The Journal of Fourier Analysis and Applications

Volume 11, Issue 6, 2005

Linear Independence of Gabor Systems in Finite Dimensional Vector Spaces

Jim Lawrence, Götz E. Pfander, and David Walnut

Communicated by Chris Heil

ABSTRACT. We discuss the linear independence of systems of m vectors in n-dimensional complex vector spaces where the m vectors are time-frequency shifts of one generating vector. Such systems are called Gabor systems. When n is prime, we show that there exists an open, dense subset with full-measure of such generating vectors with the property that any subset of n vectors in the corresponding full Gabor system of n^2 vectors is linearly independent. We derive consequences relevant to coding, operator identification and time-frequency analysis in general.

1. Introduction

The goal of this article is to show that there exist Gabor frames for $\mathbb{C}^n$ consisting of n^2 vectors in $\mathbb{C}^n$ with the property that every subset of n vectors is linearly independent. In other terminology, we say that the vectors in such a Gabor frame are in *linear general position* or possess the *Haar property* (cf. [4]).

This result, given as Theorem 1 in Section 2, has implications for operator identification (e.g., [2, 11]), for the structure of the discrete short-time Fourier transform, and for the robust coding of signals transmitted over lossy channels. Theorems 2 and 3 in Section 3 summarize these implications. In addition, the result can be thought of as a discrete analog of the so-called HRT conjecture which asserts that every finite collection of time-frequency translates of a single function in $L^2(\mathbb{R})$ is linearly independent. See [8] for details on recent progress on proving the HRT conjecture. Section 4 contains the proof of a slightly more general form of Theorem 1.

Math Subject Classifications. 15A15, 42C15.
Keywords and Phrases. Linearly independent Gabor systems, Haar property.

© 2005 Birkhäuser Boston. All rights reserved
ISSN 1069-5869 DOI: 10.1007/s00041-005-5017-6

2. Notation and Terminology

Definition 1. Set $\omega = e^{2\pi i/n}$. The translation operator T is the unitary operator on $\mathbb{C}^n$ given by $Tx = T(x_0, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \ldots, x_{n-2})$, and the modulation operator M is the unitary operator defined by $Mx = M(x_0, \ldots, x_{n-1}) = (\omega^0 x_0, \omega^1 x_1, \ldots, \omega^{n-1} x_{n-1})$. We set $\pi(\lambda) = M^l T^k$ for $\lambda = (l, k)$. Given a vector $g \in \mathbb{C}^n$ the *full Gabor system with window* g is the collection $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$, where $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Given $n \in \mathbb{N}$, the *discrete Fourier matrix* W_n is defined by $W_n = (\omega^{pq})_{p,q=0}^{n-1}$ and given a vector $g \in \mathbb{C}^n$ the *Discrete Fourier Transform (DFT)* of g, denoted $\widehat{g}$, is the vector $\widehat{g} = \frac{1}{n} W_n^* g$.

Let $g = (g_0, g_1, \ldots, g_{n-1}) \in \mathbb{C}^n$ be given. For $k = 0, 1, \ldots, n-1$, let D_k be the diagonal matrix

$$D_k = \operatorname{diag}(g_k, g_{k+1}, \ldots, g_{n-1}, g_0, \ldots, g_{k-1}) .$$

Define the $n \times n^2$ *full Gabor system matrix* G by

$$G = (D_0 \cdot W_n \mid D_1 \cdot W_n \mid \cdots \mid D_{n-1} \cdot W_n) . \tag{2.1}$$

We will write $G = G(g)$ to emphasize that G is a matrix-valued function on $\mathbb{C}^n$. It is clear that the columns of $G(g)$ are the vectors $\pi(\lambda)g$, for $\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n$.

Definition 2. A family $\mathcal{F}$ of $m \geq n$ vectors in $\mathbb{C}^n$ has the *Haar property* (cf. [4]) if any subset $\mathcal{F}' \subseteq \mathcal{F}$ with $|\mathcal{F}'| = n$ is linearly independent.

The following is immediate.

Proposition 1. *The Gabor system $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$ has the Haar property if and only if every minor (Definition 9) of $G(g)$ of order n is nonzero.*

The main result of this article is the following.

Theorem 1. *If n is prime then there is a dense open set E of full measure*[1] *in $\mathbb{C}^n$ such that for every $g \in E$, the full Gabor system $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$ has the Haar property.*

3. Implications of Theorem 1

3.1 Operator Identification and the Short-Time Fourier Transform

Definition 3. A linear space of operators (matrices) $\mathcal{M} \subseteq \mathcal{L}(\mathbb{C}^m, \mathbb{C}^n) \equiv \operatorname{Mat}(n \times m)$ is called *identifiable with identifier* $g \in \mathbb{C}^m$ if the linear map $\varphi_g : \mathcal{M} \longrightarrow \mathbb{C}^n,\ M \mapsto Mg$ is injective, i.e., if $Mg \neq 0$ for all $M \in \mathcal{M} \setminus \{0\}$. If there exists an identifier for $\mathcal{M}$, then we call $\mathcal{M}$ *identifiable,* In other words, $\mathcal{M}$ is identifiable if there exists a vector $g \in \mathbb{C}^m$ such that for all $M \in \mathcal{M}$, $Mg = 0$ implies $M = 0$.

[1] E is of *full measure* if the Lebesgue measure of $\mathbb{C}^n \setminus E$ is 0.

Example 1.

(1) $\mathcal{M} = \text{Mat } (3 \times 3)$, $\mathcal{M}$ not identifiable since $\dim \mathcal{M} = 9 \geq 3 = \dim \mathbb{C}^3$, and, hence, $\mathcal{M}$ cannot be mapped injectively by a linear map to $\mathbb{C}^3$. This reduces to the obvious statement that for every $g \in \mathbb{C}^3$ there is a nonzero matrix $M \in \mathcal{M}$ such that $Mg = 0$.

(2) $\mathcal{M} = \left\{ \begin{pmatrix} a & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ a, b, c \in \mathbb{C} \right\}$, $\mathcal{M}$ not identifiable since $\dim \mathcal{M} = 3 \geq 1 \geq \dim \mathcal{M}g \quad \forall g \in \mathbb{C}^3$, where $\mathcal{M}g = \{Mg,\ M \in \mathcal{M}\} = \text{range } \varphi_g$. This is equivalent to the statement that for every $g \in \mathbb{C}^3$ there is a nonzero $M \in \mathcal{M}$ such that $Mg = 0$. This is accomplished by simply choosing $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ to be a nonzero vector orthogonal to g.

(3) $\mathcal{M} = \left\{ \begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{pmatrix},\ a, b, c \in \mathbb{C} \right\}$, $\mathcal{M}$ identifiable since $\begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$.

Definition 4. The *spreading function* of a matrix $H \in \text{Mat } (n \times n)$ given by $H = (h_{i,j})_{i,j=0}^{n-1}$, denoted $\eta_H \in \mathbb{C}^{n^2}$, is defined by

$$\eta_H(l, k) = \frac{1}{n} \sum_{m=0}^{n-1} h_{m,m-k}\, \omega^{-ml}$$

for $k,\ l = 0,\ \ldots,\ n-1$, where here and in the following, indices are taken modulo n.

Lemma 1. *The family of operators* $\{M^l T^k\}_{(l,k) \in \mathbb{Z}_n \times \mathbb{Z}_n} \subseteq \text{Mat}(n \times n)$ *is a basis for* $\text{Mat}(n \times n)$. *In particular,*

$$H = \sum_{l=0}^{n-1} \sum_{k=0}^{n-1} \eta_H(l, k) M^l T^k = \sum_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n} \eta_H(\lambda) \pi(\lambda)\ ,$$

where $\eta_H \in \mathbb{C}^{n^2}$ *is the spreading function of* H.

Proof. Note first that for each k, $\eta_H(\cdot, k)$ is the discrete Fourier transform of the vector $(h_{p,p-k})_{p \in \mathbb{Z}_n}$ and the identity

$$h_{p,p-k} = \sum_{l=0}^{n-1} \eta_H(l, k)\, \omega^{pl}$$

holds for each $p,\ k \in \mathbb{Z}_n$. Given $x \in \mathbb{C}^n$,

$$\begin{aligned} (Hx)_p &= \sum_{k=0}^{n-1} h_{p,k}\, x_k = \sum_{k=0}^{n-1} h_{p,p-k}\, x_{p-k} \\ &= \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} \eta_H(l, k)\, \omega^{pl}\, x_{p-k} = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} \eta_H(l, k) \left(M^l T^k x\right)_p \end{aligned}$$

and the result follows. □

Definition 5. For $\Lambda \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ define $\mathcal{H}_\Lambda = \text{span}\,\{\pi(\lambda),\ \lambda \in \Lambda\} = \{H \in \text{Mat}(n \times n) : \text{supp}\, \eta_H \subseteq \Lambda\}$.

Lemma 2. *Let $g \in \mathbb{C}^n$. The family $\{\pi(\lambda)g\}_{\lambda\in\Lambda}$ is linearly independent if and only if g identifies $\mathcal{H}_\Lambda$.*

Proof. The vector g fails to identify $\mathcal{H}_\Lambda$ if and only if there is an element $H \in \mathcal{H}_\Lambda \setminus \{0\}$ such that $Hg = \sum_{\lambda\in\Lambda} \eta_H(\lambda)\pi(\lambda)g = 0$. But by Lemma 1 $H \neq 0$ if and only if $\eta_H \neq 0$. Hence, g fails to identify H_Λ if and only if $\sum_{\lambda\in\Lambda} \eta_H(\lambda)\pi(\lambda)g = 0$ for some $\eta_H \neq 0$, that is, if and only if $\{\pi(\lambda)g\}_{\lambda\in\Lambda}$ fails to be linearly independent. □

Definition 6. We define the short-time Fourier transform V_g with respect to a window $g \in \mathbb{C}^n$ on $\mathbb{C}^n$ by setting for $f \in \mathbb{C}^n$, $V_g f(\lambda) = \langle f, \pi(\lambda)g\rangle$, $\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n$.

Lemma 3. *If g identifies $\mathcal{H}_\Lambda$ with $|\Lambda| = n$, then $V_g f|_\Lambda \neq 0$ for all $f \neq 0$.*

Proof. If g identifies $\mathcal{H}_\Lambda$ with $|\Lambda| = n$, then by Lemma 2, $\{\pi(\lambda)g\}_{\lambda\in\Lambda}$ is a basis for $\mathbb{C}^n$. Hence, $V_g f(\lambda) \neq 0$ for at least one $\lambda \in \Lambda$ whenever $f \neq 0$. □

Theorem 2. *For $g \in \mathbb{C}^n \setminus \{0\}$, the following are equivalent:*

(1) *$\{\pi(\lambda)g\}_{\lambda\in\mathbb{Z}_n\times\mathbb{Z}_n}$ has the Haar property.*
(2) *$\mathcal{H}_\Lambda$ is identifiable by g if and only if $|\Lambda| \leq n$.*
(3) *For all $f \in \mathbb{C}^n$, $f \neq 0$, the vector $V_g f \in \mathbb{C}^{n^2}$ has at most $n-1$ components which equal 0.*
(4) *For all $f \in \mathbb{C}^n$, $V_g f(\lambda)$ is completely determined by its values on any set Λ with $|\Lambda| = n$.*

Proof.
(1) $\Longleftrightarrow$ (2) This follows immediately from Lemma 2.
(2) $\Longrightarrow$ (3) If (3) does not hold then there is a Λ with $|\Lambda| = n$ such that $V_g f|_\Lambda = 0$ and $f \neq 0$. By Lemma 3 g does not identify $\mathcal{H}_\Lambda$ and hence (2) fails to hold.
(3) $\Longrightarrow$ (1) If (1) does not hold then there is a set $\Lambda \in \mathbb{Z}_n \times \mathbb{Z}_n$ such that $|\Lambda| = n$ and $\{\pi(\lambda)g\}_{\lambda\in\Lambda}$ is not linearly independent. Let f be a nonzero vector perpendicular to span $\{\pi(\lambda)g\}_{\lambda\in\Lambda}$. Then for this f,

$$V_g f(\lambda) = \langle f, \pi(\lambda)g\rangle = 0$$

for all $\lambda \in \Lambda$. Since $|\Lambda| = n$, (3) does not hold.
(1) $\Longrightarrow$ (4) If (1) holds then for any Λ with $|\Lambda| = n$, $\{\pi(\lambda)g\}_{\lambda\in\Lambda}$ is a basis for $\mathbb{C}^n$. If $V_g f(\lambda) = \langle f, \pi(\lambda)g\rangle = 0$ for all $\lambda \in \Lambda$ then $f = 0$ and $V_g f$ is identically zero.
(4) $\Longrightarrow$ (3) If (3) does not hold then there is a $f \neq 0$ such that $V_g f$ has at least n components which vanish. If (4) also holds then $f = 0$, a contradiction. □

Corollary 1. *If $\{\pi(\lambda)g\}_{\lambda\in\mathbb{Z}_n\times\mathbb{Z}_n}$ has the Haar property, then $g_i \neq 0$ and $\widehat{g}_i \neq 0$ for all $i \in \mathbb{Z}_n$.*

Proof. If $g_{i_0} = 0$ for $i_0 \in \mathbb{Z}_n$, choose $f = (1, 0, 0, 0, \ldots, 0)$ and observe that $V_g f(l, i_0) = 0$ for $l \in \mathbb{Z}_n$. Hence, Theorem 2 (3), is not satisfied and $\{\pi(\lambda)g\}_{\lambda\in\mathbb{Z}_n\times\mathbb{Z}_n}$ does not have the Haar property.

To see that $\widehat{g}_i \neq 0$ for all $i \in \mathbb{Z}_n$, note that by a straightforward calculation $(\pi(l,k)g)^\wedge = \omega^{kl}\pi(k,-l)\widehat{g}$ where, as before, the indices are taken modulo n. This

means that

$$V_g f(l,k) = \langle f, \pi(l,k)g\rangle = n\,\omega^{kl}\left\langle \widehat{f}, \pi(k,-l)\widehat{g}\right\rangle = n\,\omega^{kl}\,V_{\widehat{g}}\big(\widehat{f}\big)(k,-l)\ .$$

If $\widehat{g}_{i_0} = 0$ for $i_0 \in \mathbb{Z}_n$, and with $\widehat{f} = (1,0,0,0,\ldots,0)$, then $V_g f(-i_0,k) = 0$ for $k \in \mathbb{Z}_n$ and the result follows as before. □

Corollary 2. *For n prime, $\mathcal{H}_\Lambda$ is identifiable if and only if $|\Lambda| \le n$.*

Proof. This follows immediately from Theorems 1 and 2. □

3.2 Uniform Tight Finite Frames and Channels with Erasures

Definition 7. A *frame* in a Hilbert space is a set of vectors $\{x_k\}_{k\in K}$ with the property that there exist constants $c_1,\ c_2 > 0$, called *frame bounds* such that for all x in the Hilbert space

$$c_1\,\|x\|^2 \le \sum_{k\in K} |\langle x, x_k\rangle|^2 \le c_2\,\|x\|^2\ . \tag{3.1}$$

A frame is *tight* if we can take $c_1 = c_2$ and is *uniform* if $\|x_j\| = \|x_k\|$ for all j and k.

It is obvious that, in an n-dimensional Hilbert space, any collection of $m \ge n$ vectors spanning the space is a (finite) frame for the space.

If our Hilbert space is $\mathbb{C}^n$ then it is convenient to represent a finite frame for $\mathbb{C}^n$, $\{x_k\}_{k=1}^m$, as an $m \times n$ matrix F whose rows are the complex conjugates of the m vectors $\{x_k\}_{k=1}^m$. In this case, the frame coefficients of a vector x are given by the vector Fx, the sum in (3.1) reduces to $\langle x, F^*Fx\rangle$, and the inequality (3.1) can be written as $c_1\,I \le F^*F \le c_2\,I$. The frame is tight if and only if F^*F is a multiple of the identity matrix.

Proposition 2. *For any $g \ne 0$, the collection $\{\pi(\lambda)g\}_{\lambda\in\mathbb{Z}_n\times\mathbb{Z}_n}$ is a uniform tight finite frame for $\mathbb{C}^n$ with frame bound $c_1 = c_2 = n^2\,\|g\|^2$.*

Proof. Let $F = G(g)^*$ where $G(g)$ is given by (2.1). Then the rows of F are the complex conjugates of the elements of the Gabor system $\{\pi(\lambda)g\}_{\lambda\in\mathbb{Z}_n\times\mathbb{Z}_n}$. Specifically

$$F = \begin{pmatrix} W_n^*\,D_0^* \\ W_n^*\,D_1^* \\ \cdots \\ W_n^*\,D_{n-1}^* \end{pmatrix}$$

so that

$$\begin{aligned} F^*F &= D_0\,W_n\,W_n^*\,D_0^* + D_1\,W_n\,W_n^*\,D_1^* + \cdots + D_{n-1}\,W_n\,W_n^*\,D_{n-1}^* \\ &= n\left(D_0\,D_0^* + D_1\,D_1^* + \cdots + D_{n-1}\,D_{n-1}^*\right) \\ &= \left(n^2\sum_{k=0}^{n-1}|g_k|^2\right) I \end{aligned}$$

and $\{\pi(\lambda)g\}_{\lambda\in\mathbb{Z}_n\times\mathbb{Z}_n}$ is a tight frame for $\mathbb{C}^n$. Moreover, it is clear that

$$\|\pi(\lambda)g\| = \left(\sum_{k=0}^{n-1}|g_k|^2\right)^{1/2}$$

for each $\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n$ so that the frame is also uniform. □

The basic problem we are interested in is the transmission of information in the form of a vector $x \in \mathbb{C}^n$ over a channel in such a way that recovery of the information at the receiver is robust to errors introduced by the channel. In the particular model of interest we first transform the signal x by forming $y = Fx \in \mathbb{C}^m$. This vector is then quantized in some fashion yielding $\widehat{y} = Q(y)$. In other words, we transmit not x but the quantized frame coefficients of x. Each such quantized coefficient is considered a *packet* of data sent over the channel. It is assumed that the channel distorts the transmitted vector by erasing packets at random. Robustness to this sort of distortion means maximizing the number of packets that can be erased while still allowing reconstruction of the signal as accurately as possible from the remaining packets. For more, see [7, 9, 15] and the references cited therein.

Definition 8 ([6]). A frame $\mathcal{F} = \{x_k\}_{k=1}^m$ in $\mathbb{C}^n$ is *maximally robust to erasures* if the removal of any $l \leq m - n$ vectors from $\mathcal{F}$ leaves a frame.

If the rows of F form a frame that is maximally robust to erasures, and if no more than $m - n$ packets are erased by our theoretical channel then the error in the reconstructed signal $\widehat{x}$ recovered from the received packets will be due entirely to quantization error in the coefficients $\widehat{y}$. Indeed, if the quantization error is modelled as zero-mean uncorrelated noise, the mean square error of the reconstructed signal is minimized if and only if the frame is uniform and tight (Theorem 3.1, [6]).

The above discussion is summarized in the following theorem.

Theorem 3. *The following are equivalent.*

(1) $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$ *has the Haar property.*
(2) $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$ *is maximally robust to erasures.*
(3) *The $n^2 \times n$ matrix F whose rows are the complex conjugates of the vectors in the Gabor system $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$ has the property that every minor of order n is nonzero.*

Corollary 3. *For n prime there exists $g \in \mathbb{C}^n$ such that the tight Gabor frame $\{\pi(\lambda)g\}_{\lambda \in \mathbb{Z}_n \times \mathbb{Z}_n}$ is maximally robust to erasures.*

Proof. Follows immediately from Theorem 1. □

4. Minors of Full Gabor System Matrices

The goal of this section is to prove Theorem 4 which, in light of Proposition 1, is a generalization of Theorem 1.

Theorem 4. *If n is prime then there exists a dense open set E of full measure*[2] *in $\mathbb{C}^n$ such that if $g \in E$ then every minor of $G = G(g)$ is nonzero.*

Before getting to the proof, we specify in the following two subsections some notation and basic results from the theory of determinants.

[2] In fact E is the complement of the union of the zero sets of finitely many homogeneous polynomials in n complex variables.

4.1 Basic Results on Determinants

The following is adapted from [12], Chapter 2 and [1], Chapter 6.

Definition 9. The *determinant* of an $n \times n$ matrix $A = (a_{i,j})_{i,j=1}^{n}$, denoted $\det(A)$, is defined to be

$$\det(A) = \sum_{j} (-1)^{t(j)} a_{1j_1} a_{2,j_2} \cdots a_{nj_n} \tag{4.1}$$

where $j = (j_1, j_2, \ldots, j_n)$ runs through all permutations of $\{1, 2, \ldots, n\}$ and $t(j)$ is the parity of j. Given an $m \times n$ matrix A and $1 \le p \le \min(m, n)$, the determinant of a $p \times p$ submatrix of A obtained by deleting $m - p$ rows and $n - p$ columns is called a *minor of order* p of A. If the p rows and columns retained have indices given by $i = (i_1, i_2, \ldots, i_p)$ with $i_1 < i_2 < \cdots < i_p$ and $j = (j_1, j_2, \ldots, j_p)$ with $j_1 < j_2 < \cdots < j_p$, respectively, then the corresponding minor of order p is denoted

$$A \begin{pmatrix} i_1 & i_2 & \cdots & i_p \\ j_1 & j_2 & \cdots & j_p \end{pmatrix} \equiv A \begin{pmatrix} i \\ j \end{pmatrix} .$$

The proof of the following theorem is found in [1], Section 35.

Theorem 5 (Extended Laplace Expansion). *Let A be an $n \times n$ matrix and let s be a partition of the column indices of A, that is, $s = (s_1, s_2, \ldots, s_m)$ where s_k is a set of p_k column indices such that $s_k \cap s_{k'} = \emptyset$ when $k \neq k'$ and where $p_1 + \cdots + p_m = n$. Then*

$$\det(A) = \sum_{t} (-1)^{\sum_{k=1}^{m} |s_k| + |t_k|} A \begin{pmatrix} t_1 \\ s_1 \end{pmatrix} A \begin{pmatrix} t_2 \\ s_2 \end{pmatrix} \cdots A \begin{pmatrix} t_m \\ s_m \end{pmatrix} \tag{4.2}$$

where $t = (t_1, t_2, \ldots, t_m)$ runs through all

$$\binom{n}{p_1} \binom{n - p_1}{p_2} \cdots \binom{n - p_1 - \cdots - p_{m-1}}{p_m}$$

partitions of the row indices into subsets of size $(p_1, p_2, \ldots, p_m)$.

Note that each term of the sum in (4.2) contributes exactly $p_1! p_2! \cdots p_m!$ terms to the sum in (4.1) which defines $\det(A)$ and that

$$\binom{n}{p_1} \binom{n - p_1}{p_2} \cdots \binom{n - p_1 - \cdots - p_{m-1}}{p_m} p_1! p_2! \cdots p_m! = n! ,$$

thereby accounting for all terms in this sum.

4.2 Generalized Vandermonde Determinants

The proof of Theorem 4 requires the following lemma, proved in [5]. The proof is algebraic in nature and we will describe it briefly below with the notation of [5].

Lemma 4. *If n is prime then every minor of the discrete Fourier matrix W_n is nonzero.*

Definition 10. Given a p-tuple $a = (a_0, a_1, \ldots, a_{p-1})$ of distinct nonnegative integers and a point $x = (x_0, x_1, \ldots, x_{p-1}) \in \mathbb{C}^p$, let

$$V_a(x) = V_a(x_0, x_1, \ldots, x_{p-1})$$

be the determinant of the matrix $(x_k^{a_l})_{k,l=0}^{p-1}$. $V_a(x)$ is referred to as a *generalized Vandermonde determinant.*

With $s = (0, 1, \ldots, p-1)$,

$$V_s(x) = V_s(x_0, x_1, \ldots, x_{p-1}) = \prod_{0 \le k < l \le p} (x_k - x_l)$$

is the standard Vandermonde determinant and does not vanish if and only if the x_k are distinct. Let $W_n \binom{i}{j}$ be a minor of order p of the Fourier matrix W_n. Then

$$W_n \binom{i}{j} = V_j\left(\omega^{i_0}, \omega^{i_1}, \ldots, \omega^{i_{p-1}}\right)$$

where $\omega = e^{2\pi i/n}$. The polynomial $P_a(x) = V_a(x)/V_s(x)$ is a homogeneous polynomial in x with integer coefficients.[3]

The following fundamental results are due to Mitchell [14] (see [5] for elementary proofs and interesting consequences of these results).

Theorem 6. *Let $a = (a_0, \ldots, a_{p-1})$ with $0 \le a_0 < a_1 < \cdots < a_{p-1}$. Then all the coefficients of the polynomial $P_a(x)$ are nonnegative.*

Theorem 7. *Let $a = (a_0, \ldots, a_{p-1})$. Then the sum of the coefficients of $P_a(x)$ is*

$$V_s(a_0, a_1, \ldots, a_{p-1})/V_s(0, 1, \ldots, p-1)\ .$$

In other words,

$$P_a(1, 1, \ldots, 1) = \frac{V_s(a_0, a_1, \ldots, a_{p-1})}{V_s(0, 1, \ldots, p-1)} = \prod_{0 \le k < l \le p} \frac{(a_k - a_l)}{(k - l)}\ .$$

Suppose that

$$W_n \binom{i}{j} = V_j\left(\omega^{i_0}, \omega^{i_1}, \ldots, \omega^{i_{p-1}}\right) = 0$$

and consider the polynomial in $z \in \mathbb{C}$ defined by

$$P(z) = \frac{V_j\left(z^{i_0}, z^{i_1}, \ldots, z^{i_{p-1}}\right)}{V_s\left(z^{i_0}, z^{i_1}, \ldots, z^{i_{p-1}}\right)} = \frac{V_j\left(z^{i_0}, z^{i_1}, \ldots, z^{i_{p-1}}\right)}{\prod_{0 \le k < l \le p}\left(z^{i_k} - z^{i_l}\right)}\ . \tag{4.3}$$

Since n is prime and since the $0 \le i_k \le n-1$ are distinct integers the denominator of the last term in (4.3) is nonzero when $z = \omega$, and since its numerator is assumed to vanish, $P(\omega) = 0$. Moreover, $P(\omega) = 0$ implies that P is divisible by $z^{n-1} + z^{n-2} + \cdots + z + 1$ in $\mathbb{Z}[z]$.[4] Consequently, $P(1)$ is an integer multiple of n.

[3] It follows by direct calculation that for each $k < l$, $(x_k - x_l)$ divides $V_a(x)$. Since $\mathbb{Z}[x]$ is a unique factorization domain [10], p. 164, Theorem 6.14, and since $(x_k - x_l)$ is irreducible, $V_a(x)/V_s(x)$ is a polynomial. That it is homogeneous follows from the fact that a polynomial P is homogeneous of degree k if and only if $P(ax) = a^k P(x)$.

[4] That P is divisible by $z^{n-1} + z^{n-2} + \cdots + z + 1$ in $\mathbb{Q}[z]$ follows from the fact that $I = \{f \in \mathbb{Q}[z] : f(\omega) = 0\}$ is an ideal in the principle ideal domain $\mathbb{Q}[z]$ generated by $z^{n-1} + z^{n-2} + \cdots + z + 1$ [10], p. 123. That P also factors in $\mathbb{Z}[z]$ is an application of Gauss' Lemma, [13], p. 181.

Now, by Theorem 7, it also holds that

$$P(1) = \prod_{0 \le k < l \le p} \frac{(j_k - j_l)}{(k - l)} \, .$$

However, since $0 \le j_k \le n - 1$ and all j_k are distinct, $P(1) \neq 0$ cannot be a multiple of n since in that case n would be the product of integers strictly less than n contradicting the assertion that n is prime. Hence, $W_n \begin{pmatrix} i \\ j \end{pmatrix}$ is not zero and Lemma 4 is proved.

4.3 Proof of Theorem 4

Fix $1 \le l \le n$ and let M be an $l \times l$ submatrix of $G(g)$ [given by (2.1)] formed by deleting $n^2 - l$ columns and $n - l$ rows of $G(g)$. Associate to M the n-tuple $(l_0, l_1, \ldots, l_{n-1})$ where l_k is the number of columns of the matrix $D_k \cdot W_n$ that appear in M (see (2.1) and Example 2).

Note that $\det(M)$ is a homogeneous polynomial of degree l in the variables $g_0, g_1, \ldots, , g_{n-1}$ and can be written uniquely in the form

$$\sum_{\substack{\alpha \in \mathbb{Z}_+^n \\ |\alpha| = l}} a_\alpha \, g_0^{\alpha_0} g_1^{\alpha_1} \cdots g_{n-1}^{\alpha_{n-1}} \, .$$

It will be sufficient to show that this polynomial does not vanish identically by finding a multiindex α with $|\alpha| = l$ such that $a_\alpha \neq 0$. We define this multiindex and its corresponding monomial by means of the following recursive algorithm.

Definition 11. The minor $\det(M)$ is formally a sum of $l!$ monomials in $g_0, g_1, \ldots, g_{n-1}$. Of those monomials that formally appear in this sum we define p_M recursively as follows. If $l = 1$ then M is simply a multiple of a single variable g_j and we define $p_M = g_j$. For $l > 1$, let g_j be the variable of lowest index appearing in M. Choose any entry of M in which g_j appears, eliminate from M the row and column containing that entry, and call the remaining matrix M'. Define $p_M = g_j \, p_{M'}$.

Of course it now must be argued that this definition makes sense, that is, that the monomial p_M is uniquely determined by M. It is clear that what must be shown is that the choice of the term in M containing the variable g_j does not affect the variable of least index appearing in M'. So suppose that g_j is the variable of lowest index appearing in M. There are three possibilities. (i) the variable g_j appears in more than one row of M, (ii) the variable g_j appears in exactly one row and more than one column of M, and (iii) the variable g_j appears in exactly one row and one column of M.

Consider case (i). Because M is a submatrix of $G(g)$, and because of the structure of $G(g)$ given in (2.1), it follows that the variable g_j cannot appear twice in the same column of M. Hence, no matter which term containing g_j is chosen, the variable g_j will still appear in the reduced matrix M', and will be the variable of least index appearing in M'.

Consider case (ii). Again by the structure of $G(g)$, and since M is a submatrix of $G(g)$, the columns in which g_j appears must come from the same submatrix $D_k \cdot W_n$ of $G(g)$. Consequently, the variables appearing in each such column are the same and appear in the same order in each column. Hence, all the variables that are removed by eliminating one of the columns in which g_j appears still appear in the reduced matrix M'. Hence, the term of lowest index in M' is unaffected.

Consider case (iii). In this case, there is no ambiguity about which row and column to eliminate so M' is uniquely determined.

Lemma 5. *The number of diagonals of M whose product is a multiple of the monomial p_M is $\prod_{k=0}^{n-1} l_k!$.*

Proof. For any submatrix M of $G(g)$, we define $\mu(M)$ to be the number of diagonals of M whose product is a multiple of p_M. The proof proceeds by induction on l. If $l = 1$ then the result is obvious. Let M be given with its associated n-tuple $(l_0, l_1, \ldots, l_{n-1})$. We may assume without loss of generality that the variable of smallest index in p_M with a nonzero exponent is g_0. In this case, there is a row of M in which the variable g_0 appears l_j times for some index j. Choose one of these terms and delete the row and column in which it appears. Call the remaining matrix M'. The n-tuple associated with M' is $(l_0, \ldots, l_{j-1}, l_j - 1, l_{j+1}, \ldots, l_{n-1})$, and this n-tuple does not depend on which term was chosen from the given row to form M'. By Definition 11, $p_M = g_0\, p_{M'}$ and by the induction hypothesis

$$\mu\big(M'\big) = l_0! \cdots l_{j-1}!\,(l_j - 1)!\,l_{j+1}! \cdots l_{n-1}!\,.$$

Since there are l_j ways to choose a term from the given row to produce M' we have that

$$\mu(M) = l_j\,\mu\big(M'\big) = l_0! \cdots l_{j-1}!\,l_j(l_j - 1)!\,l_{j+1}! \cdots l_{n-1}! = \prod_{k=0}^{n-1} l_k!$$

which was to be proved. □

Proof of Theorem 4. Let $s = (s_1, s_2, \ldots, s_m)$ be the partition of the column indices of M defined as follows. Let $0 \le j_1 < j_2 < \cdots < j_m < n$ be such that $l_{j_k} > 0$ and let s_k be the set of those l_{j_k} column indices of M corresponding to columns chosen from the submatrix $D_{j_k} \cdot W_n$ of $G(g)$ (cf. Example 2). By (4.2), $\det(M)$ is given by the sum

$$\det(M) = \sum_t (-1)^{\sum_{k=1}^m |s_k| + |t_k|}\, M\begin{pmatrix} t_1 \\ s_1 \end{pmatrix} M\begin{pmatrix} t_2 \\ s_2 \end{pmatrix} \cdots M\begin{pmatrix} t_m \\ s_m \end{pmatrix} \tag{4.4}$$

where the sum runs over all partitions of the row indices of M for which t_k is the same size as s_k. Note that each term in this sum is a multiple of a monomial of degree l in the variables $g_0, g_1, \ldots, g_{n-1}$.

We will now choose a term in this sum that is a nonzero multiple of the monomial p_M. That is, we will choose a particular $t = (t_1, t_2, \ldots, t_m)$ with the property that the product

$$M\begin{pmatrix} t_1 \\ s_1 \end{pmatrix} M\begin{pmatrix} t_2 \\ s_2 \end{pmatrix} \cdots M\begin{pmatrix} t_m \\ s_m \end{pmatrix} \tag{4.5}$$

is a nonzero multiple of p_M. Define this partition as follows. Choose any diagonal of M whose product is formally a multiple of p_M. Define t_k to be the set of row indices of M such that the term in the chosen diagonal in that row is in one of the columns whose index is in s_k. Then for each k, the submatrix of M formed by choosing the columns indexed by s_k and the rows indexed by t_k has the property that the same variable g_j appears in each row of the submatrix. Hence, the minor $M\begin{pmatrix} t_k \\ s_k \end{pmatrix}$ is a product of these variables and of a minor of the Fourier matrix W_n. Moreover, the product of all the variables that appear in

each of the submatrices is precisely p_M. Finally, we conclude that the quantity in (4.5) is p_M multiplied by a coefficient which is the product of m minors of W_n. By Lemma 4 this coefficient is nonzero.

Finally, we assert that the term in the sum (4.4) described above is the only one that is a multiple of p_M. To see why this is true note that the product (4.5) represents $\prod_{k=0}^{n-1} l_k!$ terms in the sum for $\det(M)$ given by (4.1). However, by Lemma 5 this is precisely the number of terms in the sum (4.1) for $\det(M)$ in which the monomial p_M formally appears. Hence, the coefficient of p_M in $\det(M)$ is nonzero and the polynomial $\det(M)$ is not identically zero.

Let $\mathcal{Z}(M)$ be the set of zeros of $\det(M)$ and define $E^c = \cup_M \mathcal{Z}(M)$ where M runs through all $l \times l$ submatrices of $G(g)$, $1 \le l \le n$. Since this is a finite union and since each set $\mathcal{Z}(M)$ has measure zero, is closed, and has empty interior, E is an open dense subset of $\mathbb{C}^n$ of full measure. Clearly if $g \in E$ then every minor of the matrix $G(g)$ is nonzero. $\square$

Example 2. The matrix

$$M = \left(\begin{array}{cc|ccc|c} \omega^0 g_2 & \omega^0 g_2 & \omega^0 \underline{g_3} & \omega^0 g_3 & \omega^0 g_3 & \omega^0 g_6 \\ \omega^1 g_3 & \omega^2 g_3 & \omega^0 g_4 & \omega^2 g_4 & \omega^5 g_4 & \omega^3 \underline{g_0} \\ \omega^2 g_4 & \omega^4 g_4 & \omega^0 g_5 & \omega^4 \underline{g_5} & \omega^3 g_5 & \omega^6 g_1 \\ \omega^3 g_5 & \omega^6 g_5 & \omega^0 g_6 & \omega^6 g_6 & \omega^1 \underline{g_6} & \omega^2 g_2 \\ \omega^5 \underline{g_0} & \omega^3 g_0 & \omega^0 g_1 & \omega^3 g_1 & \omega^4 g_1 & \omega^1 g_4 \\ \omega^6 g_1 & \omega^5 \underline{g_1} & \omega^0 g_2 & \omega^5 g_2 & \omega^2 g_2 & \omega^4 g_5 \end{array}\right)$$

gives an exemplary submatrix M of $G(g)$ in the case $n = 7$.

M is obtained by removing the row of $G(g)$ with index 4, and all columns with indices not in $\{15, 16, 21, 23, 26, 45\}$. Recall that rows and columns are numbered starting with 0 in this article. Underlined are the appearances of g_j which contribute to the construction of p_M which is given by $p_M(g) = g_0^2 g_1 g_3 g_6$.

The 7-tuple assigned to M in the proof of Theorem 4 is

$$(l_0, l_1, \dots, l_{n-1}) = (0, 0, 2, 3, 0, 0, 1)\ ,$$

and the partition s is given by

$$s = (s_1, s_2, s_3) = (\{15, 16\}, \{21, 23, 26\}, \{45\})\ .$$

We conclude that $t_1 = \{4, 5\}$, $t_2 = \{0, 2, 3\}$, and $t_3 = \{1\}$.

We have

$$\begin{aligned} & M\begin{pmatrix} t_1 \\ s_1 \end{pmatrix} M\begin{pmatrix} t_2 \\ s_2 \end{pmatrix} M\begin{pmatrix} t_3 \\ s_3 \end{pmatrix} \\ =& \det\begin{pmatrix} \omega^5 \underline{g_0} & \omega^3 g_0 \\ \omega^6 g_1 & \omega^5 \underline{g_1} \end{pmatrix} \det\begin{pmatrix} \omega^0 \underline{g_3} & \omega^0 g_3 & \omega^0 g_3 \\ \omega^0 g_5 & \omega^4 \underline{g_5} & \omega^3 g_5 \\ \omega^0 g_6 & \omega^6 g_6 & \omega^1 \underline{g_6} \end{pmatrix} \cdot \det\left(\omega^3 \underline{g_0}\right) \\ =& g_0^2 g_1 g_3 g_6 \cdot \det\begin{pmatrix} \omega^5 & \omega^3 \\ \omega^6 & \omega^5 \end{pmatrix} \det\begin{pmatrix} \omega^0 & \omega^0 & \omega^0 \\ \omega^0 & \omega^4 & \omega^3 \\ \omega^0 & \omega^6 & \omega^1 \end{pmatrix} \cdot \omega^3 \end{aligned}$$

and this coefficient of $g_0^2 g_1 g_3 g_6$ is nonzero by Lemma 4. The counting argument in the proof of Theorem 4 shows that $p_M(g)$ appears with this coefficient in $\det M$.

Acknowledgments

The authors acknowledge the helpful insights provided for this article by the late Des Sheiham of the International University Bremen. The article is dedicated to his memory.

References

[1] Aitken, A. C. (1939). *Determinants and Matrices,* Oliver and Boyd, Ltd., Edinburgh.

[2] Bello, P. A. (1969). Measurement of random time-variant linear channels, *IEEE Trans. Inform. Theory* **IT-15**(4), (July).

[3] Casazza, P. G. and Kovačević, J. (2003). Equal-norm tight frames with erasures, *Adv. Comput. Math.* **18**(2-4), 387–430.

[4] Cheney, E. W. (1998). *Introduction to Approximation Theory,* AMS Chelsea Publishing, Providence, RI.

[5] Evans, R. J. and Isaacs, I. M. (1976). Generalized Vandermonde determinants and roots of unity of prime order, *Proc. Amer. Math. Soc.* **58**, 51–54.

[6] Goyal, V. K., Kovačević, J., and Kelner, J. (2001). Quantized frame expansions with erasures, *Appl. Comput. Harmon. Anal.* **10**(3), 203–233.

[7] Goyal, V. K., Kovačević, J., and Vetterli, M. (1998). Multiple description transform coding: Robustness to erasures using tight frame expansions in *Proc. IEEE Int. Symp. Inform. Th.* Cambridge, MA, August,

[8] Heil, C. Linear independence of finite Gabor systems in *Harmonic Analysis and Applications,* Heil, C., Ed., Birkhäuser, Boston, to appear.

[9] Holmes, R. B. and Paulsen, V. I. (2004). Optimal frames for erasures, *Linear Algebra Appl.* **377**, 31–51.

[10] Hungerford, T. W. (1974). *Algebra, Springer Edition,* Springer-Verlag, New York.

[11] Kozek, W., and Pfander, G. E. (2005). Identification of operators with bandlimited symbols, *SIAM J. Math. Anal.,* to appear.

[12] Lancaster, P. and Tismenetsky, M. (1985). *The Theory of Matrices, Second Edition with Applications,* Academic Press, New York.

[13] Lang, S. (1993). *Algebra,* 3rd ed., Addison-Wesley Publishing Company.

[14] Mitchell, O. H. (1881). Note on determinants of powers, *Amer. J. Math.* **4**(1-4), 341–344.

[15] Strohmer, T. and Heath, Jr., R. W. (2003). Grassmannian frames with applications to coding and communication, *Appl. Comput. Harmon. Anal.* **14**(3), 257–275.

Received March 16, 2005

Revision received October 01, 2005

Department of Mathematical Sciences, George Mason University, Fairfax, VA 22030
e-mail: lawrence@gmu.edu

School of Engineering and Science, International University Bremen, 28759 Bremen, Germany
e-mail: g.pfander@iu-bremen.de

Department of Mathematical Sciences, George Mason University, Fairfax, VA 22030,
e-mail: dwalnut@gmu.edu