16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP

DETERMINISTIC DICTIONARIES FOR SPARSITY: A GROUP REPRESENTATION APPROACH

Shamgar Gurevich[1], *Ronny Hadani*[2], *and Nir Sochen*[3]

[1]Department of Mathematics, University of California Berkeley
Berkeley, CA 94720, USA
E-mail: shamgar@math.berkeley.edu

[2]Department of Mathematics, University of Chicago
Chicago, IL, 60637, USA
E-mail: hadani@math.uchicago.edu

[3]School of Mathematical Sciences, Tel Aviv University
Tel Aviv, 69978, Israel
E-mail: sochen@math.tau.ac.il

ABSTRACT

We describe two deterministic constructions of dictionaries of functions on the finite line which support certain degree of sparsity.

1. INTRODUCTION

Digital signals, or simply signals, can be thought of as functions on the finite line $\mathbb{F}_p$, namely the finite field with p elements, where p is an odd prime. The space of signals $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ is equipped with a natural Hermitian product

$$\langle \varphi, \phi \rangle = \sum_{x \in \mathbb{F}_p} \varphi(x) \overline{\phi(x)}.$$

A central problem is constructing useful classes of signals that demonstrate strong descriptive power and at the same time are characterized by formal mathematical conditions. Meeting these two requirements is a non trivial task and is a source for many novel developments in the field of signal processing. The problem was tackled, over the years, by various approaches.

In the classical approach, a signal is characterized in terms of its expansion with respect to a specific basis. A standard example of this kind is the class of *band-limited* signals which is defined using the Fourier basis and consists of signals with a specified support of their Fourier representation.

However, for certain applications this approach is too restrictive. In a more general approach, the signal is characterized in terms of its expansion with respect to a frame, which is kind of a generalized basis. The theory of *wavelets* is a particular application of this approach. As it turns out, many classical results from linear algebra have appropriate generalizations to the setting of frames. As a consequence, wavelet analysis exhibits structural similarity to Fourier analysis.

Recently, a novel approach was introduced, hinting towards a fundamental change of perspective about the nature of signals. This new approach uses the notion of *sparse dictionary* which is yet another kind of generalized basis. The basic idea is the same as before, namely, a signal is characterized in terms of its expansion as a linear combination of vectors in the dictionary. The main difference is that here the characterization is intrinsically non-linear. As a consequence, one comes to deal with classes of signals which are not closed with respect to addition. More formally:

Definition 1. *A set $\mathfrak{D} \subset \mathcal{H}$ of signals is called an N-* ***independent*** *set if every subset $\mathfrak{D}' \subset \mathfrak{D}$, with $\#\mathfrak{D}' = N$, is linearly independent.*

Given an $2N$-independent set $\mathfrak{D}$, every signal $\varphi \in \mathcal{H}$, has at most one expansion of the form

$$\varphi = \sum_{s \in \mathfrak{D}'} a_s s,$$

for $\mathfrak{D}' \subset \mathfrak{D}$ with $\#\mathfrak{D}' \leq N$. Such an expansion, if exists, is unique and is called the sparse expansion. Consequently another name for such a set $\mathfrak{D}$ is an N-sparse dictionary. Given that a signal φ admits a sparse expansion, it is natural to ask whether the coefficients a_s can be effectively reconstructed. A dictionary $\mathfrak{D}$ for which there exists a polynomial time algorithm for reconstructing the "sparse" coefficients is called an effectively N-sparse dictionary.

To give the reader some feeling for the new concept, we note that an orthonormal basis appears as a degenerate example of an effectively sparse dictionary. More precisely, it is $\dim \mathcal{H}$-sparse, consisting of $\dim \mathcal{H}$ signals. The effectiveness follows from the fact that the coefficient a_s can be reconstructed from φ by $a_s = \langle s, \varphi \rangle$.

A basic problem in the new theory is introducing systematic constructions of "good" effectively N-sparse dictionaries. Here "good" means that the size of the dictionary and the sparsity factor N are made as large as possible. Currently, the only known methods use either certain amount of randomness or are based on ad-hoc considerations (see [BDE] and references therein).

In this short paper, we begin to develop a systematic approach to the construction of effectively sparse dictionaries and, in particular, we describe two examples of such dictionaries. Our approach is based on the representation theory of groups over finite fields.

Showing that a dictionary is effectively N-sparse is difficult. A way to overcome this difficulty is to introduce the notion of *incoherent dictionaries*.

Definition 2. *A set of unit length vectors $\mathfrak{D} \subset \mathcal{H}$ is called μ-coherent dictionary, for $0 \leq \mu \ll 1$ if for every two different* *vectors* $s_1, s_2 \in \mathfrak{D}$ *we have* $|\langle s_1, s_2 \rangle| \leq \varepsilon$.

The two notions of coherence and sparsity are related by the following proposition (see [BDE, DE, EB, GN, Tr])

Proposition 1. *If* $\mathfrak{D}$ *is* $\frac{1}{R}$*-coherent then* $\mathfrak{D}$ *is effectively* $\lfloor \frac{R}{2} \rfloor$*-sparse* [1].

In this paper we construct two incoherent dictionaries. The first dictionary $\mathfrak{D}_H$ is called the *Heisenberg* dictionary and is constructed using the representation theory of the finite *Heisenberg group. It is* $\frac{1}{\sqrt{p}}$-coherent, consisting of $O(p^2)$ vectors. This collection of vectors appears in the literature in various contexts (e.g. [H, HCM]). Our aim here is merely to clarify its representation theoretic origin and use it as a suggestive model example.

The main contribution of this paper is the introduction of a subtler dictionary $\mathfrak{D}_O$, that we will call the *oscillator* dictionary, which is constructed using the representation theory of the two dimensional symplectic group $SL_2(\mathbb{F}_p)$. The representation is known as the Weil representation. The group $SL_2(\mathbb{F}_p)$ is the group of automorphism of the Heisenberg group. The importance of the latter in signal processing is well known (see for recent account [FHKMN] and references therein). We show in this paper that the Weil representation is a central object in digital signal processing. In particular it enables the construction of a dictionary which is $\frac{4}{\sqrt{p}}$-coherent and consists of $O(p^3)$ vectors. We also introduce a natural extension of this dictionary which is $\frac{4}{\sqrt{p}}$-coherent and consists of $O(p^5)$ signals. Signals in $\mathfrak{D}_O$ constitute, in an appropriate formal sense, a finite field analogue of the pure modes of the harmonic oscillator in the real setting. In this paper we explain the construction of $\mathfrak{D}_O$ and state some of its properties which are relevant to sparsity, referring the reader to [GHS] for a more comprehensive treatment.

2. THE HEISENBERG AND THE OSCILLATOR DICTIONARIES

2.1 The Heisenberg group

Let (V, ω) be a two-dimensional symplectic vector space over the finite field $\mathbb{F}_p$. The reader should think of V as $\mathbb{F}_p \times \mathbb{F}_p$ with the standard form $\omega((\tau, w), (\tau', w')) = \tau w' - w\tau'$. Considering V as an abelian group, it admits a non-trivial central extension called the *Heisenberg* group. Concretely, the group H can be presented as the set $H = V \times \mathbb{F}_p$ with the multiplication given by

$$(v,z) \cdot (v',z') = (v+v', z+z' + \tfrac{1}{2}\omega(v,v')).$$

The center of H is $Z = Z(H) = \{(0,z) : z \in \mathbb{F}_p\}$. The symplectic group $Sp = Sp(V,\omega)$, which in this case is just isomorphic to $SL_2(\mathbb{F}_p)$, acts by automorphism of H through its action on the V-coordinate.

2.2 The Heisenberg representation

One of the most important attributes of the group H is that it admits, principally, a unique irreducible representation. The precise statement goes as follows. Let $\psi : Z \to \mathbb{C}^\times$ be a character of the center. For example we can take $\psi(z) = e^{\frac{2\pi i}{p} z}$.

Theorem 1. (Stone-von Neumann) *There exists a unique (up to isomorphism) irreducible unitary representation* $(\pi, H, \mathscr{H})$ *with the center acting by* ψ, *i.e.,* $\pi_{|Z} = \psi \cdot Id_{\mathscr{H}}$.

The representation π which appears in the above theorem will be called the *Heisenberg representation*. More concretely, $(\pi, H, \mathscr{H})$ can be realized as follows: $\mathscr{H}$ is the Hilbert space $\mathbb{C}(\mathbb{F}_p)$ of complex valued functions on the finite line, with the standard Hermitian product. The action π is given by $\pi(\tau,0) \triangleright f(t) = f(t+\tau)$, $\pi(0,w) \triangleright f(t) = \psi(wt) f(t)$ and $\pi(z) \triangleright f(t) = \psi(z) f(t)$.

2.3 The Weil representation

A direct consequence of Theorem 1 is the existence of a projective representation $\widetilde{\rho} : Sp \to PU(\mathscr{H})$. The construction of $\widetilde{\rho}$ out of the Heisenberg representation π is due to Weil [W] and it goes as follows. Considering the Heisenberg representation π and an element $g \in Sp$, one can define a new representation π^g acting on the same Hilbert space via $\pi^g(h) = \pi(g(h))$. Clearly both π and π^g have the same central character ψ hence by Theorem 1 they are isomorphic. Since the space $\mathsf{Hom}_H(\pi, \pi^g)$ is one dimensional, choosing for every $g \in Sp$ a non-zero representative $\widetilde{\rho}(g) \in \mathsf{Hom}_H(\pi, \pi^g)$ gives the required projective representation. In more concrete terms, the projective representation $\widetilde{\rho}$ is characterized by the formula

$$\rho(g)\,\pi(h)\,\rho\left(g^{-1}\right) = \pi(g(h)), \qquad (1)$$

for every $g \in Sp$ and $h \in H$. It is a peculiar phenomenon of the finite field setting that the projective representation $\widetilde{\rho}$ can be linearized into an honest representation

Theorem 2. ([GH2] and reference therein) *There exists a unique*[2] *linear representation*

$$\rho : Sp \longrightarrow GL(\mathscr{H}),$$

which satisfies equation (1).

2.4 The Heisenberg dictionary

The Heisenberg dictionary is a collection of $p+1$ orthonormal bases, each characterized, roughly, as eigenvectors of a specific linear operator. The most elegant way to define this dictionary is using the Heisenberg representation.

2.4.1 Bases associated with lines

The Heisenberg group is non-commutative, yet it consists of various commutative subgroups which can be easily described. Let $L \subset V$ be a line in V, one can associate to L a commutative subgroup $A_L \subset H$, $A_L = \{(l,0) : l \in L\}$. It will be convenient to identify the group A_L with the line L. Restricting the Heisenberg representation π to the commutative subgroup L yields a decomposition into character spaces

$$\mathscr{H} = \bigoplus_{\chi} \mathscr{H}_\chi,$$

where χ runs in the set $L^\vee$ of (complex valued) characters of L. More concretely, choosing a non-zero vector $l \in L$, each character space $\mathscr{H}_\chi$ naturally corresponds to specific

[1] Here $\lfloor \frac{R}{2} \rfloor$ stands for the greatest integer which is less then or equal to $\frac{R}{2}$.

[2] Unique, except in the case the finite field is $\mathbb{F}_3$. since the group $SL_2(F_p)$ is perfect for $p \neq 3$ i.e. it has no multiplicative characters.

eigenspace of the linear operator $\pi(l)$. It is very easy to verify that

Lemma 1. *For every $\chi \in L^{\vee}$ we have* $\dim \mathscr{H}_{\chi} = 1$.

Choosing a unit vector $\varphi_{\chi} \in \mathscr{H}_{\chi}$ we obtain an orthonormal basis which we denote by B_L. Since there exists $p+1$ different lines in V, we have this number orthonormal bases, overall we constructed a dictionary of vectors $\mathfrak{D}_H = \{\varphi \in B_L : L \subset V\}$ consisting of $p(p+1)$ vectors. We will call the dictionary $\mathfrak{D}_H$, for obvious reasons, the *Heisenberg dictionary*. The main property of the Heisenberg dictionary is summarized in the following theorem [H, HCM]

Theorem 3. *For every pair of different lines $L, M \subset V$ and for every $\varphi \in B_L$, $\phi \in B_M$*

$$|\langle \phi, \varphi \rangle| = \frac{1}{\sqrt{p}}.$$

Example 1. *There are two standard examples of bases of the form B_L. Considering the lines $T = \{(\tau, 0) : \tau \in \mathbb{F}_p\}$ and $W = \{(0, w) : w \in \mathbb{F}_p\}$, we have $B_W = \{\delta_a : a \in \mathbb{F}_p\}$ and $B_T = \{\psi_a : a \in \mathbb{F}_p\}$, where $\psi_a(t) = \frac{1}{\sqrt{p}}\psi(at)$. Indeed, functions of the form δ_a are common eigenvectors of $\pi(0,w)$ and ψ_a are common eigenvectors of $\pi(\tau, 0)$. Finally, it can be easily verified that $|\langle \delta_a, \psi_b \rangle| = \frac{1}{\sqrt{p}}$ for every $\delta_a \in B_W$ and $\psi_b \in B_T$. The content of Theorem 2.4.1 is that this example is a particular case of a more general phenomena related to a larger dictionary of $p+1$ orthonormal bases.*

2.5 The Oscillator dictionary

Reflecting back on the Heisenberg dictionary we see that it was characterized in terms of commutative subgroups in the Heisenberg group H via the Heisenberg representation π. In comparison, the oscillator dictionary [GHS] is characterized in terms of commutative subgroups of the symplectic group Sp via the Weil representation ρ.

2.5.1 Bases associated with maximal tori

A maximal (algebraic) torus in Sp is a maximal commutative subgroup which becomes diagonalizable over some field extension. There exists two conjugacy classes of maximal (algebraic) tori in Sp. The first class consists of those tori which are diagonalizable already over $\mathbb{F}_p$, these tori are conjugated to the standard diagonal torus

$$T_{std} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_p \right\}.$$

A torus in this class is called a *split* torus. The second class consists of those tori which become diagonalizable over a quadratic extension $\mathbb{F}_{p^2}$, these tori are not conjugated to T_{std}. A torus in this class is called a *non-split* torus (sometimes it is called inert torus). All split (non-split) tori are conjugated to one another, therefore the number of split tori is $\#(Sp/N_s) = \frac{p(p+1)}{2}$, where N_s is the normalizer group of some split torus. In the same fashion, the number of non-split tori is $\#(Sp/N_{ns}) = p(p-1)$, where N_{ns} is the normalizer group of some non-split torus.

Example 2. *It might be suggestive to explain further the notion of non-split tori by exploring, first, the analogue notion in the more familiar setting of the field $\mathbb{R}$. Here, the standard example of a maximal non-split torus is the circle group $SO(2) \subset SL_2(\mathbb{R})$. Indeed, it is a maximal commutative subgroup which becomes diagonalizable when considered over the extension field $\mathbb{C}$ of complex numbers. The above analogy suggests a way to construct examples of maximal non-split tori in the finite field setting as well. Let us assume for simplicity that -1 does not admit a square root in $\mathbb{F}_p$. The group Sp acts naturally on the plane $V = \mathbb{F}_p \times \mathbb{F}_p$. Consider the symmetric bilinear form B on V given by*

$$B((x,y),(x',y')) = xx' + yy'.$$

An example of maximal non-split torus is the subgroup $T_{ns} \subset Sp$ consisting of all elements $g \in Sp$ preserving the form B, namely $g \in T_{ns}$ if and only if $B(gu, gv) = B(u,v)$ for every $u, v \in V$. The reader might think of T_{ns} as the "finite circle".

Restricting the Weil representation to a maximal torus $T \subset Sp$ yields a decomposition

$$\mathscr{H} = \bigoplus_{\chi} \mathscr{H}_{\chi}, \tag{2}$$

where χ runs in the set $T^{\vee}$ of complex valued characters of the torus T. More concretely, choosing a generator[3] $t \in T$, the decomposition (2) naturally corresponds to the eigenspaces of the linear operator $\rho(t)$. The decomposition (2) depends on the type of T. If T is a split torus then $\dim \mathscr{H}_{\chi} = 1$ unless $\chi = \sigma$, where σ is the unique quadratic character of T (also called *Legendre* character), in the latter case $\dim \mathscr{H}_{\sigma} = 2$. If T is a non-split torus then $\dim \mathscr{H}_{\chi} = 1$ for every character χ which appears in the decomposition, in this case the quadratic character σ does not appear in the decomposition [GH1].

Choosing for every character $\chi \in T^{\vee}$, $\chi \neq \sigma$, a unit vector $\varphi_{\chi} \in \mathscr{H}_{\chi}$ we obtain an orthonormal set of vectors $B_T = \{\varphi_{\chi} : \chi \neq \sigma\}$. We note that when T is non-split the set B_T is an orthonormal basis. Considering the union of all these sets, we obtain the oscillator dictionary

$$\mathfrak{D}_O = \{\varphi \in B_T : T \subset Sp\}.$$

It is convenient to separate the dictionary $\mathfrak{D}_O$ into two sub-dictionaries $\mathfrak{D}_O^s$ and $\mathfrak{D}_O^{ns}$ which correspond to the split tori and the non-split tori respectively. The sub-dictionary $\mathfrak{D}_O^s$ consists of $\frac{p(p+1)}{2}$ sets, each consisting of $p-2$ orthonormal vectors, altogether $\#\mathfrak{D}^s = \frac{p(p+1)(p-2)}{2}$. The non-split sub-dictionary $\mathfrak{D}_O^{ns}$ consists of $p(p-1)$ bases each consisting of p orthonormal vectors, altogether $\#\mathfrak{D}_O^{ns} = p^2(p-1)$. The oscillator class satisfies many desired properties [GHS]. In this note we are only interested in the following:

Theorem 4([GHS]) *For every $\phi \in B_{T_1}$ and $\varphi \in B_{T_2}$*

$$|\langle \phi, \varphi \rangle| \leq \frac{4}{\sqrt{p}}.$$

[3]A maximal torus T in $SL_2(\mathbb{F}_p)$ is a cyclic group, thus there exists a generator.

Example 3. *Consider the standard torus $T_{std} \subset Sp$, which is isomorphic to the multiplicative group $\mathbb{F}_p^{\times}$. Given a non-trivial multiplicative character[4] $\chi : \mathbb{F}_p^{\times} \to \mathbb{C}^{\times}$, we define the function $\underline{\chi} \in \mathbb{C}(\mathbb{F}_p)$ by*

$$\underline{\chi}(t) = \begin{cases} \frac{1}{\sqrt{p-1}}\chi(t) & t \neq 0 \\ 0 & t = 0 \end{cases}.$$

We have $B_T = \left\{ \underline{\chi} : \chi \in G_m^{\vee},\ \chi \neq 1 \right\}$. Indeed, elements of the standard torus act via the Weil representation, principally, by scaling, $\rho(a) \triangleright f(t) = \sigma(t) f(at)$, hence the function $\underline{\chi}$ is an eigenvector of $\rho(a)$ for every $a \in T$.

2.5.2 *Extended oscillator dictionary*

The oscillator dictionary can be extended to a much larger dictionary using the action of the Heisenberg group. Given a vector $\varphi \in \mathfrak{D}_O$ one can consider its orbit under the action of the set $V \subset H$

$$\mathscr{O}_\varphi = V \cdot \varphi \triangleq \{\pi(v)\varphi : v \in V\}.$$

It is not hard to show that orbits associated to different vectors are disjoint, therefore, we obtained a dictionary $\mathfrak{D}_E = \bigcup_{\varphi \in \mathfrak{D}} \mathscr{O}_\varphi$, consisting of $\#(V) \cdot \#(\mathfrak{D}_O) \sim O(p^5)$ vectors. Interestingly, the extended dictionary $\mathfrak{D}_E$ continues to be $\frac{4}{\sqrt{p}}$-coherent, this is a consequence of the following generalization of Theorem 2.5.1

Theorem 5([GHS]) *Given two vectors $\varphi, \phi \in \mathfrak{D}_O$ and an element $h \in H$ such that $h \notin Z(H)$ then*

$$|\langle \varphi, \pi(h)\phi \rangle| \leq \frac{4}{\sqrt{p}}.$$

Remark *A particular interpretation of Theorem 5 is that any two different vectors $\varphi \neq \phi \in \mathfrak{D}_O$ are weakly coherent in a stable sense, that is, their coherence is $\frac{4}{\sqrt{p}}$ no matter if any one of them undergoes an arbitrary phase/time shift. This property seems to be important in communication where a transmitted signal may acquire time shift due to asynchronous communication and phase shift due to Doppler effect.*

2.5.3 *Field extension*

All the results in this paper were stated for the basic finite field $\mathbb{F}_p$, where p is an odd prime, for the reason of making the terminology more accessible. In fact, all the results can be stated and proved [GHS] for any field extension of the form $F = \mathbb{F}_q$, $q = p^n$, one should only replace p by q in all appropriate places.

REFERENCES

[BDE] A.M. Bruckstein, D.L. Donoho and M. Elad, "From Sparse Solutions of Systems of Equations to Sparse Modeling of Signals and Images", to appear in *SIAM Review*.

[DE] Donoho D.L. and Elad M., Optimally sparse representation in general (non-orthogonal) dictionaries via l_1 minimization. *Proc. Natl. Acad. Sci. USA 100, no. 5, 2197–2202* (2003).

[EB] Elad M. and Bruckstein A.M., A Generalized Uncertainty Principle and Sparse Representation in Pairs of Bases. *IEEE Trans. On Information Theory, Vol. 48, pp. 2558-2567* (2002).

[FHKMN] H. G. Feichtinger, M. Hazewinkel, N. Kaiblinger, E. Matusiak, M. Neuhauser, Metaplectic operators on C^n, Quart. J. Math. 59 (2008), no. 1, 15-28.

[GG] S.W. Golomb and G. Gong, *Signal design for good correlation For wireless communication, cryptography, and radar*, Cambridge University Press, Cambridge (2005).

[GH1] S. Gurevich and R. Hadani, "Self-reducibility of the Weil representation and applications", *arXiv:math/0612765* (2005).

[GH2] , Gurevich S. and Hadani R., "The geometric Weil representation", Selecta Mathematica 13(3) (2006) pp. 465-481.

[GHS] S. Gurevich, R. Hadani and N. Sochen, "The Finite Harmonic Oscillator and its Associated Sequences", to appear in *Proceedings of the National Academy of Sciences of the United States of America*.

[GN] Gribonval R. and Nielsen M. Sparse representations in unions of bases. *IEEE Trans. Inform. Theory 49, no. 12, 3320–3325* (2003).

[H] R. Howe, "Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries", *Indag. Math. (N.S.) 16* (2005), no. 3-4, pp. 553–583.

[HCM] S. D. Howard, A. R. Calderbank and W. Moran, "The finite Heisenberg-Weyl groups in radar and communications", *EURASIP J. Appl. Signal Process. 2006* (2008) pp.1–12.

[Tr] Tropp, J.A., Greed is good: algorithmic results for sparse approximation. *IEEE Trans. Inform. Theory 50, no. 10* (2004) 2231–2242.

[W] A. Weil, "Sur certains groupes d'operateurs unitaires", *Acta Math. 111* (1964) pp. 143–211.

[4] A multiplicative character is a function $\chi : \mathbb{F}_p^{\times} \to \mathbb{C}$ which satisfies $\chi(xy) = \chi(x)\chi(y)$ for every $x, y \in \mathbb{F}_p^{\times}$.