq C_1 \cdot p / \log C_2 p$ and some $\delta < \sqrt{2} - 1$, where $C_1, C_2 > 0$ are universal constants. Under a number-theoretic conjecture in [11], Bandeira, Mixon and Moreira [5] proved that when $p \equiv 1$ (mod 4), the Paley matrix has the $(K, \delta)$-RIP with $K = \Omega(p^\gamma)$ for some $\gamma > 1/2$, which provides a conditional solution to Problem 2. Recently, assuming that the Paley graph conjecture (see Remark 9) holds, Satake [22] extended the result in [5] for general odd primes $p$, and also gave some implications to a Ramsey-theoretic problem proposed by Erdős and Moser [12]. Also, under another type of number-theoretic conjecture, Arikan and Yılmaz [2] proved that for a sufficiently large prime $p \equiv 3$ (mod 4), a $(p+1)/2 \times p$ matrix obtained by deleting the last column from the Paley matrix (see Remark 14) has the $(K, \delta)$-RIP for any $K < p^{5/7}/2$ and $\delta < 1/\sqrt{2}$. These results are summarized in Table I.

In this paper, we aim to investigate the RIP of certain matrices defined by higher power residues modulo primes. In particular, under the widely-believed generalized Paley graph conjecture formulated in Section II, we prove that these
matrices are new solutions to Problem 2, which forms our main theorem as described below.

Theorem 3. Suppose that the generalized Paley graph conjecture holds. Let \( \varepsilon_0 > 0 \) be a small real number and \( \varepsilon_1, \varepsilon_2 \) be real numbers with \( 0 \leq \varepsilon_1 < \varepsilon_2 < \varepsilon_0 \). Then for a sufficiently large prime \( p > n \) such that \( p - 1 \) contains a factor \( k \) with \( p^{s - 1} < k \leq p^{s + 2} \), there are \( M \times N \) matrices with \( (M,M^*) \), \( o(1) \)-RIP for some \( \gamma > 1/2 \), where \( M = (p + k - 1)/k \).

In terms of applications to signal processing, it is desirable to construct an \( M \times N \) matrix with RIP whose compression ratio \( N/M \) (e.g. \([18]\)) is as large as possible. As will be shown later, these matrices substantially contain the Paley matrix as a particular case, and realize compression ratio significantly better than that from the Paley matrix in general; see Remarks 14 and 15, respectively.

The remainder of this paper is organized as follows. Section II introduces some fundamental terminologies and results in finite fields, as well as some key notions related to RIP and the number-theoretic results on factors of shifted primes. Section III defines the matrix that we investigate in this paper, and then Section IV proves Theorem 3.

**II. Preliminaries**

**A. Finite fields and characters**

Throughout this paper, let \( p \) denote a prime number. Let \( \mathbb{F}_p \) be a finite field with \( p \) elements which can be identified to the residue ring \( \mathbb{Z}/p\mathbb{Z} \). It is well known that the multiplicative group of \( \mathbb{F}_p \), denoted by \( \mathbb{F}_p^* \), is a cyclic group of order \( p - 1 \), consisting of all non-zero elements of \( \mathbb{F}_p \).

The canonical additive character \( \psi \) of \( \mathbb{F}_p \) is a map from \( \mathbb{F}_p \) to the unit circle in \( \mathbb{C} \) such that \( \psi(x) := \exp(2\pi i x) \) for all \( x \in \mathbb{F}_p \). Notice that for every pair of \( x, y \in \mathbb{F}_p \), we have \( \psi(x + y) = \psi(x)\psi(y) \). A multiplicative character \( \chi \) of \( \mathbb{F}_p \) is a map from \( \mathbb{F}_p^* \) to the unit circle in \( \mathbb{C} \) such that \( \chi(xy) = \chi(x)\chi(y) \) for every pair of \( x, y \in \mathbb{F}_p^* \). We also adopt the convention that \( \chi(0) := 0 \). Note that if \( g \) is a generator of \( \mathbb{F}_p^* \), then each multiplicative character \( \chi \) is a map such that \( \chi(x) := \exp(2\pi i x/g) \) for all \( x = g^t \in \mathbb{F}_p^* \) and some \( 0 \leq s \leq p - 2 \). The multiplicative character of \( \mathbb{F}_p^* \) for \( s = 0 \) is said to be trivial. The order of a multiplicative character \( \chi \) is the minimum positive integer \( k \) such that \( (\chi(x))^k = 1 \) for all \( x \in \mathbb{F}_p^* \). Notice that the order of the trivial multiplicative character of \( \mathbb{F}_p^* \) is 1. For each \( 2 \leq k \leq p - 2 \) with \( k(p - 1) \), we can define a non-trivial multiplicative character \( \chi_k \) of \( \mathbb{F}_p^* \) of order \( k \), that is, \( \chi_k(x) := \exp\left(\frac{2\pi \sqrt{-1}}{k}x\right) \) for all \( x \in \mathbb{F}_p^* \) with \( x = g^t \). For each \( 1 \leq h \leq k - 1 \), define the multiplicative character \( \chi_k^{-h}(x) := \exp\left(\frac{2\pi \sqrt{-1}}{k}(-ht)\right) \) for all \( x \in \mathbb{F}_p^* \) with \( x = g^t \). Notice that \( \chi_k^{-h} \) is non-trivial for every \( 1 \leq h \leq k - 1 \).

**B. Gauss sums**

This subsection provides two types of Gauss sums; for details, see e.g. \([6]\).

**Definition 4** \((k-th power Gauss sum)\). Let \( 2 \leq k \leq p - 2 \). Then for each \( a \in \mathbb{F}_p \), the \( k-th power Gauss sum \( G_k(a) \) is defined as

\[
G_k(a) := \sum_{x \in \mathbb{F}_p^*} \psi(ax^k).
\]

**Definition 5** (Gauss sum). Let \( a \in \mathbb{F}_p \) and \( \chi \) a multiplicative character of \( \mathbb{F}_p \). Then define the Gauss sum \( G(a, \chi) \) as

\[
G(a, \chi) := \sum_{x \in \mathbb{F}_p^*} \chi(x)\psi(ax).
\]

For simplicity, let \( G(\chi) := G(1, \chi) \).

The following two lemmas are useful in this paper.

**Lemma 6.** \((6. \text{Theorem 1.1.3 and (1.1.4))}\) For each \( a \in \mathbb{F}_p^* \), it holds that

\[
G_k(a) = \sum_{h=1}^{k-1} G(a, \chi_k^h) = \sum_{h=1}^{k-1} \chi_k^{-h}(a) G(\chi_k^h).
\]

**Lemma 7.** \((6. \text{Theorem 1.1.4})\) For each \( 1 \leq h \leq k - 1 \), it holds that

\[
|G(\chi_k^h)| = \sqrt{p}.
\]
Remark 9. The Paley graph conjecture is Conjecture 8 for the case that \( \chi = \chi_2 \), where \( \chi_2 \) is a non-trivial multiplicative character of \( \mathbb{F}_p \) of order 2. According to the observations by Lenstra (see [28]), it may be reasonable to believe that Conjecture 8 would be true for any non-trivial \( \chi \) if the Paley graph conjecture holds. Indeed, it is well-known (e.g. [16]) that Conjecture 8 is true for any non-trivial multiplicative character \( \chi \) of \( \mathbb{F}_p \) and any \( S,T \subset \mathbb{F}_p \) with \( |S| > p^{1/2+\alpha} \) and \( |T| > p^{\alpha} \), where \( 0 < \alpha \leq 1/2 \). In [9], Chang made a significant progress towards Conjecture 8, confirming the conjecture for any non-trivial \( \chi \) and any \( S,T \subset \mathbb{F}_p \) such that \( |S| > p^{4/9+\alpha} \), \( |T| > p^{1/9+\alpha} \) with \( |S|+|T| < |T| \) for some \( K > 0 \) and arbitrary \( \alpha > 0 \), where \( T+T := \{ t_1 + t_2 : t_1,t_2 \in T \} \). For further and related results, see e.g. [15], [24], [25], [26].

D. A theorem on factors of shifted primes

To prove Theorem 3, it is necessary to certify the existence of infinitely many primes \( p \) such that the shifted prime \( p - 1 \) admits the prescribed factors. In this paper, we shall use the following theorem due to Ford [13, Theorem 7].

Theorem 10 ([13]). For any \( 0 \leq \varepsilon_1 < \varepsilon_2 \leq 1 \), there exists a constant \( C_{\varepsilon_1,\varepsilon_2} > 0 \) depending only on \( \varepsilon_1 \) and \( \varepsilon_2 \) such that there exist at least \( C_{\varepsilon_1,\varepsilon_2} \cdot x/\log x \) primes \( p \leq x \) so that \( p - 1 \) contains at least one factor \( k \) with \( x^{\varepsilon_1} < k < x^{\varepsilon_2} \). In particular, there exist infinitely many primes \( p \) such that \( p - 1 \) contains at least one factor \( k \) with \( p^{\varepsilon_1} < k < p^{\varepsilon_2} \).

Note that finding primes \( p \) in Theorem 10 can be done by the exhaustive search and the AKS primality test in [1] for example.

E. Flat restricted isometry property

The following notion, flat restricted isometry property (flat RIP), has been employed as an intermediate property to verify the RIP of matrices in [4] and [7].

Definition 11 (Flat RIP, [4], [7]). Let \( \Phi \) be an \( M \times N \) matrix with columns \( \phi_1, \ldots, \phi_N \). Suppose that \( K \leq M \leq N \) and \( \theta > 0 \). Then \( \Phi \) is said to have the \((K, \theta)\)-flat restricted isometry property (flat RIP) if

\[
|\sum_{i \in I} \phi_i, \sum_{j \in J} \phi_j| \leq \theta \sqrt{|I||J|}
\]

for every pair of disjoint subsets \( I, J \subset \{1, 2, \ldots, N\} \) with \( |I|, |J| \leq K \).

Proposition 12 ([4], [7]). Suppose that each column of \( \Phi \) has unit \( \ell_2 \) norm. Then \( \Phi \) has the \((K, 150 \theta \log K)\)-RIP provided that \( \Phi \) has the \((K, \theta)\)-flat RIP.

III. Construction of matrices

In this section, we define a type of matrices based on higher power residues modulo primes and later investigate their RIP in Section IV.

Definition 13. Let \( p \) be an odd prime and \( k|p-1 \). Let \( R_p^{(k)} := \{ x^k : x \in \mathbb{F}_p^* \} \) denote the set of all non-zero \( k \)-th powers of \( \mathbb{F}_p \), notice that \( |R_p^{(k)}| = (p-1)/k \). Suppose that elements of \( \mathbb{F}_p \) and \( R_p^{(k)} \) are labelled as \( \mathbb{F}_p = \{ 0 = a_1, a_2, \ldots, a_p \} \) and \( R_p^{(k)} = \{ b_1, b_2, \ldots, b_{(p-1)/k} \} \), respectively. Recall that \( \psi \) denotes the canonical additive character of \( \mathbb{F}_p \).

Then the matrix \( \Phi_p^{(k)} \) is defined as an \( M \times N \) complex matrix with \( M = \frac{p+k-1}{k} \) and \( N = p \) of the following form.

\[
\begin{bmatrix}
\frac{1}{\sqrt{p}} & \frac{1}{\sqrt{p}} & \cdots & \frac{1}{\sqrt{p}} \\
\frac{\sqrt{\frac{k}{p}}}{\sqrt{p}} & \frac{\sqrt{\frac{k}{p}} \psi(b_1 a_2)}{\sqrt{p}} & \cdots & \frac{\sqrt{\frac{k}{p}} \psi(b_1 a_p)}{\sqrt{p}} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{\sqrt{\frac{k}{p}}}{\sqrt{p}} & \frac{\sqrt{\frac{k}{p}} \psi(b_{p-1} a_2)}{\sqrt{p}} & \cdots & \frac{\sqrt{\frac{k}{p}} \psi(b_{p-1} a_p)}{\sqrt{p}}
\end{bmatrix}
\]

Note that each column \( \phi_i \) of \( \Phi_p^{(k)} \) has \( \ell_2 \)-norm 1 since for each \( 1 \leq i \leq p \),

\[
||\phi_i||^2 = (\phi_i, \phi_i) = 1 + \frac{k}{p} \sum_{l=1}^{p-1} \psi((a_i - a_l) b_l) = 1 + \frac{k}{p} \cdot \frac{p-1}{k} = 1.
\]

Remark 14. Let \( p \) be an odd prime. The Paley matrix in [5] is a \((p+1)/2 \times (p+1)\) matrix obtained from the matrix \( \Phi_p^{(2)} \) joining the vector \([\sqrt{-1}, 0, \ldots, 0]^T\) as the last column, where \( r = 0 \) if \( p \equiv 1 \pmod{4} \) and \( r = 1 \) if \( p \equiv 3 \pmod{4} \). The matrix investigated in [2] is exactly \( \Phi_p^{(2)} \).

Remark 15. By Definition 13, the compression ratio of \( \Phi_p^{(k)} \) is \( kp/(p+k-1) \approx k \) as long as \( k = o(p) \), while the compression ratio of the Paley matrix is only 2. Thus when \( k \geq 3 \), \( \Phi_p^{(k)} \) has compression ratio significantly better than that from the Paley matrix in general.

Proposition 12 shows that the flat-RIP provides a sufficient condition for the RIP. In [5], [22], the flat-RIP of Paley matrices was derived using the Paley graph conjecture (see Remark 9) which, however, is not enough to tackle with the matrix \( \Phi_p^{(k)} \) with \( k > 2 \) here. Later we shall make use of the generalized Paley graph conjecture (Conjecture 8) and the related techniques on Gauss sums to prove the flat-RIP for \( \Phi_p^{(k)} \) with \( k > 2 \), see Section IV for more details.

IV. Proof of Theorems

This section aims to prove the main result Theorem 3. To that end, we shall prove the following Theorem 16.

Theorem 16. Assuming that Conjecture 8 is true, and

1) let \( 0 < \alpha < 1/2 \) be a real number;
2) let \( \beta_0 = \beta_0(\alpha) > 0 \) be a real number such that \( \alpha + 2\beta_0 < 1/2 \) and the property \( P(\alpha, \beta_0) \) holds for any
non-trivial multiplicative character of $\mathbb{F}_q$ and any prime $q > p(\alpha)$, where $p(\alpha) > 0$ is from Conjecture 8;
3) take real numbers $\epsilon_1$ and $\epsilon_2$ with $0 \leq \epsilon_1 < \epsilon_2 < \beta_0$;
4) let $p > p(\alpha)$ be a prime such that there exists an integer $k$ such that $k|p-1$ and $p^{\epsilon_1} < k \leq p^{\epsilon_2}$.

Then for any real number $\tau$ with
\[ \max \left\{ \alpha + \beta_0, \frac{1}{2} - \frac{\epsilon_1}{\epsilon_2} \right\} < \tau < \frac{1}{2} - \epsilon_2, \quad (10) \]
the $(p + k - 1)k \times k$ matrix $\Phi_p^{(k)}$ in Definition 13 has the $(p^{\epsilon_1} + \beta_0, O(p^{\epsilon_2} + 1 + o(1)))$-RIP as $p \to \infty$.

**Remark 17.** We remark that for each $\alpha$, $\beta_0$, $\epsilon_1$ and $\epsilon_2$ satisfying the conditions 1), 2) and 3), it is possible to take a real number $\tau$ satisfying (10). Indeed, notice that $\alpha + \beta_0 < 1/2 - \epsilon_2$ holds since $\alpha + \beta_0 < 1/2 - \beta_0 < 1/2 - \epsilon_2$, where the first and second inequalities follow from the conditions 2) and 3), respectively. Also $\epsilon_2 - \epsilon_1 < 1/2 - \beta_0$ is valid, since $\epsilon_2 - \epsilon_1 / 2 < \beta_0$ holds for any $\epsilon_1$ and $\epsilon_2$ satisfying 3).

Before proceeding to prove Theorem 16, we show that Theorem 3 can be immediately derived from Theorems 10 and 16.

**Proof of Theorem 3.** According to Theorem 16,
- let $0 < \alpha < 1/2$ and $\beta_0 = \beta_0(\alpha) > 0$ be a real number satisfying the condition 2);
- take $\epsilon_0 = \epsilon_0(\alpha) = \beta_0$ and then choose $\epsilon_1$ and $\epsilon_2$ so that $0 \leq \epsilon_1 < \epsilon_2 < \epsilon_0$;
- take a prime $p > p(\alpha)$ satisfying the condition 4), which is doable by Theorem 10.

Note that based on the condition 4), we have $p^{\epsilon_1} < k \leq p^{\epsilon_2}$, implying $M = (p + k - 1)/k = O(p^{\epsilon_1})$. Therefore Theorem 16 shows that the $M \times k$ matrix $\Phi_p^{(k)}$ has the $(K, o(1))$-RIP, where $K = p^{\epsilon_1 + \beta_0} = \Omega(M)$
and $\gamma$ is a real number such that $\gamma \geq (\tau + \beta_0) \cdot (1 - \epsilon_1)^{-1} > 1/2$. This proves Theorem 3.

In order to prove Theorem 16, we need the following two key lemmas.

**A. Two key lemmas**

The first key lemma is an extension of [5, Lemma 3.3] and [22, Lemma 13] to multiplicative characters of order $k \geq 2$.

**Lemma 18.** Let $0 < \alpha < 1/2$ and $p$ a prime with $p > p(\alpha)$. Let $\chi$ be a non-trivial multiplicative character of $\mathbb{F}_p$. Suppose that there exists $\beta = \beta(\alpha) > 0$ such that $\alpha + \beta < 1/2$ and the property $\mathcal{P}(\alpha, \beta)$ holds. Let $\tau$ be an arbitrarily fixed real number with $\alpha + \beta < \tau < 1/2$. Then it holds that
\[ \left| \sum_{s \in S, t \in T} \chi(s - t) \right| \leq p^{\tau + \beta} \sqrt{|S||T|} \quad (11) \]
for every pair of $S, T \subset \mathbb{F}_p$ with $|S||T| \leq p^{\tau + \beta}$.

**Proof.** Let $S, T \subset \mathbb{F}_p$ with $|S||T| \leq p^{\tau + \beta}$. The proof is done by considering the following cases.

**Case 1.** If $|S||T| \leq p^{2\tau}$, then, by the trivial bound of $|\sum_{s \in S, t \in T} \chi(s - t)|$, we have
\[ \left| \sum_{s \in S, t \in T} \chi(s - t) \right| \leq |S||T| = \sqrt{|S||T| \cdot \sqrt{|S||T|}} \leq p^{\tau} \sqrt{|S||T|}. \]

**Case 2.** Next, suppose that $|S||T| > p^{2\tau}$ and we may assume $|S| > p^{\tau}$ without loss of generality.

**Case 2.1.** If $|T| \leq p^{\tau}$, recall that $|S| > p^{\tau} > p^{\tau+\beta} > p^\alpha$, by the assumption that the property $\mathcal{P}(\alpha, \beta)$ holds for $S$ and $T$, that is,
\[ \left| \sum_{s \in S, t \in T} \chi(s - t) \right| \leq p^{-\beta} |S||T|. \]

Together with the assumption that $|S|, |T| \leq p^{\tau + \beta}$, we have
\[ \left| \sum_{s \in S, t \in T} \chi(s - t) \right| \leq p^{-\beta} \sqrt{|S||T|} \cdot \sqrt{|S||T|} \leq p^{-\beta} \sqrt{p^{2(\tau + \beta)} \cdot |S||T|} = p^{\tau} \sqrt{|S||T|}. \]

The second key lemma generalizes [5, equation (3)] and [22, Lemma 12].

**Lemma 19.** Let $\phi_i$ be the $i$-th column of $\Phi_p^{(k)}$. Then, for each $1 \leq i \neq j \leq p$,
\[ \langle \phi_i, \phi_j \rangle = \frac{1}{p} \cdot G_k(a_i - a_j) = \frac{1}{p} \sum_{h=1}^{k-1} \chi_k^h(a_i - a_j) G_k^h(\chi_k^h). \quad (12) \]

**Proof.** Recall that $R_p^{(k)} = \{b_1, b_2, \ldots, b_{p-1}/k\}$ is the set of all non-zero $k$-th powers of $\mathbb{F}_p$. Note that for every $1 \leq l \leq p-1$, the equation $X^k \equiv b_l \pmod{p}$ has exactly $k$ distinct non-zero solutions; see e.g. [6, p.11 and Lemma 10.4.1]. Then we have
\[ \langle \phi_i, \phi_j \rangle = \frac{1}{p} \cdot \frac{k}{p} \sum_{l=1}^{p-1} \psi((a_i - a_j)b_l) \]
\[ = \frac{1}{p} \cdot \frac{k}{p} \cdot \frac{1}{k} \sum_{x \in \mathbb{F}_p} \psi(a_i - a_j)x^k \]
\[ = \frac{1}{p} \sum_{x \in \mathbb{F}_p} \psi((a_i - a_j)x^k) = \frac{1}{p} \cdot G_k(a_i - a_j), \]
which, together with Lemma 6, proves the lemma.

$\Box$
B. Proof of Theorem 16

Proof of Theorem 16. Suppose that Conjecture 8 holds. Then for each 0 < α < 1/2 and each prime p > p(α), there exists some β = β(α) > 0 such that the property $P(\alpha, \beta)$ holds for any non-trivial multiplicative character of $\mathbb{F}_p$.

Now fix 0 < α < 1/2 arbitrarily. If α + 2β < 1/2 holds, we may take $\beta_0 = \beta$. If α + 2β ≥ 1/2, choose $\beta_0 < \beta$ so that $\alpha + 2\beta_0 < 1/2$; note that the property $P(\alpha, \beta)$ implies the weaker property $P(\alpha, \beta_0)$ since $\beta_0 < \beta$. Now take real numbers $\varepsilon_1$ and $\varepsilon_2$ with $0 \leq \varepsilon_1 < \varepsilon_2 < \beta_0$. Let $p > p(\alpha)$ be a prime such that there exists a factor $k$ of $p - 1$ with $p^{\varepsilon_1} < k < p^{\varepsilon_2}$, which is possible by Theorem 10. Pick a real number $\tau$ with $\max\{\alpha + \beta_0, (1 - \varepsilon_1)/2 - \beta_0\} < \tau < 1/2 - \varepsilon_2$; recall Remark 17.

It suffices to prove that the matrix $\Phi_p^{(k)}$ satisfies the $(p^{\tau + \beta_0}, (k - 1)p^{\tau - 1/2})$-flat RIP. Since if this is true, Proposition 12 shows that $\Phi_p^{(k)}$ has the $(K, \delta)$-RIP with $K = p^{\tau + \beta_0}$ and $\delta = 150 \cdot (k - 1)p^{-1/2} \cdot \log(p^{\tau + \beta_0})$, implying that $\delta = O(p^{\tau + \varepsilon_2 - 1/2 + o(1)})$ since $k < p^{\varepsilon_2}$. This gives the desired conclusion in Theorem 16.

To that end, recall that $\phi_i$ is the $i$-th column of $\Phi_p^{(k)}$ and $\chi_k$ is a non-trivial multiplicative character of $\mathbb{F}_p$ of order $k$. For every pair of disjoint subsets $I, J \subseteq \{1, \ldots, p\}$, we have

\[
\left| \sum_{i \in I} \phi_i, \sum_{j \in J} \phi_j \right| \leq \frac{1}{p} \cdot \left| \sum_{k \in I \cup J} \chi_k^{-1}(a_i - a_j)G_\chi^h(a_i - a_j) \right| \\
\leq \frac{1}{p} \cdot \left| \sum_{k = 1}^{k - 1} G_\chi^h(a_i - a_j) \right| \cdot \left| \sum_{k = 1}^{k - 1} \chi_k^{-1}(a_i - a_j) \right| \\
= \frac{1}{\sqrt{p}} \cdot \left| \sum_{h = 1}^{k - 1} \chi_k^{-1}(a_i - a_j) \right|,
\]

where the first equality follows from Lemma 19; the inequality follows from the triangle inequality; and the last equality follows from Lemma 7. Recall that $\chi_k^{-1}$ is a non-trivial multiplicative character of $\mathbb{F}_p$ for every $1 \leq h \leq k - 1$. Since the condition 2) implies that $\alpha + \beta_0 < 1/2$, if $|I|, |J| \leq p^{\tau + \beta_0}$, then (14) together with Lemma 18 yields

\[
\left| \sum_{i \in I} \phi_i, \sum_{j \in J} \phi_j \right| \leq \frac{1}{\sqrt{p}} \cdot (k - 1) \cdot p^{\tau - 1/2} \sqrt{|I||J|} \\
= (k - 1) \cdot p^{\tau - 1/2} \sqrt{|I||J|}.
\]

Therefore $\Phi_p^{(k)}$ has the $(p^{\tau + \beta_0}, (k - 1)p^{\tau - 1/2})$-flat RIP. This completes the proof.

Acknowledgement

The authors are grateful to Professor Igor Shparlinski for his constructive comments and pointing out the references [13], [15], [24], [25], [26]. The authors express their sincere thanks to the anonymous reviewers for their valuable comments and suggestions. S. Satake has been supported by Grant-in-Aid for JSPS Fellows 20J00469 of the Japan Society for the Promotion of Science.

References

[1] M. Agrawal, N. Kayal and N. Saxena, “PRIMES is in P”, Ann. of Math. (2), vol. 160, no. 2, pp. 781–793, 2004.
[2] A. Arian and O. Yilmaz, “RIP constants for deterministic compressed sensing matrices-beyond Gershgorin”, arXiv:1911.07428, 2019.
[3] A. S. Bandeira, E. Dobriban, D. G. Mixon and W. F. Sawin, “Certifying the restricted isometry property is hard”, IEEE Trans. Inf. Theory, vol. 59, no. 6, pp. 3448–3450, June 2013.
[4] A. S. Bandeira, M. Fickus, D. G. Mixon and P. Wong, “The road to deterministic matrices with the restricted isometry property”, J. Fourier Anal. Appl., vol. 19, no. 6, pp. 1123–1149, 2013.
[5] A. S. Bandeira, D. G. Mixon and J. Moreira, “A conditional construction of restricted isometries”, Int. Math. Res. Not. IMRN, no. 2, pp. 372–381, 2017.
[6] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, John Wiley & Sons, Inc., 1998.
[7] J. Bourgain, S. Dilyworth, K. Ford, S. Konyagin and D. Kutzarova, “Explicit constructions of RIP matrices and related problems”, Duke Math. J., vol. 159, no. 1, pp. 145–185, 2011.
[8] E. Candès, “The restricted isometry property and its implications for compressed sensing”, C. R. Acad. Sci. Paris, Ser. I, vol. 346, no. 9-10, pp. 589–592, 2008.
[9] M.-C. Chang, “On a question of Davenport and Lewis and new character sums in finite fields”, Duke Math. J., vol. 145, no. 3, pp. 409–442, 2008.
[10] E. Chattopadhyay and D. Zuckerman, “New extractors for interleaved sources”, Proceeding of 31st Conference on Computational Complexity (CCC 2016), 2016.
[11] F. R. K. Chung, “Several generalizations of Weil’s sums”, J. Number Theory, vol. 49, no. 1, pp. 95–106, 1994.
[12] P. Erdős and L. Moser, “On the representation of directed graphs as unions of orderings”, Magyar Tud. Akad. Mat. Kutató Int. Közl., vol. 9, pp. 125–132, 1964.
[13] K. Ford, “The distribution of integers with a divisor in a given interval”, Ann. of Math. (2), vol. 168, no. 2, pp. 367–433, 2008.
[14] A. M. Guloğlu and M. R. Murty, “The Paley graph conjecture and Diophantine m-tuples”, J. Combin. Theory Ser. A, vol. 170, 105155, 2020.
[15] B. Hanson, “Estimates for character sums with various convolutions”, Acta Arith., vol. 179, no. 2, pp. 133–146, 2017.
[16] A. A. Karatsuba, “Arithmetic problems in the theory of Dirichlet characters”, Russian Math. Surveys, vol. 65, no. 4, pp. 641–690, 2008.
[17] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994.
[18] W. Lu, W. Li, K. Kpalma and J. Ronsin, “Compressed sensing performance of random Bernoulli matrices with high compression ratio”, IEEE Signal Process. Lett., vol. 22, no. 8, pp. 1074–1078, Aug. 2015.
[19] D. G. Mixon, “Deterministic RIP matrices: Breaking the square-root bottleneck”, Short, Fat Matrices (weblog).
[20] D. G. Mixon, “Explicit matrices with the restricted isometry property: breaking the square-root bottleneck”, Compressed Sensing and Its Applications, pp. 389–417, Birkhäuser/Springer, 2015.
[21] D. Ramalho, K. Melo, M. Khorasay, F. Asharif, M. S. S. Danish and C. A. Duque, “A review of deterministic sensing matrices”, Compressive Sensing in Healthcare, pp. 89–110, Academic Press, 2020.
[22] S. Satake, “On the restricted isometry property of the Paley matrix”, arXiv:2011.02907, 2020.
[23] I. D. Shkredov, “Sumsets in quadratic residue”, Acta Arith., vol. 164, no. 3, pp. 221–243, 2014.
[24] I. E. Shparlinski, Additive decompositions of subgroups of finite fields, SIAM J. Discrete Math., vol. 27, no. 4, pp. 1870–1879, 2013.
[25] A. S. Volostnov, “On double sums with multiplicative characters”, Math. Notes, vol. 104, no. 1-2, pp. 197–203, 2018.
[26] A. S. Volostnov, I. D. Shkredov, “Sums of multiplicative characters with additive convolutions”, Proc. Steklov Inst. Math., vol. 296, no. 1, pp. 256–269, 2017.
[27] L. R. Welch, “Lower bounds on the maximum cross correlation of signals”, IEEE Trans. Inf. Theory, vol. 20, no. 3, pp. 397–399, May 1974.
[28] D. Zuckerman, Computing Efficiently Using General Weak Random Sources, Ph.D. dissertation, University of California at Berkeley, US, 1991.