Spanning families of the form $m_j = \gamma \circ f_j$

Brian Preskitt

May 30, 2018

1 Notation

- Indices of matrices in $\mathbb{C}^{d\times d}$ and vectors in $\mathbb{C}^d$ are always taken modulo d.
- For $k \in \mathbb{N}, n \in \mathbb{Z}, [k]_n = \{n, n+1, \ldots, n+k-1\}$ and $[k] = [k]_1$.
- $S_d \in \mathbb{R}^{d\times d}$ is the $d \times d$ shift operator, such that $(S_d x)_i = x_{i-1}$. Typically we imply the subscript by context, writing S.
- $R \in \mathbb{R}^{d\times d}$ is the operator that reverses a vector's entries, leaving the first entry fixed. Namely, $(Rx)_i = x_{2-i}$.
- Given $x \in \mathbb{C}^d$ and $k \in [d], \mathrm{circ}_k(x) \in \mathbb{C}^{d\times k}$ denotes the first k columns of the circulant matrix whose first column is x. In particular, $\mathrm{circ}_k(x)e_i = S^{i-1}x$ for $i \in [k]$. When the subscript is omitted, $\mathrm{circ}(x) = \mathrm{circ}_d(x)$.
- $\omega_d := \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}$ is the d^{th} root of unity. When context permits, d is implied and we use just ω.
- For $i, n \in \mathbb{N}, e_i^n \in \mathbb{R}^n$ is the i^{th} column of the $n \times n$ identity matrix. When context permits, n is implied and we write e_i. In particular, whenever e_i is used in a matrix multiplication, n is taken to be appropriate so that the multiplication is legal.
- For $k \in \mathbb{Z}, F_k \in \mathbb{C}^{k\times k}$ is the $k \times k$ unitary Fourier matrix with $(F_k)_{ij} = \frac{1}{\sqrt{k}}\omega_k^{(i-1)(j-1)}$.
- For $m, n \in \mathbb{N}, f_n^m = F_m e_n$ is the n^{th} column of the $m \times m$ unitary Fourier matrix, where $e_n \in \mathbb{R}^m$ has its index taken modulo m.
- Given $x, y \in \mathbb{C}^d, x \circ y$ denotes the Hadamard/elementwise product of x and y; specifically $(x \circ y)_i = x_i y_i$.
- Given $A \in \mathbb{C}^{d\times d}, \mathrm{diag}(A, m) \in \mathbb{C}^d$ denotes the m^{th} circulant off-diagonal of A. That is, $\mathrm{diag}(A, m)_i = A_{i,i+m}$.
- Given $x \in \mathbb{C}^d, \mathrm{diag}(x) \in \mathbb{C}^{d\times d}$ is the diagonal matrix whose diagonal entries are the entries of x. Namely, $\mathrm{diag}(x)e_i = x_i e_i$. When the intention is clear from context, we may write $D_x := \mathrm{diag}(x)$.
- $\mathcal{H}^d$ is the set of Hermitian matrices in $\mathbb{C}^{d\times d}$, to be viewed as a d^2-dimensional vector space over $\mathbb{R}$.

- $\mathcal{R}_d : \bigcup_{k=1}^{\infty} \mathbb{C}^k \to \mathbb{C}^d$ is a resize mapping, where for $v \in \mathbb{C}^k$ and $i \in [d]$,

$$\mathcal{R}_d(v)_i = \begin{cases} v_i, & i \leq k \\ 0, & \text{otherwise} \end{cases} \quad \text{for } i \in [d]$$

- Given $k, d \in \mathbb{N}$, we define the operator $T_k : \mathbb{C}^{d \times d} \to \mathbb{C}^{d \times d}$ by

$$T_k(A)_{ij} = \begin{cases} A_{ij}, & |i-j| \mod d < k \\ 0, & \text{otherwise.} \end{cases}$$

  Note that T_k is simply the orthogonal projection operator onto its range $T_k(\mathbb{C}^{d \times d})$. We use T_k interchangeably to refer to both the operator and its range.

2 Necessary and sufficient conditions for a spanning family

In this chapter, we consider when a local measurement system $\{m_j\}_{j=1}^K$ composes a *spanning family* of masks.

Definition 1. We say that $\{m_j\}_{j=1}^K \subseteq \mathbb{C}^d$ is a *local measurement system* or *family of masks* of support δ if $1 \in \text{supp}(m_j)$ and $\text{supp}(m_j) \subseteq [\delta]$ for each j.

Definition 2. We say that a family of masks $\{m_j\}_{j=1}^K \subseteq \mathbb{C}^d$ of support δ is a *spanning family* if $\text{span}\{S^\ell m_j m_j^* S^{-\ell}\}_{(\ell,j) \in [d]_0 \times [K]} = T_\delta(\mathcal{H}^d)$.

Conditions for a spanning family

Proposition 1. *Suppose that $\gamma \in \mathbb{R}^d$ has $1 \in \text{supp}(\gamma) = [\delta]$. Set $D = \min\{2\delta - 1, d\}$, take $K \geq 2\delta - 1$ and let*

$$\begin{matrix} v_j = \\ v_j^D = \end{matrix} \begin{matrix} \sqrt{K}\mathcal{R}_d(F_K e_j) \\ \sqrt{K}\mathcal{R}_D(F_K e_j) \end{matrix}, \quad j \in [D],\ 2\delta - 1 \leq K.$$

Define a local measurement system $\{m_j\}_{j \in [D]}$ by setting $m_j = \gamma \circ v_j$. Then $\{m_j\}_{j \in [D]}$ is a spanning family if and only if all the sets $J_k := \{m \in [\delta]_0 : (F_d(\gamma \circ S^{-m}\gamma))_k \neq 0\}$, for all $k \in [d]$ satisfy

$$\begin{cases} 2|J_k| - 1 \geq D, & 0 \in J_k \\ 2|J_k| \geq D, & \textit{otherwise} \end{cases}.$$

The proof will make use of the following lemmas.

Lemma 1. *Define $w_j = \mathcal{R}_{N_1}(f_j^{N_2}), j \in [N_2]$ and set*

$$\rho_j = \mathfrak{Re}(w_j) \quad \textit{and} \quad \mu_j = \mathfrak{Im}(w_j)$$

to be vectors containing the real and imaginary components of w_j. Then for $1 \leq \ell_1 < \cdots < \ell_k \leq \frac{N_2+1}{2}$ with $k \leq N_1$, we have

$$\begin{aligned} \dim \text{span}\{w_{\ell_i}, w_{2-\ell_i}\}_{i=1}^k &= \dim \text{span}\{\rho_{\ell_i}, \mu_{\ell_i}\}_{i=1}^k \\ &= \begin{cases} 2k-1, & \ell_1 = 1 \\ 2k, & \textit{otherwise} \end{cases}, \end{aligned}$$

where the indices are taken modulo N_2.

Proof of lemma 1. The first equality is clear by considering that $w_{2-i} = \overline{w_i}$, so $\rho_k = \frac{1}{2}(w_i + w_{2-i})$ and $\mu_i = -\frac{i}{2}(w_i - w_{2-i})$. We set $M = \dim \operatorname{span}\{w_{\ell_i}, w_{2-\ell_i}\}_{i=1}^k$ to be the common dimension of the two spaces under consideration.

We now divide into two cases: if $N_1 < N_2$, then $\{w_j\}_{j\in[N_2]}$ is full spark, as any $N_1 \times N_1$ submatrix of $\begin{bmatrix} w_1 & \cdots & w_{N_2} \end{bmatrix}$ will be a Vandermonde matrix of the form

$$V = \frac{1}{\sqrt{N_2}} \begin{bmatrix} w_{\ell_1} & \cdots & w_{\ell_{N_1}} \end{bmatrix}$$

with determinant

$$N_2^{-N_1/2} \prod_{1\le i<j\le N_1} (\omega_{N_2}^{\ell_i - 1} - \omega_{N_2}^{\ell_j - 1}),$$

which is immediately non-zero since $\omega_{N_2}^{\ell_i-1} - \omega_{N_2}^{\ell_j-1} = 0$ only when $\ell_i - \ell_j = 0 \mod N_2$, which cannot happen when $N_1 < N_2$.

When $N_1 \ge N_2, \{w_j\}_{j\in[N_2]}$ is linearly independent, since its members form the matrix $\begin{bmatrix} F_{N_2} \\ 0_{N_1 - N_2 \times N_2} \end{bmatrix}$.

In either case, M is equal to the cardinality of $\{\ell_i, 2-\ell_i\}_{i=1}^k$, which has $2k-1$ elements if and only if $\ell_1 = 1$; otherwise it has $2k$. We remark that a collision where $\ell_i = (2 - \ell_i \mod N_2) = N_2/2 + 1$ is precluded since we have asserted $\ell_i \le \frac{N_2+1}{2}$.

□

Lemma 2. *For $v \in \mathbb{R}^d$, we have*

$$\operatorname{circ}(v)\rho_k^d = \frac{1}{2}\mathfrak{Re}((Fv)_k f_k^d) \tag{1}$$

$$\operatorname{circ}(v)\mu_k^d = \frac{1}{2}\mathfrak{Im}((Fv)_k f_k^d). \tag{2}$$

In particular, if $(Fv)_k \neq 0$ and $k \notin \{1, \frac{d}{2}+1\}$, then $\rho_k^d, \mu_k^d \notin \operatorname{Nul}(\operatorname{circ}(v))$; if $k \in \{1, \frac{d}{2}+1\}$, then $\rho_k^d \notin \operatorname{Nul}(\operatorname{circ}(v))$ and $\mu_k^d = 0$. On the other hand, if $(Fv)_k = 0$, then $\rho_k^d, \mu_k^d \in \operatorname{Nul}(\operatorname{circ}(v))$.

Proof of lemma 2. We set $\lambda_k^d = (Fv)_k$, and recalling that $\operatorname{circ}(v) = F \operatorname{diag}(Fv) F^*$, we observe that

$$\begin{aligned}\operatorname{circ}(v)\mu_k^d &= \operatorname{circ}(v)\frac{1}{2}(f_k^d + f_{2-k}^d) = \frac{1}{2}(\operatorname{circ}(v)f_k^d + \operatorname{circ}(v)f_{2-k}^d) \\ &= \frac{1}{2}(\lambda_k^d f_k^d + \lambda_{2-k}^d f_{2-k}^d).\end{aligned}$$

(1) follows immediately since $\lambda_k^d = \overline{\lambda_{2-k}^d}$ when $v \in \mathbb{R}^D$. (2) follows from an analogous calculation.

If $\lambda_k^d \neq 0$ and $k \notin \{1, \frac{d}{2}+1\}$, then ω_d^{k-1} is a non-real root of unity and there exists some j such that $\mathfrak{Re}(\omega_d^{(j-1)(k-1)}\lambda_k^d) \neq 0$, and similarly for $\mathfrak{Im}(\omega_d^{(j-1)(k-1)}\lambda_k^d) \neq 0$. When

$k \in \{1, \frac{d}{2}+1\}, \omega_d^{(k-1)} \in \mathbb{R}$ so $\mu_k^d = 0$, but $\lambda_k^d \in \mathbb{R}$ in this case (because $v \in \mathbb{R}^d$), so $\mathrm{circ}(v)\rho_k^d = \lambda_k^d \rho_k^d \neq 0$. The claim concerning the case of $\lambda_k^d = 0$ is immediate from (1) and (2). □

Proof of proposition 1. For this proof, we set

$$\begin{aligned}(\rho_k^d, \mu_k^d) &= (\mathfrak{Re}(f_k^d), \mathfrak{Im}(f_k^d))\\ (\rho_k, \mu_k) &= (\mathfrak{Re}(v_k), \mathfrak{Im}(v_k))\\ (\rho_k^D, \mu_k^D) &= (\mathfrak{Re}(v_k^D), \mathfrak{Im}(v_k^D))\end{aligned}$$

We consider the conditions under which a linear combination of the matrices $B_\gamma := \{S^\ell m_j m_j^* S^{-\ell}\}_{(\ell,j)\in[d]\times[D]}$ can be equal to zero; by a basic dimension count, $\{m_j\}_{j\in[D]}$ is a spanning family if and only if B_γ is linearly independent. To this end, we define the operator $\mathcal{A} : \mathbb{R}^{d\times D} \to \mathbb{C}^{d\times d}$ by

$$\mathcal{A}(C) = \sum_{\ell\in[d], j\in[D]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell}$$

and begin with the observation that, for any $A \in \mathbb{C}^{d\times d}$ we have

$$\mathrm{diag}(S^\ell A S^{-\ell}, m) = S^\ell \,\mathrm{diag}(A, m).$$

We then have

$$\begin{aligned}&\sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell} = 0\\ \iff &\mathrm{diag}\left(\sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell}, m\right) = 0 \quad \text{for all } m \in [\delta]_0\\ \iff &\sum_{j\in[D],\ell\in[d]} C_{\ell,j}\,\mathrm{diag}(S^\ell m_j m_j^* S^{-\ell}, m) = 0 \quad \text{for all } m \in [\delta]_0\\ \iff &\sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell\,\mathrm{diag}(m_j m_j^*, m) = 0 \quad \text{for all } m \in [\delta]_0\end{aligned}$$

At this point, we consider that

$$\begin{aligned}\mathrm{diag}(m_j m_j^*, m) &= \mathrm{diag}((\gamma\circ f_j)(\gamma\circ f_j)^*, m) = \mathrm{diag}(D_{f_j}\gamma\gamma^* D_{\overline{f_j}}, m)\\ &= \omega_K^{m(j-1)}\,\mathrm{diag}(\gamma\gamma^*, m).\end{aligned}$$

We now set $g_m := \mathrm{diag}(\gamma\gamma^*, m) = \gamma \circ S^{-m}\gamma$ and proceed with the previous chain of implications:

$$\begin{aligned}&\sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell\,\mathrm{diag}(m_j m_j^*, m) = 0 \quad \text{for all } m \in [\delta]_0\\ \iff &\sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell(\omega_K^{m(j-1)} g_m) = 0 \quad \text{for all } m \in [\delta]_0\\ \iff &\sum_{j\in[D],\ell\in[d]} C_{\ell,j}\omega_K^{m(j-1)} S^\ell g_m = 0 \quad \text{for all } m \in [\delta]_0\\ \iff &\mathrm{circ}(g_m) C\, v_{m+1}^D = 0 \quad \text{for all } m \in [\delta]_0\end{aligned}$$

We now recall that any circulant matrix $\mathrm{circ}(v)$ is diagonalized by the Discrete Fourier Matrix, such that, for $v \in \mathbb{C}^d$,

$$\mathrm{circ}(v) = F_d \,\mathrm{diag}(\sqrt{d} F_d v) F_d^* = \sqrt{d} \sum_{j=1}^{d} (F_d v)_j f_j^d (f_j^d)^*.$$

By writing $\lambda_k^m = \sqrt{d}(F g_m)_k$, we get a natural decoupling of the previous equations: for a fixed m, we have that $\mathrm{circ}(g_m) C f_{m+1} = 0$ if and only if

$$\sum_{k=1}^{d} \lambda_k^m f_k^d (f_k^d)^* C \, f_{m+1} = \sum_{k=1}^{d} (\lambda_k^m (f_k^d)^* C \, f_{m+1}) f_k^d = 0.$$

Since this last expression is a linear combination of an orthonormal basis, it occurs only when $\lambda_k^m (f_k^d)^* C \, f_{m+1} = 0$ for all $k \in [d]$. We collect these equations over $m \in [\delta]_0$, considering the definition of J_k and that $g_m \in \mathbb{R}^d$ implies $\lambda_k^m = 0 \iff \lambda_{2-k}^m = 0$ to restate this condition as $\begin{bmatrix} f_k^d & f_{2-k}^d \end{bmatrix}^* C v_{m+1}^D = 0$ for all $k \in [d], m \in J_k$. Since $\mathrm{span}\{f_k^d, f_{2-k}^d\} = \mathrm{span}\{\rho_k^d, \mu_k^d\}$, we further restate this as $\begin{bmatrix} \rho_k^d & \mu_k^d \end{bmatrix}^* C v_{m+1}^D = 0$ for all $k \in [d], m \in J_k$; setting $W_k = C^* \begin{bmatrix} \rho_k^d & \mu_k^d \end{bmatrix} \in \mathbb{R}^{D \times 2}$, we now get that $\mathcal{A}(C) = 0 \iff \mathrm{Col}(W_k) \subseteq \{v_{m+1}^D\}_{m \in J_k}^{\perp} \cap \mathbb{R}^D$ for all $k \in [d]$.

We now claim that $\mathcal{A}$ is invertible if and only if the subspaces $\{v_{m+1}^D\}_{m \in J_k}^{\perp} \cap \mathbb{R}^D$ are all trivial. Indeed, if we fix a k and have some non-zero $u \in \{v_{m+1}^D\}_{m \in J_k}^{\perp} \cap \mathbb{R}^D$, then we may set $C = \rho_k^d u^*$, such that

$$\mathrm{circ}(g_m) C v_{m+1}^D = (\mathrm{circ}(g_m) \rho_k^d)(u^* v_{m+1}^D).$$

For $m \in J_k, u^* v_{m+1}^D = 0$ by hypothesis on u, and for $m \notin J_k, \mathrm{circ}(g_m) \rho_k^d = 0$ by definition of J_k and lemma 2.

For the other direction, assume $\{v_{m+1}^D\}_{m \in J_k}^{\perp} \cap \mathbb{R}^D = 0$ for each $k \in [d]$. Then $\mathcal{A}(C) = 0 \iff \mathrm{Col}(W_k) = \{0\} \iff W_k = 0$ for all k. However, $\{\rho_k^d\}_{k \in [d]} \cup \{\mu_k^d\}_{k \in [d] \setminus \{1, \frac{d}{2}+1\}}$ is an orthogonal basis for $\mathbb{R}^d$, so

$$\begin{aligned} & W_k = 0 \quad \text{for all } k \in [d] \\ \iff \quad & C^* \rho_k^d = C^* \mu_k^d = 0 \quad \text{for all } k \in [d] \\ \iff \quad & C = 0 \end{aligned}$$

We complete the proof by considering that, for $u \in \mathbb{R}^D, \langle v_j^D, u \rangle = 0$ if and only if $\langle \rho_j^D, v \rangle = \langle \mu_j, v \rangle = 0$, so

$$\{v_{m+1}\}_{m \in J_k}^{\perp} \cap \mathbb{R}^D = \{\rho_{m+1}, \mu_{m+1}\}_{m \in J_k}^{\perp}$$

which has dimension $\max\{D - (2|J_k| - \mathbb{1}_{0 \in J_k}), 0\}$ by lemma 1. Therefore, $\mathcal{A}$ is invertible if and only if $2|J_k| - \mathbb{1}_{0 \in J_k} \leq D$ for all $k \in [d]$, as claimed. □

Remark. It turns out that this condition is generic, in the sense that it fails to hold only on a subset of $\mathbb{R}^d$ with Lebesgue measure zero. We consider that the set of $\gamma \in \mathbb{R}^d$ giving at least one zero in $F(\gamma \circ S^{-m} \gamma)$ is a finite union of zero sets of non-trivial quadratic polynomials (except when $2 \mid d, \delta \geq d/2$, and $m = d/2$, discussed below) and hence a set of

zero measure; therefore, $J_k = [\delta]_0$ for all γ outside a set of measure zero and B_γ is linearly independent under generic conditions.

To address the case of $m = d/2$, we first remark that this is the only possible exception: indeed, when $m \neq d/2$, we have that

$$F((e_1 + e_{m+1}) \circ S^m(e_1 + e_{m+1}))_k = f_k^* e_{m+1} = \omega^{m(k-1)},$$

so $\gamma \to F(\gamma \circ S^m \gamma)_k$ is a non-zero, homogeneous quadratic polynomial and therefore has a zero locus of measure zero.

However, when $d = 2m$, then $\gamma \circ S^m \gamma$ is periodic with period m and $F(\gamma \circ S^m \gamma)_{2i} = 0$ for $i \in [m]_0$. In particular, if $\delta \geq m$, then $D = d$ and $m \notin J_{2i}$ for all $i \in [m]_0$ for any γ. In particular, $|J_2| \leq \delta - 1$ and $2|J_2| - \mathbb{1}_{0 \in J_2} \leq 2\delta - 3$, so if $\delta \in \{d/2, d/2 + 1\}$, all choices of γ automatically fail to produce a spanning family.

This exception is quite pathological, though: since our intention is to have $\delta \ll d$, this will rarely be an impediment. Nonetheless, in the case that you *do* want to have $\operatorname{span} B_\gamma = \mathcal{H}^d$, then taking $\delta > d/2 + 1$ gives some space for the condition $2|J_k| - \mathbb{1}_{0 \in J_k}$, and we again have that generic γ will produce spanning families.