Explicit universal sampling sets in finite vector spaces
Lucia Morotti

Abstract
In this paper we construct explicit sampling sets and present reconstruction algorithms for Fourier signals on finite vector spaces $G$, with $|G| = p^r$ for a suitable prime $p$. The two sampling sets have sizes of order $O(pt^2 r^2)$ and $O(pt^2 r^3 \log(p))$ respectively, where $t$ is the number of large coefficients in the Fourier transform. The algorithms approximate the function up to a small constant of the best possible approximation with $t$ non-zero Fourier coefficients. The fastest of the algorithms has complexity $O(p^2 t^2 r^3 \log(p))$.

1 Introduction

The problem of compressive sensing originated in the context of Fourier series [3]. The aim is to reconstruct a linear combination of a small number of complex exponentials from as few samples as possible, when only the number of the exponentials entering the linear combination is known. The additional challenge was to come up with practical and efficient methods for the reconstruction (which by its combinatorial nature is NP-hard, unless extra information is available).

Later on, the compressed sensing problem evolved to include a more general setup. The overall problems and main challenges, however, remained the same; and they concerned mostly the construction of sampling schemes that would allow (and guarantee) efficient reconstruction from as few measurements as possible, and the design of efficient reconstruction algorithms. For the latter, $\ell^1$-minimization turned out to be a popular choice, and the chief technical condition to guarantee success for the reconstruction method was the restricted isometry condition (see [4] for the first introduction of these ideas, and [6] for an in-depth study). However, there still remained the problem of constructing measurement matrices (or, in the Fourier case, sampling sets) for which the RIP was actually provably fulfilled. An important (somewhat partial) answer to this problem was provided by random methods; e.g., in the case of random sampling of Fourier matrices the RIP assumption turns out to be true under rather weak assumptions on the number of samples [12], at least with high probability.

However, the case of deterministic sampling sets with provably guaranteed reconstruction poses altogether different challenges. Firstly, the verification of properties like RIP is a very complex problem by itself [13], hence special care must be taken to allow such estimates. A first successful example for a
A deterministic construction with the RIP property was presented by DeVore [5]. For the Fourier setting, in [1] sampling sets and inversion algorithms were constructed for cyclic groups; an alternative construction of deterministic sampling sets guaranteeing RIP for the cyclic case was developed in [7]. All these constructions have a common restriction, commonly known as quadratic bottleneck: In order to reconstruct linear combinations of \( t \) basis vectors, they need \( O(t^2) \) samples. A more recent paper by Bourgain and collaborators [2] managed to improve this to \( O(t^2 - \epsilon) \), for a very small \( \epsilon > 0 \), using rather involved arguments from additive combinatorics.

This paper considers efficiently sampling Fourier-sparse vectors on finite abelian groups. It can be seen as complementary to [1, 7, 8], with the main difference being that this paper focuses on finite vector spaces rather than cyclic groups. We develop a general, simple scheme for the design of sampling sets, together with algorithms that allow reconstruction.

Hence the new methods provide an alternative means of explicitly designing universal sampling sets in a specific family of finite abelian groups \( G \), i.e., sampling sets \( \Omega \subset G \) that allow the reconstruction of any given linear combination of \( t \) characters of \( G \) from its restriction on \( \Omega \), together with explicit inversion algorithms, both for the noisy and noise free cases. The groups \( G \) we consider are finite vector spaces, and the sampling sets will be written as unions of suitable affine subspaces. The sampling sets actually fulfill the RIP property, which allows one to use the standard methods such as \( \ell^1 \)-minimization. However, the special structure of the sampling set makes the inversion algorithm particularly amenable to the use of a more structured (and potentially faster) reconstruction algorithm, using FFT methods. It should be stressed, though, that our construction is not able to beat the quadratic bottleneck.

### 2 Notation

Let \( p \) be a prime and \( r \) a positive integer. When considering their additive groups structure we have that \((\mathbb{Z}/p\mathbb{Z})^r \cong \mathbb{F}_p^r\). The vector space structure of \( \mathbb{F}_p^r \) will enable us to construct the sampling sets needed in the algorithms described in this paper. We will write \( \mathbb{F}_p^r \) also when considering only its additive group structure. Also in order to avoid complicated notations we will identify, where needed, elements of \( \mathbb{Z} \) with their images in \( \mathbb{F}_p \), so that for example 1 could be viewed as either an element of \( \mathbb{Z} \) or of \( \mathbb{F}_p \).

We will write \( H \leq G \) for a subgroup \( H \) of \( G \). Subsets of \( \mathbb{F}_p^r \) are subgroups if and only if they are vector spaces (since \( \mathbb{F}_p \) is a field of prime order). So when looking at \( \mathbb{F}_p^r \) as a vector space we will write \( H \leq \mathbb{F}_p^r \) for a subspace.
For any subgroup $H \leq G$ we will also write $\text{Rep}(G/H)$ for a set of representatives of cosets of $H$ in $G$.

In Section 4 we will also be working with both $\mathbb{F}_p$ and $\mathbb{F}_q$, where $q$ is a power of $p$. Since vector spaces over $\mathbb{F}_q$ can be viewed also as vector spaces over $\mathbb{F}_p$, we will write $\dim_{\mathbb{F}_p}(V)$ and $\dim_{\mathbb{F}_q}(V)$ for the dimension of $V$ as a vector space over $\mathbb{F}_p$ or $\mathbb{F}_q$ respectively. Similarly we will write $\text{span}_{\mathbb{F}_p}(A)$ and $\text{span}_{\mathbb{F}_q}(A)$ for the span of $A$ as vector space over $\mathbb{F}_p$ or $\mathbb{F}_q$ respectively.

Let $\hat{\mathbb{F}}_r^p$ consist of all group homomorphisms $\mathbb{F}_r^p \to \mathbb{C}$. We have that $\hat{\mathbb{F}}_r^p = \{ \chi(y_1, \ldots, y_r) : y_i \in \mathbb{F}_r^p \} = \{ \chi_{y_1, \ldots, y_r} : y \in \mathbb{F}_r^p \}$, where, if $\omega_p = e^{2\pi i/p}$, we define

$$\hat{\chi}_{y_1, \ldots, y_r}(x_1, \ldots, x_r) = \omega_p^{y_1x_1 + \ldots + y_rx_r}$$

for $(x_1, \ldots, x_r) \in \mathbb{F}_r^p$. This is well defined since $\omega_p^p = 1$. Also it is easy to check that $\chi_{y+z}(x) = \chi_y(x) \chi_z(x)$ for $y, z \in \mathbb{F}_r^p$.

For any function $f : (\mathbb{Z}/p\mathbb{Z})^r \to \mathbb{C}$ let $\hat{f} : \hat{\mathbb{F}}_r^p \to \mathbb{C}$ be its Fourier transform, so that

$$f = \sum_{\chi_y \in \hat{\mathbb{F}}_r^p} \hat{f}(\chi_y) \chi_y.$$ 

Formulas for the Fourier transform for $\mathbb{F}_r^p$ are given by

$$\hat{f}(\chi_y) = \frac{1}{p^r} \sum_{x \in \mathbb{F}_r^p} f(x) \chi_y(x)^{-1}.$$ 

Under the bijection $\chi_y \leftrightarrow y$ this corresponds (up to a scalar multiple) to the usual discrete Fourier transform on the grid $\{0, 1, \ldots, p-1\}^r$ (under the identification of this grid with $\mathbb{F}_r^p$).

For any function $h : X \to Y$ and any subset $Z \subseteq X$ let $h|_Z : Z \to Y$ be the restriction of $h$ to $Z$.

Let now $t$ be a positive integer and assume that $\hat{f} = \hat{g} + \epsilon$ with $\hat{g}$ having support consisting of at most $t$ elements and with $\|\epsilon\|_1$ “small”. We will present in this paper two algorithms which approximate $\hat{f}$ by a function $\hat{f}'$ which, like $\hat{g}$, also has support consisting of at most $t$ elements. Further $\hat{f}'$ satisfies

$$\|\hat{f} - \hat{f}'\|_1 \leq (1 + 3\sqrt{2})\|\epsilon\|_1,$$

that is $\hat{f}'$ is close to the best possible such approximation of $\hat{f}$. In particular if $\|\epsilon\|_1 = 0$ then $\hat{f}' = \hat{f}$, so that the algorithms reconstruct $\hat{f}$ (and then also $f$) in this case.

The algorithms presented here are based on similar algorithms presented in [1, 8] for the group of unit length elements of $\mathbb{C}$. As in [1, 8] sampling sets
will be obtained by taking unions of cosets of subgroups. In [1, 8] subgroups of distinct prime orders are considered. This cannot be applied here since \( F_p \) is a \( p \)-group. However, using the vector space structure of \( F_p \), we can construct many small subgroups with certain “orthogonality” properties (as will be seen in the next section), which will be used to construct the sampling sets presented here.

### 3 Complexities of sets and algorithms

Before describing the sampling sets and the corresponding algorithms, we present their size/running time complexities and compare them to those presented in other papers.

| (Size of) group | Sampling set | Time complexity |
|-----------------|--------------|-----------------|
| Theorem 10 \( F_p \) | \( O(p \cdot t^2 \cdot r^2) \) | \( O(p \cdot t^2 \cdot r^2) \) |
| Theorem 12 \( F_p \) | \( O(p \cdot t^2 \cdot r^3 \cdot \log(p)) \) | \( O(p \cdot t^2 \cdot r^3 \cdot \log(p)) \) |
| Algorithm 1 of [1] \( \mathbb{Z}/n\mathbb{Z} \) | \( O(t^2 \cdot \log^2(n/t)) \) | \( O(t^2 \cdot \log^2(n/t)) \) |
| Section 2 of [2] \( \mathbb{Z}/p\mathbb{Z} \) | \( O(t^2 \cdot \log(t \cdot \log(n))) \) | \( O(t^2 \cdot \log(t \cdot \log(n))) \) |
| Section 3 of [5] \( n \) | \( O(t^2 \cdot \log(n/t) \cdot \log(t \cdot \log(n))^3) \) | \( O(n \cdot t^2 \cdot \log(n/t) \cdot \log(t \cdot \log(n))^3) \) |
| Section 2 of [7] \( \mathbb{Z}/p\mathbb{Z} \) | \( \Omega(t^2) \) | \( \Omega(t^2) \) |
| Algorithm 1 of [8] \( \mathbb{Z}/n\mathbb{Z} \) | \( O(t^2 \cdot \log(n)^2) \) | \( O(n \cdot t \cdot \log(n)^2) \) |
| Algorithm 2 of [8] \( \mathbb{Z}/n\mathbb{Z} \) | \( O(t^2 \cdot \log(n)^4) \) | \( O(t^2 \cdot \log(n)^4) \) |

As can be seen from the table, the second algorithm presented here needs more sampling points than the first one (it needs about \( r \cdot \log(p) = \log(|F_p|) \) times as many sampling points). However the first algorithm has a factor \( p^r = |F_p| \) in its running time, while the second algorithm is much faster.

The complexities for the construction of the sampling sets used in Theorem 10 and 12 are given as follows.

| Time complexity for the construction of the sampling set |
|--------------------------------------------------------|
| Theorem 10 | \( O(p \cdot t^2 \cdot r^3 \cdot \log(p)^2) \) |
| Theorem 12 | \( O(p \cdot t^2 \cdot r^3 \cdot \log(p)^3) \) |

### 4 Construction of the sampling sets

The sets constructed here are unions of (shifted) subspaces of \( F_p \). We begin with a lemma that will allow us to find certain families of subspaces which will be of basic importance for the construction of our sampling sets.
Lemma 1. Let $p$ be a prime. Also let $1 \leq h \leq r$ be integer and define $q := p^h$ and $s := \lceil r/h \rceil$. Let $\pi : \mathbb{F}_q^s \to \mathbb{F}_p^r$ be a surjective homomorphism and fix $a_1, \ldots, a_n \in \mathbb{F}_q^s$. For $1 \leq i \leq n$ integer choose $H_i \leq \mathbb{F}_p^r$ of dimension $h$ containing $\pi(\text{span}_{\mathbb{F}_q}(a_i))$. Fix a positive integer $m \leq n$. If

$$\text{span}_{\mathbb{F}_q}(a_1, \ldots, a_m) = \mathbb{F}_q^s$$

for every $1 \leq i_1 < \ldots < i_m \leq n$ then

$$\text{span}_{\mathbb{F}_p}(H_{i_1}, \ldots, H_{i_m}) = \mathbb{F}_p^r$$

for every $1 \leq i_1 < \ldots < i_m \leq n$.

In the lemma $\{a_{i_1}, \ldots, a_{i_m}\}$ is a subset of $\{a_1, \ldots, a_n\}$ with $m$ elements. Also, if $z$ is a primitive element of $\mathbb{F}_q$, so that elements of $\mathbb{F}_q$ can be written as $b_0 + b_1 z + \ldots + b_{h-1} z^{h-1}$ with $b_i \in \mathbb{F}_p$, we can take $\pi : \mathbb{F}_q^s \to \mathbb{F}_p^r$ to be the composition of $\pi_1 : \mathbb{F}_q^s \to \mathbb{F}_p^{hs}$ and $\pi_2 : \mathbb{F}_p^{hs} \to \mathbb{F}_p^r$ given as follows

$$\pi_1(\sum b_i^{(1)} z^i, \ldots, \sum b_i^{(s)} z^i) := (b_0^{(1)}, \ldots, b_{h-1}^{(1)}, \ldots, b_0^{(s)}, \ldots, b_{h-1}^{(s)}),$$

$$\pi_2(c_1, \ldots, c_{hs}) := (c_1, \ldots, c_r).$$

If $\pi(\text{span}_{\mathbb{F}_q}(a_i))$ has dimension $h$ as vector space over $\mathbb{F}_p$, then we have to take $H_i = \pi(\text{span}_{\mathbb{F}_q}(a_i))$. If $\pi(\text{span}_{\mathbb{F}_q}(a_i))$ has dimension less than $h$ as vector space over $\mathbb{F}_p$, then we can choose $H_i = \text{span}_{\mathbb{F}_p}(\pi(\text{span}_{\mathbb{F}_q}(a_i)), e_1, \ldots, e_j)$ for a certain $1 \leq j \leq r$ (here $e_k$ is the $k$-th standard basis element of $\mathbb{F}_p^r$).

Proof. Notice that a surjective homomorphism $\pi : \mathbb{F}_q^s \to \mathbb{F}_p^r$ always exists since, as $\mathbb{F}_p$-vector spaces,

$$\mathbb{F}_p^r \leq \mathbb{F}_p^{hs} \cong \mathbb{F}_q^s.$$ 

In particular $\dim_{\mathbb{F}_p}(\mathbb{F}_p^r) \leq \dim_{\mathbb{F}_q}(\mathbb{F}_q^s)$. Also we can construct $H_i$, as

$$\dim_{\mathbb{F}_p}(\pi(\text{span}_{\mathbb{F}_q}(a_i))) \leq \dim_{\mathbb{F}_p}(\text{span}_{\mathbb{F}_q}(a_i)) = h \dim_{\mathbb{F}_q}(\text{span}_{\mathbb{F}_q}(a_i)) \leq h.$$

If $\text{span}_{\mathbb{F}_q}(a_1, \ldots, a_m) = \mathbb{F}_q^s$ then

$$\mathbb{F}_p^r \geq \text{span}_{\mathbb{F}_p}(H_{i_1}, \ldots, H_{i_m}) \geq \pi(\text{span}_{\mathbb{F}_q}(a_1, \ldots, a_m)) = \pi(\mathbb{F}_q^s) = \mathbb{F}_p^r$$

and so the lemma follows. \(\square\)

If some subspaces $H_1, \ldots, H_n$ of $\mathbb{F}_p^r$ satisfy $\text{span}_{\mathbb{F}_p}(H_{i_1}, \ldots, H_{i_m}) = \mathbb{F}_p^r$ for every $1 \leq i_1 < \ldots < i_m \leq n$, we say that $H_1, \ldots, H_n$ are $m$-generating. Similarly, if $a_1, \ldots, a_n \in \mathbb{F}_q^s$ satisfy $\text{span}_{\mathbb{F}_q}(a_{i_1}, \ldots, a_{i_m}) = \mathbb{F}_q^s$ for every $1 \leq i_1 < \ldots < i_m \leq n$, we say that $a_1, \ldots, a_n$ are $m$-generating.
$i_1 < \ldots < i_m \leq n$, we say that $\{a_1, \ldots, a_n\}$ is $m$-generating. For $m = s$ we have that $\{a_1, \ldots, a_n\} \subseteq \mathbb{F}_q^s$ is $s$-generating if and only if any $s$ of its elements are linearly independent. So a subset of $\mathbb{F}_q^s$ is $s$-generating if and only if it has full spark.

It is not always possible to construct a $m$-generating subset of $\mathbb{F}_q^s$ of size $n$, for any $n$. We will in the next lemma show though that $\mathbb{F}_q^s$ has a $s$-generating multiset for $\mathbb{F}_q^s$ of size $q + 1$ (we will consider multisets and not sets in order to cover also the case $s = 1$) and construct one such multiset explicitly.

**Lemma 2.** Let

$$A := \{(1, x, \ldots, x^{s-1}) : x \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1) \in \mathbb{F}_q^s\}.$$  

Then $A \subseteq \mathbb{F}_q^s$ is $s$-generating and $|A| = q + 1$.

**Proof.** It’s clear that $|A| = q + 1$. For the proof of $A$ being $s$-generating see the beginning of Chapter 11 §5 of [9]. This can also be seen by noticing that the matrices obtained from any $s$ distinct elements of $A$ all have one of the following forms (up to exchanging rows):

$$\begin{pmatrix}
1 & x_1 & \cdots & x_1^{s-1} \\
\vdots & \vdots & & \vdots \\
1 & x_s & \cdots & x_s^{s-1}
\end{pmatrix} \quad \text{or} \quad \begin{pmatrix}
1 & x_1 & \cdots & x_1^{s-2} & x_1^{s-1} \\
\vdots & \vdots & & \vdots & \vdots \\
1 & x_{s-1} & \cdots & x_{s-1}^{s-2} & x_{s-1}^{s-1} \\
0 & 0 & \cdots & 0 & 1
\end{pmatrix}$$

with distinct $x_j$ and so such matrices are invertible. \(\Box\)

In order to construct one of the two sampling sets needed in the algorithms, we still need a stable sampling set for 1-sparse Fourier signals on $\mathbb{F}_p$. We will show in the next lemma how such a set can be found. In the same lemma we will also give an algorithm which, applied to the function $f(x) = \sum_{y=0}^{p-1} a_y \omega_y^x$, under certain assumptions on $f$, returns $y'$ with $|a_{y'}|$ maximal. In order to state the theorem we need the following definition.

**Definition 3.** For $d > 0$ and $x \in \mathbb{R}$ let $|x|_d := \text{dist}(x, d\mathbb{Z})$ be the minimum distance of $x$ from an integer multiple of $d$.

**Lemma 4.** Let $K := \{0\} \cup \{2^i : 0 \leq i \leq k \text{ and } i \in \mathbb{Z}\} \subseteq \mathbb{F}_p$, where $k \in \mathbb{Z}$ is minimal such that $2^k \geq p/3$. Let $f(x) = \sum_{y=0}^{p-1} a_y \chi_y(x)$. If there exists $y'$ such that $|a_{y'}| > 2 \sum_{y \neq y'} |a_y|$, then the following algorithm returns $y'$.

Set $b(2^l) := \arg(f(2^l)/f(0))$, for $0 \leq l \leq k$ (if $f(2^l)$ or $f(0)$ are zero set $b(2^l) := 0$).

Set $e := (0, \ldots, 0)$ (Length$(e) = p$).
for \( l \) from 0 to \( k \) do
for \( j \) from 0 to \( p-1 \) do
if \( e(j+1) = 0 \) and \( |p b(2^l)/(2\pi) - 2^l j|_p \geq p/6 \) then
\( e(j+1) := 1 \)
end if
end for
return the index \( j \) such that \( e(j+1) = 0 \). If such a \( j \) does not exist, return 0.

Proof. If no \( y' \) exists then there is nothing to prove, so we will now assume that there exists \( y' \) with \( |a_{y'}| > 2 \sum_{y\neq y'} |a_y| \). Then, for \( x \in \mathbb{F}_p \), we have that

\[
\left| \sum_{y\neq y'} a_y \chi_y(x) \right| = \left| \sum_{y\neq y'} a_y \omega_p^{y y'} \right| \leq \sum_{y\neq y'} |a_y \omega_p^{y y'}| = \sum_{y\neq y'} |a_y| < |a_{y'}|/2
\]

and so

\[
|f(x)| = \sum_{y=0}^{p-1} a_y \chi_y(x) = \sum_{y=0}^{p-1} a_y \omega_p^{y y'} \geq |a_{y'} \omega_p^{y y'}| - \sum_{y\neq y'} |a_y \omega_p^{y y'}| > |a_{y'}|/2 \geq 0.
\]

So \( f(x) \neq 0 \) for every \( x \in \mathbb{F}_p \). In particular \( b(2^l) = \text{arg}(f(2^l)/f(0)) \).

For \( z \in \mathbb{C} \) with \( |z| < 1/2 \) we have that \( |\text{arg}(1+z)|_{2\pi} < \pi/6 \). It then follows that

\[
|\text{arg}(f(x)) - \text{arg}(a_{y'} \omega_p^{y y'})|_{2\pi} = |\text{arg}(f(x)/(a_{y'} \omega_p^{y y'}))|_{2\pi} < \pi/6
\]

and so

\[
|\text{arg}(f(x)/f(0)) - \text{arg}(\omega_p^{y y'})|_{2\pi} = |\text{arg}(f(x)) - \text{arg}(f(0)) - \text{arg}(a_{y'} \omega_p^{y y'}) + \text{arg}(a_{y'})|_{2\pi}
\]

\[
\leq |\text{arg}(f(x)) - \text{arg}(a_{y'} \omega_p^{y y'})|_{2\pi}
\]

\[
+ |\text{arg}(f(0)) - \text{arg}(a_{y'})|_{2\pi}
\]

\[
< \pi/3
\]

for every \( x \in \mathbb{F}_p \). Then

\[
|p b(2^l)/(2\pi) - 2^l y'|_p = |p/(2\pi)(\text{arg}(f(2^l)/f(0)) - \text{arg}(\omega_p^{2^l y'}))|_p
\]

\[
= p/(2\pi) |\text{arg}(f(2^l)/f(0)) - \text{arg}(\omega_p^{2^l y'})|_{2\pi}
\]

\[
< p/6
\]
for $0 \leq l \leq k$, in particular $e(y' + 1) = 0$.

We will now show that if $y \neq y'$ then $e(y + 1) = 1$, which will then prove the lemma. In order to do this we will show that if $j \neq 0$ then there exists $l$ such that $0 \leq l \leq k$ and $|2^l j|_p \geq p/3$, which also proves that if $y \neq y'$ then there exists $l$, $0 \leq l \leq k$, with $|2^l (y' - y)|_p \geq p/3$. Hence, for the same $l$ we have that

$$|pb(2^l)/(2\pi) - 2^l y|_p \geq |2^l (y' - y)|_p - |pb(2^l)/(2\pi) - 2^l y'|_p \geq p/3 - p/6 = p/6.$$  

Assume that $j \neq 0 \mod p$ and that $|2^l j|_p < p/3$ for all $0 \leq l \leq k$. Then, up to a multiple of $p$, we also have that $j \in \pm \{1, \ldots, [p/3] - 1\}$ (by considering the case $l = 0$). As $|2^l j|_p = |2^l (-j)|_p$ we can assume that $j \in \{1, \ldots, [p/3] - 1\}$. Let $l$ be minimal such that $2^l j \geq p/3$. As $1 \leq j < p/3$ we have that $1 \leq l \leq k$ by definition of $k$. As $1 \leq 2^{(l-1)} j < p/3$ it follows that $p/3 \leq 2^l j < 2p/3$ and so $|2^l j|_p \geq p/3$. Since $1 \leq l \leq k$ this gives a contradiction and so the lemma is proved.

We will now construct the sampling sets which will be used in the algorithms presented in the next section.

**Definition 5.** Let $m \geq 1$ and $n := 4t(m - 1) + 1$ and let $H_1, \ldots, H_n \leq \mathbb{F}_p$ be $m$-generating and all of dimension $h$ with $1 \leq h \leq r$. Also let $K \subset \mathbb{F}_p$ be as in Lemma 4. For $1 \leq i \leq n$ choose $x_{1,i}, \ldots, x_{r-h,i} \in \mathbb{F}_p$ such that span$_p \{H_i, x_{1,i}, \ldots, x_{r-h,i}\} = \mathbb{F}_p$. The wanted sets are

$$\Gamma_1 := \cup_i H_i,$$
$$\Gamma_2 := \cup_i (H_i + \{kx_{i,j} : k \in K, 1 \leq j \leq r - h\}),$$

where for sets $A$ and $B$ we define $A + B := \{a + b : a \in A, b \in B\}$.

**Remarks 6.** From Lemmas 7 and 8, $m$-generating $H_1, \ldots, H_n$ exist if $m = \lceil r/h \rceil$ and $4t(\lceil r/h \rceil - 1) \leq p^h$. Also $x_{1,i}, \ldots, x_{r-h,i}$ exists for $1 \leq i \leq n$ as $H_i$ is of dimension $h$.

It can be easily checked from the definitions that

$$|\Gamma_1| \leq np^h,$$
$$|\Gamma_2| \leq np^h |K|(r - h).$$

We will now bound $np^h$ and $|K|$.

**Theorem 7.** Let $h \in \mathbb{Z}$ be minimal such that $h \geq 1$ and $4t(\lceil r/h \rceil - 1) \leq p^h$ and let $K$ as in Lemma 4. Also let $n := 4t(\lceil r/h \rceil - 1) + 1$. Then $np^h < 16pt^2r^2$ and $|K| \leq 2 + \log_2(p)$.  

\[8\]
Proof. Notice that $h \leq r$, since $4t(\lceil r/r \rceil - 1) = 0 \leq p^r$

If $h = 1$ we have that $np^h \leq (4t(r - 1) + 1)p \leq 4ptr < 16pt^2r^2$.

If $h > 1$ then $p^{h-1} < 4t(\lceil r/(h - 1) \rceil - 1) < 4tr$ and so

$$np^h \leq pp^{h-1} \left(4t \left(\left\lceil \frac{r}{h} \right\rceil - 1\right) + 1\right) < p \cdot 4tr \cdot \left(\frac{4tr}{h} + 1\right) \leq 16pt^2r^2.$$  

When looking at $|K|$, we have that $|K| = 2 + k$, where $k \in \mathbb{Z}$ is minimal such that $2^k \geq p/3$. So $2^k < 2p/3$ and then $k < \log_2(2p/3) < \log_2(p)$. \[\Box\]

From Remark 8 and Theorem 7 we obtain bounds on $|\Gamma_1|$ and $|\Gamma_2|$.

**Remarks 8.** From Remark 6 and Theorem 7 we obtain that $\Gamma_1$ and $\Gamma_2$ can be chosen with

$$|\Gamma_1| \leq 16pt^2r^2,$$

$$|\Gamma_2| \leq 16pt^2r^3(2 + \log_2(p)).$$

We still need to prove that the sampling sets constructed in Definition 5 are actually sampling sets. This will be done in the next section by proving that the reconstruction algorithms which will be presented work. Since the reconstruction algorithms need values $f(x)$ with $x \in \Gamma_1$ or $x \in \Gamma_2$ respectively, this will also prove that the given sets are sampling sets. An alternative way would be to prove that $\Gamma_1$ and $\Gamma_2$ satisfy the RIP property (see Section 8 for remarks about it).

### 5 Preliminaries to the reconstruction algorithms

We will now prove a lemma which will play a crucial role in the two reconstruction algorithms we will present in Section 6. For any $H \leq \hat{\mathbb{F}}_p^r$ and $L \leq \hat{\mathbb{F}}_p^r$ let $H^\perp := \{\chi_y \in \hat{\mathbb{F}}_p^r : \chi_y(h) = 1 \ \forall h \in H\}$ and $L^\perp := \{x \in \mathbb{F}_p^r : \chi_y(x) = 1 \ \forall \chi_y \in L\}$ be the annihilators of $H$ and $L$ respectively.

**Lemma 9.** Let $H_1, \ldots, H_n$ be $m$-generating with $n = 4t(m - 1) + 1$, $f = \sum \chi_y \in \mathbb{F}_p^r a_{\chi_y} \chi_y$ be a $t$-sparse Fourier function. Write $\hat{f} = \hat{\varnothing} + \epsilon$ with the support of $\hat{\varnothing}$ having at most $t$ elements. Then for every $\chi_z \in \hat{\mathbb{F}}_p^r$ we have that

$$\left\{ 1 \leq i \leq n : \sum_{\chi_y \in \chi_z H_i^\perp \setminus \{\chi_x\}} |a_{\chi_y}| \leq \frac{\|\epsilon\|_1}{t} \right\} \geq 2t(m - 1) + 1.$$
Proof. First we will show that the matrix $M$ is $(n, m-1)$-coherent, and then we will apply (a variant of) Lemma 2 of \cite{1} to conclude the proof of the lemma.

Let $M$ be the matrix with rows labeled by

$$A := \{\chi_y H_i^\perp : 1 \leq i \leq n, \; \chi_y \in \text{Rep}(\hat{F}_p/H_i^\perp)\},$$

columns labeled by elements of $\hat{F}_p$ and $M_{\chi_y H_i^\perp, \chi_z} = 1$ if $\chi_z \in \chi_y H_i^\perp$ or $M_{\chi_y H_i^\perp, \chi_z} = 0$ otherwise. Then each column of $M$ contains exactly $n$ entries equal to 1 and

$$\sum_{a \in A} M_{a, \chi_z} M_{a, \chi_w} = \sum_{i=1}^n M_{\chi_x H_i^\perp, \chi_w} = |\{1 \leq i \leq n : (\chi_z)^{-1} \chi_w \in H_i^\perp\}|$$

for $\chi_z, \chi_w \in \hat{F}_p$. Let $\langle \chi_x \rangle \subseteq \hat{F}_p$ be the subgroup generated by $\chi_x$. Since the $H_i$ are $m$-generating, so that no more than $m-1$ of them can be contained in a fixed proper subspace of $\mathbb{F}_p$, and since $\langle \chi_x \rangle^\perp \leq \mathbb{F}_p$ for $1 \neq \chi_x \in \hat{F}_p$ (that is $x \neq 0 \in \mathbb{F}_p$), we have that

$$\sum_{a \in A} M_{a, \chi_z} M_{a, \chi_w} = |\{1 \leq i \leq n : (\chi_z)^{-1} \chi_w \in H_i^\perp\}|$$

$$= |\{1 \leq i \leq n : \chi_w - z \in H_i^\perp\}|$$

$$= |\{1 \leq i \leq n : (\chi_w - z)^{-1} H_i^\perp\}|$$

$$= |\{1 \leq i \leq n : H_i \leq \langle \chi_w - z \rangle^\perp\}|$$

$$\leq m-1$$

for $\chi_z \neq \chi_w$ (that is $x \neq w$ as elements of $\mathbb{F}_p$).

Assume first that $\epsilon \neq 0$. If $h < r$ the lemma then follows from Lemma 2 of \cite{1} with (using the notation of Lemma 2 of \cite{1}) $k = t$ (we have that $t < n$ by assumption), $\epsilon' = 1$ and $c = 4$. If $h = r$ then $H_i^\perp = \{1\}$ for every $1 \leq i \leq n$ and so

$$\sum_{\chi_y \in \chi_z H_i^\perp \setminus \{\chi_z\}} |a_{\chi_y}| = 0 \leq \frac{\|\epsilon\|_1}{t}$$

for every $\chi_z \in \hat{F}_p$ and $1 \leq i \leq n$. In particular the lemma holds also in this case.

Assume now that $\epsilon = 0$. Then

$$f = \sum_{j=1}^t a_{\chi_y} \chi_y$$

10
for some $\chi_y \in \hat{F}_p$. In particular

$$\sum_{\chi_y \in \chi_z H_i^\perp \setminus \{\chi_z\}} |a_{\chi_y}| = \sum_{1 \leq j \leq m, \chi_y \neq \chi_z, \chi_y \in \chi_z H_i^\perp} |a_{\chi_y}|.$$  

Since $\chi_y \in \chi_z H_i^\perp$ if and only if $(\chi_z)^{-1} \chi_y \in H_i^\perp$ and, for each $\chi_y \neq \chi_z$, there exists at most $m - 1$ such $i$, we have that

$$\sum_{\chi_y \in \chi_z H_i^\perp \setminus \{\chi_z\}} |a_{\chi_y}| = 0$$  

for at least $n - t(m - 1) \geq 2t(m - 1) + 1$ distinct values of $i$. In particular the lemma holds also in this case. \hfill $\square$

Let $H$ be any subgroup of $\mathbb{F}_p$. Then $\mathbb{F}_p / H^\perp \cong \hat{H}$ through $\chi_y H^\perp \mapsto (h \mapsto \chi_y(h))$. For any function $f = \sum_{\chi_y \in \mathbb{F}_p} a_{\chi_y} \chi_y$ on $\mathbb{F}_p$ we have that

$$\hat{f}|_H(\chi_y H^\perp) = \sum_{\chi_z \in \chi_y H^\perp} a_{\chi_z} = \sum_{\chi_z \in \chi_y H^\perp} \hat{f}(\chi_z)$$ \hspace{1cm} (1)

since

$$f|_H = \sum_{\chi_y \in \mathbb{F}_p} a_{\chi_y} \chi_y|_H = \sum_{\chi_y H^\perp \in \mathbb{F}_p / H^\perp} \chi_y|_H \sum_{\chi_z \in \chi_y H^\perp} a_{\chi_z}.$$  

This identification will be used in the proof of the algorithms which we will present in the next section.

### 6 Reconstruction algorithms

We are now ready to present the reconstruction algorithms. Through all of this section let $f$, $g$ and $\epsilon$ be as in Section 2 and $\Gamma_j$, $H_1, \ldots, H_n$, $K$, $m$, $n$, $h$ and $x_{i,j}$ as in Definition 5. The first algorithm we present reconstructs or approximates $\hat{f}$ from $f|_{\Gamma_1}$.

**Theorem 10.** For $1 \leq j \leq n$ let $F_j$ be the Fourier transform for $H_j$ and define $c_j := F_j(f|_{H_j})$. Then the following algorithm returns $\hat{f}'$ with $|\text{supp}(\hat{f}')| \leq t$ and $\|\hat{f} - \hat{f}'\|_1 \leq (1 + 3\sqrt{2})\|\epsilon\|_1$.

Set $\hat{f} := (0, \ldots, 0)$, $\hat{f}'' := (0, \ldots, 0)$ and $Y := (0, \ldots, 0)$

for $j$ from 1 to $n$ do

for $2t - 1$ values of $\chi_y H_j^\perp$ such that $|c_j(\chi_y H_j^\perp)|$ is largest do
\begin{verbatim}
for $\chi_z \in \chi_y H_j^{\perp}$ do
    $Y(\chi_z) := Y(\chi_z) + 1$
end for
end for
end for

for $\chi_y \in \hat{F}_p$ do
    if $Y(\chi_y) > 2t(m - 1)$ then
        $X := ()$
        for $j$ from 1 to $n$ do
            Append $c_j(\chi_y H_j^{\perp})$ to $X$
        end for
        $\hat{f}''(\chi_y) := \text{Median}(\{\text{Re}(x) : x \in X\}) + i\text{Median}(\{\text{Im}(x) : x \in X\})$
    end if
end for

for $t$ values of $\chi_y$ for which $|\hat{f}''(\chi_y)|$ is largest do
    $\hat{f}'(\chi_y) := \hat{f}''(\chi_y)$
end for
return $\hat{f}'$.
\end{verbatim}

In the algorithm $\hat{f}'$, $\hat{f}''$ and $Y$ are labeled by elements of $\hat{F}_p$. The Fourier transform for $H_j$ can be defined similarly to that of $F_p$ (notice that $H_j \cong F_p$ by definition). Under the identification at the end of Section 5 giving $\hat{H}_j \cong \hat{F}_p/\hat{H}_j^{\perp}$ we can also define $F_j$ as a function $F_j : \hat{F}_p/\hat{H}_j^{\perp} \to \mathbb{C}$.

\textbf{Proof.} We will first show that if $|a_{\chi_z}| > 2\|\epsilon\|_1/t$ then $Y(\chi_z) > 2t(m - 1)$ and next prove that if $Y(\chi_w) > 2t(m - 1)$ then $|\hat{f}''(\chi_w) - a_{\chi_w}| \leq \sqrt{2}\|\epsilon\|_1/t$. Using these results we will then prove the theorem.

By definition of $\epsilon$, for $1 \leq j \leq n$ we have that
\begin{equation}
|\{\chi_y H_j^{\perp} \in \hat{F}_p/\hat{H}_j^{\perp} : |c_j(\chi_y H_j^{\perp})| > \|\epsilon\|_1/t\}| \leq 2t - 1,
\end{equation}
since, if $g = \sum_{l=1}^t a_{\chi_{y_l}}\chi_{y_l}$ (where some of the coefficients might be 0) and
\( \{\chi_y H^+_{j}\} := \{\chi_y H^+_1, \ldots, \chi_y H^+_t\} \), then, from Equation (1),

\[
\sum_{\chi_y H^+_j \in (\mathbb{F}_p^*/H^+) \setminus \{\chi_y H^+_1\}} |c_j(\chi_y H^+_j)| = \sum_{\chi_y H^+_j \in (\mathbb{F}_p^*/H^+) \setminus \{\chi_y H^+_1\}} \sum_{\chi_y \in \chi_y H^+_j} a_{\chi_y} \leq \sum_{\chi_y H^+_j \in (\mathbb{F}_p^*/H^+) \setminus \{\chi_y H^+_1\}} \sum_{\chi_y \in \chi_y H^+_j} |a_{\chi_y}| \leq \sum_{\chi_y \in \mathbb{F}_p^\times \setminus \{\chi_y \ldots \chi_y\}} \|a_{\chi_y}\| \leq \|\epsilon\|_1
\]

and then in particular there are less than \( t \) elements \( \chi_y H^+_1 \in (\mathbb{F}_p^*/H^+) \setminus \{\chi_y H^+_1\} \) such that \( |c_j(\chi_y H^+_j)| > \|\epsilon\|_1/t \). In particular there are at most \( 2t - 1 \) elements \( \chi_y H^+_j \in (\mathbb{F}_p^*/H^+) \) with \( |c_j(\chi_y H^+_j)| > \|\epsilon\|_1/t \).

If \( |a_{\chi_x}| > 2\|\epsilon\|_1/t \) then

\[
|\{j : |c_j(\chi_x H^+_j)| > \|\epsilon\|_1/t\}| > 2t(m - 1)
\]

by Lemma 9 and Equation (11) as then for at least \( 2t(m - 1) \) values \( j \) we have

\[
|c_j(\chi_x H^+_j)| = \left| \sum_{\chi_y \in \chi_x H^+_j} a_{\chi_y} \right| \geq |a_{\chi_x}| - \sum_{\chi_y \in \chi_x H^+_1 \setminus \{\chi_y\}} a_{\chi_y} > \|\epsilon\|_1/t.
\]

So \( Y(\chi_x) > 2t(m - 1) \) in this case.

Again by Lemma 9 and Equation (11), we have that whenever \( Y(\chi_w) > 2t(m - 1) \) then \( |\hat{f}''(\chi_w) - a_{\chi_w}'| \leq \sqrt{2}\|\epsilon\|_1/t \), since in this case \( \hat{f}''(\chi_w) = \text{Median}(\{\text{Re}(x) : x \in X\}) + i\text{Median}(\{\text{Im}(x) : x \in X\}) \) and

\[
|\text{Median}(\{\text{Re}(x) : x \in X\}) - \text{Re}(a_{\chi_w})| \leq \|\epsilon\|_1/t, \\
|\text{Median}(\{\text{Im}(x) : x \in X\}) - \text{Im}(a_{\chi_w})| \leq \|\epsilon\|_1/t.
\]

We will now prove that \( \|\hat{f} - \hat{f}''\|_1 \leq (1 + 3\sqrt{2})\|\epsilon\|_1 \), which will prove the theorem, since by definition \( |\text{supp}(\hat{f}'')| \leq t \). To do this let \( T := \{\chi_y, \ldots, \chi_y\} \) and \( T' := \text{supp}(\hat{f}'') \). We can write \( T \setminus T' = T_1 \cup T_2 \), where

\[
T_1 = \{\chi_y \in T \setminus T' : |a_{\chi_y}| \leq 2\|\epsilon\|_1/t\}, \\
T_2 = \{\chi_y \in T \setminus T' : |a_{\chi_y}| > 2\|\epsilon\|_1/t\},
\]

Notice that \( T', T_2 \subseteq \text{supp}(\hat{f}'') \). For \( \chi_b \in T_2 \) and \( \chi_c \in T' \setminus T \) we have

\[
|a_{\chi_c}| + \sqrt{2}\|\epsilon\|_1/t \geq |\hat{f}''(\chi_c)| \geq |\hat{f}''(\chi_b)| \geq |a_{\chi_b}| - \sqrt{2}\|\epsilon\|_1/t
\]

13
and so \(|a_{\chi_b}| \leq |a_{\chi_c}| + 2\sqrt{2}\|\epsilon\|_1/t\).

Also for \(\chi_b \in T_2\) we have by the previous part that \(\hat{f}''(\chi_b) \neq 0\). From the definition of \(\hat{f}\) if \(|T_2| > 0\) then \(|T'| = t\). In this last case, from \(T_2 \subseteq T \setminus T'\) and \(|T'| = |T'|\), it follows that \(|T' \setminus T| \geq |T_2|\) (this last inequality holds also if \(|T_2| = 0\)).

In particular

\[
\sum_{\chi_b \in T \setminus T'} |a_{\chi_b}| = \sum_{\chi_b \in T_1} |a_{\chi_b}| + \sum_{\chi_b \in T_2} |a_{\chi_b}|
\leq |T_1|2\|\epsilon\|_1/t + |T_2|2\sqrt{2}\|\epsilon\|_1/t + \sum_{\chi_c \in T \setminus T} |a_{\chi_c}|
\leq 2\sqrt{2}\epsilon + \sum_{\chi_c \in T' \setminus T} |a_{\chi_c}|
\]

and then

\[
\|\hat{f} - \hat{f}'\|_1 = \|\hat{f}|_{T'} - \hat{f}'|_{T'}\|_1 + \|\hat{f}|_{T \setminus T'} - \hat{f}'|_{T \setminus T'}\|_1 + \|\hat{f}|_{\widehat{F}_p(H \setminus T')} - \hat{f}'|_{\widehat{F}_p(H \setminus T')}\|_1
= \|\hat{f}|_{T'} - \hat{f}'|_{T'}\|_1 + \sum_{\chi_b \in T \setminus T'} |a_{\chi_b}| + \sum_{\chi_b \in \widehat{F}_p(H \setminus T')} |a_{\chi_b}|
\leq |T'|\sqrt{2}\|\epsilon\|_1/t + 2\sqrt{2}\|\epsilon\|_1 + \sum_{\chi_c \in T' \setminus T} |a_{\chi_c}| + \sum_{\chi_b \in \widehat{F}_p(H \setminus T')} |a_{\chi_b}|
\leq 3\sqrt{2}\|\epsilon\|_1 + \sum_{\chi_b \notin T} |a_{\chi_b}|
\leq (1 + 3\sqrt{2})\|\epsilon\|_1
\]

and so the theorem is proved.

Before presenting the second algorithm we need the following lemma.

**Lemma 11.** Let \(H\) be any subgroup of \(\mathbb{F}_p^r\), \(x \in \mathbb{F}_p^r\) and \(f = \sum_{\chi_w \in \mathbb{F}_p^r} a_{\chi_w} \chi_w\).

If \(\overline{f}\) is a function of \(H\) with \(\overline{f}(y) := f(x + y), y \in H\), then

\[
\hat{f}(\chi_w H^\perp) = \sum_{\chi_z \in \chi_w H^\perp} a_{\chi_z} \chi_z(x).
\]

14
Proof. We have that
\[
\overline{f}(y) = \sum_{\chi_w \in \widehat{F}_p} a_{\chi_w} \chi_w(x + y)
\]
\[
= \sum_{\chi_w \in \widehat{F}_p} a_{\chi_w} \chi_w(x) \chi_w(y)
\]
\[
= \sum_{\chi_w H^+ \in \widehat{F}_p / H^+} \sum_{\chi_z \in \chi_w H^+} a_{\chi_z} \chi_z(x) \chi_z(y)
\]
\[
= \sum_{\chi_w H^+ \in \widehat{F}_p / H^+} \chi_w(y) \sum_{\chi_z \in \chi_w H^+} a_{\chi_z} \chi_z(x)
\]
from which the lemma follows. □

We will now present the second reconstruction theorem. Here we use \(f|_{\Gamma_2}\) in order to construct \(\hat{f}'\).

**Theorem 12.** For \(1 \leq j \leq n\) and \(x \in \mathbb{F}_p^r\) let \(g_{j,x}(y) = f(x + y),\ y \in H_j\), and \(c_{j,x} = F_j(g_{j,x})\), where \(F_j\) is the Fourier transform for \(H_j\). The following algorithm returns \(\hat{f}'\) such that \(|\text{supp}(\hat{f}')| \leq t\) and \(\|\hat{f} - \hat{f}'\|_1 \leq (1 + 3\sqrt{2})\|\epsilon\|_1\).

Set \(\hat{f}' := (0, \ldots, 0), \hat{f}'' := (0, \ldots, 0), Y := (0, \ldots, 0)\) and \(Z := ()\)

for \(j\) from 1 to \(n\) do

for \(2t - 1\) values of \(\chi_w H^+_j\) for which \(|c_{j,0}(\chi_w H^+_j)|\) is largest do

\(\chi_w := ()\)

for \(1 \leq l \leq r - h\) do

Append \(\chi_w \cdot \text{span}_{\mathbb{F}_p}\{x_{l,j}\}\) obtained from the algorithm in Lemma 4 for \(\overline{f}(a) = c_{j,a,x_{l,j}}(\chi_w H^+_j),\ a \in H\) to \(\overline{\chi_w}\)
end for

Reconstruct \(\chi_w\) from \(\chi_w H^+_j\) and \(\overline{\chi_w}\)

\(Y(\chi_w) := Y(\chi_w) + 1\)

if \(Y(\chi_w) = 2t(\lceil r/h \rceil - 1) + 1\) then

Append \(\chi_w\) to \(Z\)
end if
end for

end for

for \(\chi_w \in Z\) do

\(X := ()\)

for \(j\) from 1 to \(n\) do

Append \(c_{j,0}(\chi_w H^+_j)\) to \(X\)
end for

end for
Proof. We will assume that $\chi \leq 1$ for $1 \leq t$.

So, using that $\varphi^\perp = \mathcal{H}$ for any subgroup $H \leq \mathbb{F}_p$,

\[
\varphi^\perp \oplus \varphi^\perp = \mathcal{H}
\]

We will first show how $\chi$ can be reconstructed from $\chi H^\perp$ and $\mathcal{F}$ see the proof of the theorem.

\[\tilde{f}(\chi) := \text{Median} \{ \Re(x) : x \in X \} + i \text{Median} \{ \Im(x) : x \in X \} \]

end for

for $t$ values of $\chi$ for which $|\tilde{f}(\chi)|$ is largest do

\[\tilde{f}(\chi) := \tilde{f}(\chi)\]

end for

return $\tilde{f}$.

In the algorithm $\tilde{f}$, $\tilde{f}^\perp$ and $Y$ are vectors indexed by elements of $\mathbb{F}_p$. To see how $\chi$ can be reconstructed from $\chi H^\perp$ and $\mathcal{F}$ see the proof of the theorem.

Proof. Since $c_{j,0} = F_j(s|H)$ it is enough, from the proof of Theorem 10, to prove that that if $|a_{\chi}| > 2\|\epsilon\|_1/t$ then $\chi \in Z$, that is in this case $Y(\chi) > 2t(m - 1)$.

We will first show how $\chi$ can be reconstructed from $\chi H^\perp$ and $\mathcal{F}$. We will assume that $H_j = \{(0, \ldots, 0, a_{r-h+1}, \ldots, a_r) \in \mathbb{F}_p \}$ and that $x_{l,j} = (0, \ldots, 0, 1, \ldots, 0)$ with $l$-th coefficient 1 and all other coefficients 0 for $1 \leq l \leq r - h$ (this can always be assumed, up to changing the basis of $\mathbb{F}_p$).

We easily have that

\[H^\perp_j = \{ \chi(z_1, \ldots, z_{r-h}, 0, \ldots, 0) : z_i \in \mathbb{F}_p \}, \]

\[\langle \text{span}_{\mathbb{F}_p} \{ x_{l,j} \} \rangle^\perp = \{ \chi(z_1, \ldots, z_{r-h}, 0, \ldots, z_r) : z_i \in \mathbb{F}_p \} \]

So, using that $\mathbb{F}_p^\perp / H^\perp \cong \mathcal{H}$ for any subgroup $H \leq \mathbb{F}_p$,

\[\varphi^\perp \oplus \varphi^\perp = \mathcal{H} \]

\[\text{span}_{\mathbb{F}_p} \{ x_{l,j} \} \cong \mathbb{F}_p / (\text{span}_{\mathbb{F}_p} \{ x_{l,j} \})^\perp = \{ \chi(0, \ldots, 0, y_{r-h+1}, \ldots, y_r) : y_i \in \mathbb{F}_p \} \]

If $\chi H^\perp_j = \chi(0, \ldots, 0, y_{r-h+1}, \ldots, y_r) H^\perp_j$ and $\left( \mathcal{F} \right)_l = \chi(0, \ldots, 0, y_{r-h+1}, \ldots, y_r) (\text{span}_{\mathbb{F}_p} \{ x_{l,j} \})^\perp$ for $1 \leq l \leq r - h$ then $\chi \in \mathcal{F}$. Notice that in this case

\[\left( \mathcal{F} \right)_1 = \{ \chi : z_1 = y_1 \}
\]

\[\vdots \]

\[\left( \mathcal{F} \right)_{r-h} = \{ \chi : z_{r-h} = y_{r-h} \}
\]

\[\chi H^\perp_j = \{ \chi : z_{r-h+1} = y_{r-h+1}, \ldots, z_r = y_r \} \]

In particular $\chi$ is the only element contained in $\chi H^\perp_j$ and in all of the $\left( \mathcal{F} \right)_l$.

For $\chi \in \mathbb{F}_p^\perp$ we have by Lemma 9 that if

\[J = \{ 1 \leq j \leq n : \sum_{\chi \in \chi H_j \setminus \chi} |a_{\chi_z}| \leq \|\epsilon\|_1/t \} \]
then $|J| > 2t(m - 1)$. Assume now that $|a_{\chi_w}| > 2\|\epsilon\|_1/t$ and $j \in J$. Then $|c_{j,0}(\chi_w H_j^\perp)| > \|\epsilon\|_1/t$ and so it is between the $2t - 1$ largest values of $|c_{j,0}(\chi_w H_j^\perp)|$ from Equation (2) from the proof of Theorem 10. We will now show that we reconstruct $\chi_w$ from $\chi_w H_j^\perp$ and $\chi_w$. This will prove the theorem, since then $Y(\chi_w) > 2t(m - 1)$.

Clearly $\chi_w \in \chi_w H_j^\perp$. So it is enough to prove for $1 \leq l \leq r - h$ that $\chi_w \in (\chi_w)(\text{span}_{F_p}\{x_{l,j}\})^\perp$. Using Lemma 11 we have that

$$f(a) = c_{j,ax_{l,j}}(\chi_w H_j^\perp) = \sum_{x_z \in \chi_w H_j^\perp} \chi_z(ax_{l,j})a_{\chi_z}$$

As $\text{span}_{F_p}\{x_{l,j}\} \cong F_p$ we can define $\phi_b(a) := \chi_b(ax_{l,j})$ for $a \in F_p$ and $\chi_b \in \widehat{F_p}$. Notice that if $\chi_b(\text{span}_{F_p}\{x_{l,j}\})^\perp = \chi_b(\text{span}_{F_p}\{x_{l,j}\})^\perp$ if and only if $\phi_b = \phi_k$. So

$$\bar{f} = \sum_{\chi_b(\text{span}_{F_p}\{x_{l,j}\})^\perp \in \widehat{F_p}/(\text{span}_{F_p}\{x_{l,j}\})^\perp} d_{\phi_b} \phi_b$$

where the coefficients $d_{\phi_b}$ are given by

$$d_{\phi_b} = \sum_{\chi_b \in (\chi_w H_j^\perp) \cap (\chi_b(\text{span}_{F_p}\{x_{l,j}\})^\perp)} a_{\chi_b}.$$

Let

$$c := \sum_{\chi_w \neq \chi_b \in (\chi_w H_j^\perp) \cap (\chi_b(\text{span}_{F_p}\{x_{l,j}\})^\perp)} |a_{\chi_b}|.$$

Since $j \in J$ we have that $\sum_{\chi_w \neq \chi_b \in \chi_w H_j^\perp} |a_{\chi_b}| \leq \|\epsilon\|_1/t$ (in particular $c = v\|\epsilon\|_1$ for some $0 \leq v \leq 1$) and $|a_{\chi_w}| > 2\|\epsilon\|_1$. So

$$|d_{\phi_w} | \geq |a_{\chi_w} | - c > (2 - v)\|\epsilon\|_1$$

and

$$\sum_{\phi_b \neq \phi_w} |d_{\phi_b}| \leq \sum_{\chi_b \in \chi_w H_j^\perp \setminus \{\chi_w\}} |a_{\chi_b}| - c \leq (1 - v)\|\epsilon\|_1.$$ 

Since $(2 - v) \geq 2(1 - v)$ for $0 \leq v \leq 1$, in this case the algorithm in Lemma 3 returns $\phi_w$, which corresponds to $\chi_w(\text{span}_{F_p}\{x_{l,j}\})^\perp$ under the isomorphism $\widehat{F_p}/(\text{span}_{F_p}\{x_{l,j}\})^\perp \to \widehat{F_p}$ sending $\chi_b(\text{span}_{F_p}\{x_{l,j}\})^\perp \to \phi_b$. So $\chi_w \in (\chi_w)(\text{span}_{F_p}\{x_{l,j}\})^\perp$, which concludes the proof of the theorem. \qed
7 Remarks to the extension to groups of the form \((\mathbb{Z}/p^a\mathbb{Z})^r\)

One can extend the algorithms to work also on groups of the form \((\mathbb{Z}/p^a\mathbb{Z})^r\) with \(a \geq 1\). This can be done as follows:

1. Construct \(m\)-generating subspaces \(H_1, \ldots, H_n \subseteq \mathbb{F}_p^r\) of dimension \(h\) and find a basis \(\{z_{1,i}, \ldots, z_{h,i}\}\) for each subspace \(H_i\).

   Assuming coefficients of the vectors \(z_{j,i}\) are integers, define \(\overline{H}_i := \langle z_{1,i}, \ldots, z_{h,i} \rangle \subseteq (\mathbb{Z}/p^a\mathbb{Z})^r\) (the subgroup generated by \(z_{1,i}, \ldots, z_{h,i}\)) for \(1 \leq i \leq n\).

2. Extend Lemma 4 to work for \(\mathbb{Z}/p^a\mathbb{Z}\) instead of only for \(\mathbb{F}_p^r\) by taking \(k\) maximal with \(2^k \geq p^a/3\) and changing \(p\) to \(p^a\).

3. Take \(\overline{x}_{j,i} \in \mathbb{Z}/p^a\mathbb{Z}\) with \(\langle H_i, \overline{x}_{1,i}, \ldots, \overline{x}_{r-h,i} \rangle = (\mathbb{Z}/p^a\mathbb{Z})^r\).

4. Define \(\overline{\Gamma}_1\) and \(\overline{\Gamma}_2\) similarly to \(\Gamma_1\) and \(\Gamma_2\).

5. In the algorithms substitute \(\mathbb{F}_p^r\) with \((\mathbb{Z}/p^a\mathbb{Z})^r\) and \(\hat{\mathbb{F}}_p^r\) with \((\hat{\mathbb{Z}}/p^a\mathbb{Z})^r\).

It can be proved that the set \(\overline{H}_j\) are \(m\)-generating for \((\mathbb{Z}/p^a\mathbb{Z})^r\). This depend on square matrices with integer coefficients being singular when reduced to \(\mathbb{Z}/p^a\mathbb{Z}\) exactly when the determinant is divisible by \(p\), independently of the value of \(a\). Also one can prove that

\[ (\mathbb{Z}/p^a\mathbb{Z})^r \cong \overline{H}_i \times \langle \overline{x}_{1,i} \rangle \times \cdots \times \langle \overline{x}_{r-h,i} \rangle, \]

which is needed in order to adapt the proof of the theorems. However from \(|H_i| = p^{ah}\) and \(p^h \geq 4t\) (if \(h < r\)) we have

\[ |\overline{\Gamma}_1| \geq |H_1| = p^{ah} \geq 4^a t^a.\]

So \(|\overline{\Gamma}_1|\) cannot be quadratic in \(t\) (unless possibly for \(a \leq 2\)). Looking at upper bound on \(|\overline{\Gamma}_1|\) we obtain

\[ |\overline{\Gamma}_1| \leq np^{ah} < 16pt^2r^2p^{(a-1)h}.\]

Again as \(p^h \geq 4t\) for \(h < r\),

\[ 16pt^2r^2p^{(a-1)h} \geq 16pt^2r^2(4t)^{a-1} = 4^{a+1}pt^{a+1}r^2.\]

So, also for \(a = 2\), the given upper bound is not quadratic in \(t\). For this reason we did not extend the paper to groups of the form \((\mathbb{Z}/p^a\mathbb{Z})^r\).
8 Further remarks

From

\[ \left| \mathbf{1}_H(\chi_g) \right| = \left| p^{-r} \sum_{x \in H} \chi_g(x) \right| = p^{-r} \left| H \mathbf{1}_{H^\perp}(\chi_g) \right| = p^{h-r} \mathbf{1}_{H^\perp}(\chi_g) \]

for any subspace \( H \) of \( \mathbb{F}_p^r \) of dimension \( h \), it can be checked that, if \( H_1, \ldots, H_n \) are \( m \)-generating, then

\[ \sum_i \left| \mathbf{1}_{H_i}(\chi_g) \right| \leq (m - 1)p^{h-r} \text{ for every } 1 \neq \chi_g \in \mathbb{F}_p^r \]

and

\[ \sum_i \left| \mathbf{1}_{H_i}(1) \right| = np^{h-r} := C. \]

In particular it can be proved that the matrix with columns labeled by the elements of \( \bigcup_{j \in I} H_j \) (taking the union as a multiset, so that some columns may be repeated), rows labeled by the elements of \( \mathbb{F}_p^r \) and coefficients \( \chi_g(g)/\sqrt{C} \) satisfies the RIP property of rank \( t \) and constant \( (t - 1)(m - 1)/n \). In particular if \( n > 2(t - 1)(m - 1) \)

and the subspaces \( H_i \) are \( m \)-generating then we could approximate any \( t \)-sparse Fourier signal also using reconstruction algorithms based on the RIP property.

Some slight variation of the algorithms presented in Theorem 10 and 12 (based on similar algorithms from [8]) can also be constructed taking \( n \) to be \( 2t(m - 1) \), which however returns functions with

\[ \| (\hat{f} + \epsilon) - \hat{f} \|_1 \leq (1 + 2t)\| \epsilon \|_1. \]

If \( \| \epsilon \|_1 > 0 \) these algorithms give worse approximations than the ones described here. However if \( \| \epsilon \|_1 = 0 \) then also these algorithms reconstruct \( f \) and they work on smaller (about half the size) sets. Since sizes of sampling sets and complexities of the algorithms are about the same (they differ only by a small multiplicative constant), these algorithms have not been presented here.

9 Acknowledgments

The author thanks Hartmut Führ for help in reviewing the paper.

The results presented here are part of the author Ph.d. thesis [10]. The results have also already been presented in the form of an extended abstract in [11].

The author was supported during her Ph.d. by the DFG grant GRK 1632 for the Graduiertenkolleg Experimentelle und konstruktive Algebra at RWTH Aachen University.
References

[1] J. Bailey, M. A. Iwen, C. V. Spencer, On the design of deterministic matrices for fast recovery of Fourier compressible functions, SIAM J. Matrix Anal. Appl. 33, 263-289, 2012.

[2] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, Explicit constructions of RIP matrices and related problems, Duke Math. J. 159, 145-185, 2011.

[3] E. J. Candès, J. K. Romberg, T. Tao, Stable signal recovery from incomplete and inaccurate measurements, Comm. Pure Appl. Math. 59, 1207-1223, 2006.

[4] E. J. Candès, T. Tao, Decoding by linear programming, IEEE Trans. Inform. Theory 51, 4203-4215, 2005.

[5] R. A. DeVore, Deterministic constructions of compressed sensing matrices, J. Complexity 23, 918-925, 2007.

[6] S. Foucart, H. Rauhut, A mathematical introduction to compressive sensing, Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, New York, 2013.

[7] J. Haupt, L. Applebaum, R. Nowak, On the restricted isometry of deterministically subsampled Fourier matrices, In Information Sciences and Systems (CISS), 2010 44th Annual Conference on, 1-6, 2010.

[8] M. A. Iwen, Combinatorial sublinear-time Fourier algorithms, Found. Comput. Math. 10, 303-338, 2010.

[9] F. J. Macwilliams, N. J. A. Sloane, The theory of error-correcting codes, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, North-Holland Mathematical Library, Vol. 16.

[10] L. Morotti, Explicit construction of universal sampling sets for finite abelian and symmetric groups, Ph.d. thesis, RWTH Aachen University, 2014.

[11] L. Morotti, Reconstruction of Fourier sparse signals over elementary abelian groups, ENDM 43, 161-167, 2013.

[12] M. Rudelson, R. Vershynin, On sparse reconstruction from Fourier and Gaussian measurements, Comm. Pure Appl. Math. 61, 1025-1045, 2008.
[13] A. M. Tillmann, M. E. Pfetsch, The computational complexity of the restricted isometry property, the nullspace property, and related concepts in compressed sensing, *IEEE Trans. Inform. Theory* 60, 1248-1259, 2014.