

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

Brian Preskitt

June 7, 2018

1 Notation

- Indices of matrices in $\mathbb{C}^{d \times d}$ and vectors in \mathbb{C}^d are always taken modulo d .
- For $k \in \mathbb{N}, n \in \mathbb{Z}, [k]_n = \{n, n+1, \dots, n+k-1\}$ 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 $k \in [d]$, $\text{circ}_k(x) \in \mathbb{C}^{d \times k}$ denotes the first k columns of the circulant matrix whose first column is x . In particular, $\text{circ}_k(x)e_i = S^{i-1}x$ for $i \in [k]$. When the subscript is omitted, $\text{circ}(x) = \text{circ}_d(x)$.
- $\omega_d := e^{\frac{2\pi i}{d}}$ 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 $A \in \mathbb{C}^{d \times d}, \text{diag}(A, m) \in \mathbb{C}^d$ denotes the m^{th} circulant off-diagonal of A . That is, $\text{diag}(A, m)_i = A_{i, i+m}$.
- Given $x \in \mathbb{C}^d, \text{diag}(x) \in \mathbb{C}^{d \times d}$ is the diagonal matrix whose diagonal entries are the entries of x . Namely, $\text{diag}(x)e_i = x_i e_i$. When the intention is clear from context, we may write $D_x := \text{diag}(x)$.
- \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} .

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

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

Similarly, $\mathcal{R}_{m \times n} : \bigcup_{k_1, k_2}^{\infty} \mathbb{C}^{k_1 \times k_2} \rightarrow \mathbb{C}^{m \times n}$ truncates or zero-pads matrices to size $m \times n$.

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

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

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

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*

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

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

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

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*

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

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

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

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 $M = \dim \text{span}\{w_{\ell_i}, w_{2-\ell_i}\}_{i=1}^k$ 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 $[w_1 \ \cdots \ w_{N_2}]$ will be a Vandermonde matrix of the form

$$V = \frac{1}{\sqrt{N_2}} [w_{\ell_1} \ \cdots \ w_{\ell_{N_1}}]$$

with determinant

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

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

When $N_1 \geq N_2$, $\{w_j\}_{j \in [N_2]}$ 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 $\ell_i = (2 - \ell_i \pmod{N_2}) = N_2/2 + 1$ is precluded since we have asserted $\ell_i \leq \frac{N_2+1}{2}$.

□

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

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

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

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

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

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

(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 $\Re(\omega_d^{(j-1)(k-1)} \lambda_k^d) \neq 0$, and similarly for $\Im(\omega_d^{(j-1)(k-1)} \lambda_k^d) \neq 0$. 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 $\text{circ}(v)\rho_k^d = \lambda_k^d \rho_k^d \neq 0$. 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

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

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 $\mathcal{A}^* : \mathbb{R}^{d \times D} \rightarrow \mathbb{C}^{d \times d}$ by

$$\mathcal{A}^*(C) = \sum_{\ell \in [d], j \in [D]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell} \quad (3)$$

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

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

We then have

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

At this point, we consider that

$$\text{diag}(m_j m_j^*, m) = \text{diag}((\gamma \circ v_j)(\gamma \circ v_j)^*, m) = \text{diag}(D_{v_j} \gamma \gamma^* D_{\overline{v_j}}, m) \quad (4)$$

$$= \omega_K^{m(j-1)} \text{diag}(\gamma \gamma^*, m). \quad (5)$$

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

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

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

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

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 $\text{circ}(g_m) C f_{m+1} = 0$ 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 $[f_k^d \ f_{2-k}^d]^* C v_{m+1}^D = 0$ for all $k \in [d], m \in J_k$. Since $\text{span}\{f_k^d, f_{2-k}^d\} = \text{span}\{\rho_k^d, \mu_k^d\}$, we further restate this as $[\rho_k^d \ \mu_k^d]^* C v_{m+1}^D = 0$ for all $k \in [d], m \in J_k$; setting $W_k = C^* [\rho_k^d \ \mu_k^d] \in \mathbb{R}^{D \times 2}$, we now get that $\mathcal{A}^*(C) = 0 \iff \text{Col}(W_k) \subseteq \{v_{m+1}^D\}_{m \in J_k}^\perp \cap \mathbb{R}^D$ 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

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

For $m \in J_k$, $u^* v_{m+1}^D = 0$ by hypothesis on u , and for $m \notin J_k$, $\text{circ}(g_m) \rho_k^d = 0$ 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 $\mathcal{A}^*(C) = 0 \iff \text{Col}(W_k) = \{0\} \iff W_k = 0$ 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

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

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

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

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. \square

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 $\gamma \rightarrow F(\gamma \circ S^m \gamma)_k$ 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 $\text{span } B_\gamma = \mathcal{H}^d$, 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.

3 Condition number

$$\begin{aligned} \mathcal{A} : \mathbb{C}^{d \times d} &\rightarrow \mathbb{R}^{[d] \times [D]} \\ \mathcal{A}(X)_{(\ell, j)} &= \langle S^\ell m_j m_j^* S^{-\ell}, X \rangle \end{aligned} \quad (6)$$

Now that we have characterized this collection of spanning families, we are interested in the condition number for solving the linear system $y = \mathcal{A}(T_\delta(xx^*)) + \eta$ to estimate $T_\delta(xx^*)$. We begin by introducing the main result of this section:

Proposition 2. *Accept the hypotheses of proposition 1 and define \mathcal{A} as in (6). If we additionally assume that $2\delta - 1 \leq d$ and $K = 2\delta - 1$, then the condition number of \mathcal{A} is*

$$\kappa(\mathcal{A}) = \frac{\max_{m \in [\delta]_0, j \in [d]} |F_d(\gamma \circ S^{-m} \gamma)_j|}{\min_{m \in [\delta]_0, j \in [d]} |F_d(\gamma \circ S^{-m} \gamma)_j|}. \quad (7)$$

Otherwise, we may bound the condition number by

$$\kappa(\mathcal{A}) \leq \frac{\max_{m \in [\delta]_0, j \in [d]} |F_d(\gamma \circ S^{-m} \gamma)_j|}{\min_{m \in [\delta]_0, j \in [d]} |F_d(\gamma \circ S^{-m} \gamma)_j|} \kappa(\bar{F}_K), \quad (8)$$

where $\bar{F}_K \in \mathbb{C}^{D \times D}$ is the $D \times D$ principal submatrix of F_K .

To accomplish this, we introduce the operators $P^{(d, N)} : \mathbb{C}^{dN} \rightarrow \mathbb{C}^{dN}$, each of which is a permutation defined by

$$(P^{(d, N)} v)_{(i-1)N+j} = v_{(j-1)d+i}.$$

We can view this is beginning with $v \in \mathbb{C}^{dN}$ written as N blocks of d entries, and interleaving them into d blocks each of N entries. Additionally, for $k, N_1, N_2 \in \mathbb{N}, v \in \mathbb{C}^{kN_1}$, and $H \in \mathbb{C}^{kN_1 \times N_2}$, we define circ^{N_1} by

$$\begin{aligned}\text{circ}^{N_1}(v) &= \begin{bmatrix} v & S_{kN_1}^{N_1} v & \cdots & S_{kN_1}^{(k-1)N_1} v \end{bmatrix} \\ \text{circ}^{N_1}(H) &= \begin{bmatrix} H & S_{kN_1}^{N_1} H & \cdots & S_{kN_1}^{(k-1)N_1} H \end{bmatrix}.\end{aligned}$$

We now proceed with the following lemmas.

Lemma 3. Suppose $v_i, v_{ij} \in \mathbb{C}^k, w_j \in \mathbb{C}^{kN_1}$ for $i \in [N_1], j \in [N_2]$ and

$$\begin{aligned}M_1 &= \begin{bmatrix} \text{circ}(v_1) \\ \vdots \\ \text{circ}(v_{N_1}) \end{bmatrix}, \quad M_2 = [\text{circ}^{N_1}(w_1) \quad \cdots \quad \text{circ}^{N_1}(w_{N_2})], \text{ and} \\ M_3 &= \begin{bmatrix} \text{circ}(v_{11}) & \cdots & \text{circ}(v_{1N_2}) \\ \vdots & \ddots & \vdots \\ \text{circ}(v_{N_11}) & \cdots & \text{circ}(v_{N_1N_2}) \end{bmatrix}.\end{aligned}$$

Then

$$P^{(k, N_1)} M_1 = \text{circ}^{N_1} \left(P^{(k, N_1)} \begin{bmatrix} v_1 \\ \vdots \\ v_{N_1} \end{bmatrix} \right) \quad (9)$$

$$M_2 P^{(k, N_2)*} = \text{circ}^{N_1} ([w_1 \quad \cdots \quad w_{N_2}]) \quad (10)$$

$$P^{(k, N_1)} M_3 P^{(k, N_2)*} = \text{circ}^{N_1} \left(P^{(k, N_1)} \begin{bmatrix} v_{11} & \cdots & v_{1N_2} \\ \vdots & \ddots & \vdots \\ v_{N_11} & \cdots & v_{N_1N_2} \end{bmatrix} \right). \quad (11)$$

Proof of lemma 3. We index the matrices to check the equalities. For (9), we have

$$\begin{aligned}(P^{(k, N_1)} M_1)_{(a-1)N_1+b, j} &= (M_1)_{(b-1)k+a, j} \\ &= \begin{bmatrix} S^{j-1} v_1 \\ \vdots \\ S^{j-1} v_{N_1} \end{bmatrix}_{(b-1)k+a} \\ &= (S^{j-1} v_b)_a = (v_b)_{a+j-1}\end{aligned}$$

and

$$\begin{aligned}\text{circ}^{N_1} \left(P^{(k, N_1)} \begin{bmatrix} v_1 \\ \vdots \\ v_{N_1} \end{bmatrix} \right)_{(a-1)N_1+b, j} &= \left(P^{(k, N_1)} \begin{bmatrix} v_1 \\ \vdots \\ v_{N_1} \end{bmatrix} \right)_{(a-1)N_1+b+(j-1)N_1} \\ &= (v_b)_{a+j-1}\end{aligned}$$

For (10), we have

$$(P^{(k,N_2)} M_2^*)_{(a-1)N_2+b,j} = (M_2)_{j,(b-1)k+a} = (w_b)_{j+(a-1)N_1}$$

and

$$(\text{circ}^{N_1}([w_1 \ \cdots \ w_{N_2}]))_{j,(a-1)N_2+b} = (S^{N_1(a-1)} w_b)_j = (w_b)_{j+N_1(a-1)}$$

(11) follows immediately by combining (9) and (10). \square

Lemma 4. Suppose $V \in \mathbb{C}^{kN \times m}$, then $\text{circ}^N(V)$ is block diagonalizable by

$$\text{circ}^N(V) = (F_k \otimes I_N) (\text{diag}(M_1, \dots, M_k)) (F_k \otimes I_m)^*,$$

where

$$\sqrt{k} (F_k \otimes I_N)^* V = \begin{bmatrix} M_1 \\ \vdots \\ M_k \end{bmatrix}, \quad \text{or} \quad M_j = \sqrt{k} (f_j^k \otimes I_N)^* V$$

Proof of lemma 4. We set V_i to be the $k \times m$ blocks of V such that $V^* = [V_1^* \ \cdots \ V_k^*]$ and begin by observing that, for $u \in \mathbb{C}^k$ and $W \in \mathbb{C}^{m \times p}$, the ℓ^{th} $k \times p$ block of $\text{circ}^N(V)(u \otimes W)$ is given by

$$(\text{circ}^N(V)(u \otimes W))_\ell = \sum_{i=1}^k u_i (S^{N(i-1)} V)_\ell W = \sum_{i=1}^k u_i V_{\ell-i+1} W.$$

Taking $u = f_j^k$ and $W = I_m$, this gives

$$\begin{aligned} (\text{circ}^N(V)(f_j^k \otimes I_m))_\ell &= \frac{1}{\sqrt{k}} \sum_{i=1}^k \omega_k^{(j-1)(i-1)} V_{\ell-i+1} I_m \\ &= \frac{1}{\sqrt{k}} \omega_k^{(j-1)(\ell-1)} \sum_{i=1}^k \omega_k^{-(j-1)(i-1)} V_i \\ &= (f_j^k)_\ell \left(\sqrt{k} (f_j^k \otimes I_N)^* V \right) = (f_j^k)_\ell M_j. \end{aligned}$$

This relation is equivalent to having

$$\text{circ}^N(V)(f_j^k \otimes I_m) = (f_j^k \otimes M_j) = (f_j^k \otimes I_N) M_j,$$

which is the statement of the lemma. \square

Lemma 4 immediately gives the following corollary.

Corollary 1. With notation as in lemma 4, the condition number of $\text{circ}^N(V)$ is

$$\frac{\max_{i \in [k]} \sigma_{\max}(M_i)}{\min_{i \in [k]} \sigma_{\min}(M_i)}.$$

We now consider the rows of the measurement operator \mathcal{A} defined in (6). For now, we assume $2\delta - 1 \leq d$, and we vectorize $X \in T_\delta(\mathbb{C}^{d \times d})$ by its diagonals, taking $\chi_m = \text{diag}(X, m)$, $m \in [2\delta - 1]_{1-\delta}$, and for now we set $g_m^j = \text{diag}(m_j m_j^*, m)$, for now omitting the assumption that $m_j = \gamma \circ v_j$ as in proposition 1. Therefore, each measurement looks like

$$\begin{aligned} \mathcal{A}(X)_{(\ell, j)} &= \langle S^\ell m_j m_j^* S^{-\ell}, X \rangle \\ &= \sum_{m=1-\delta}^{\delta-1} \langle S^\ell g_m^j, \chi_m \rangle, \end{aligned}$$

so if we define the matrix $A \in \mathbb{C}^{dD \times (2\delta-1)d}$ such that

$$\left(A \begin{bmatrix} \chi_{1-\delta} \\ \vdots \\ \chi_{\delta-1} \end{bmatrix} \right)_{(j-1)d+\ell} = \mathcal{A}(X)_{(\ell, j)}, \quad (12)$$

the $(j-1)d + \ell^{\text{th}}$ row of A is given by

$$\begin{bmatrix} S^\ell g_{1-\delta}^j \\ \vdots \\ S^\ell g_{\delta-1}^j \end{bmatrix}^*,$$

such that A is the block matrix given by

$$A = \begin{bmatrix} \text{circ}(g_{1-\delta}^1)^* & \cdots & \text{circ}(g_{\delta-1}^1)^* \\ \vdots & \ddots & \vdots \\ \text{circ}(g_{1-\delta}^D)^* & \cdots & \text{circ}(g_{\delta-1}^D)^* \end{bmatrix} = \begin{bmatrix} \text{circ}(Rg_{1-\delta}^1) & \cdots & \text{circ}(Rg_{\delta-1}^1) \\ \vdots & \ddots & \vdots \\ \text{circ}(Rg_{1-\delta}^D) & \cdots & \text{circ}(Rg_{\delta-1}^D) \end{bmatrix},$$

which may be transformed, by Lemma 3, to

$$P^{(d, D)} A P^{(d, 2\delta-1)*} = \text{circ}^D \left(P^{(d, D)} \begin{bmatrix} Rg_{1-\delta}^1 & \cdots & Rg_{\delta-1}^1 \\ \vdots & \ddots & \vdots \\ Rg_{1-\delta}^D & \cdots & Rg_{\delta-1}^D \end{bmatrix} \right) =: \text{circ}^D(H). \quad (13)$$

Quoting corollary 1, this establishes the next proposition.

Proposition 3. *Setting $M_j = \sqrt{d} (f_j^d \otimes I_D)^* H$, the condition number of A is*

$$\kappa(A) = \frac{\max_{i \in [d]} \sigma_{\max}(M_i)}{\min_{i \in [d]} \sigma_{\min}(M_i)}.$$

We are now able to prove proposition 2.

Proof. For the moment, we assert that $D = 2\delta - 1 \leq d$ and set $\bar{F}_K \in \mathbb{C}^{2\delta-1 \times 2\delta-1}$, $(\bar{F}_K)_{ij} = \frac{1}{\sqrt{K}} \omega_K^{(i-1)(j-\delta)}$ to be the principal submatrix of $\sqrt{K} \text{diag}(f_{1-\delta}^K) F_K$. In this case, $g_m^j =$

$\text{diag}(m_j m_j^*, m) = \omega_K^{m(j-1)} g_m$, as in (5). Therefore, we label the $2\delta - 1 \times 2\delta - 1$ blocks of H by $H^* = [H_1^* \ \cdots \ H_d^*]$, so that

$$(H_\ell)_{ij} = (Rg_{j-\delta}^i)_\ell = \omega_K^{(i-1)(j-\delta)} (Rg_{j-\delta})_\ell$$

and $M_\ell = \sum_{k=1}^d \omega_d^{(\ell-1)(k-1)} H_k$, giving

$$\begin{aligned} (M_\ell)_{ij} &= \sum_{k=1}^d \omega_d^{(\ell-1)(k-1)} (H_k)_{ij} = \omega_K^{(i-1)(j-\delta)} \sum_{k=1}^d \omega_d^{(\ell-1)(k-1)} (Rg_{j-\delta})_k \\ &= \omega_K^{(i-1)(j-\delta)} (F_d^* g_{j-\delta})_\ell. \end{aligned}$$

In other words, $M_\ell = \sqrt{K} \text{diag}(f_\ell^{d*} g_{1-\delta}, \dots, f_\ell^{d*} g_{\delta-1}) \bar{F}_K$. If $K = 2\delta - 1$, then \bar{F}_K is unitary, and the singular values of M_ℓ are $\{\sqrt{K} f_\ell^{d*} g_j\}_{j=1-\delta}^{\delta-1}$. Recognizing that $S^j g_j = g_{-j}$, then proposition 3 takes us to (7).

If $D = 2\delta - 1 < K$, then the argument remains unchanged, except that the singular values of M_ℓ , instead of being known explicitly, are bounded above and below by $\max_{|j| < \delta} |f_\ell^{d*} g_j| \sigma_{\max}(\bar{F}_K)$ and $\min_{|j| < \delta} |f_\ell^{d*} g_j| \sigma_{\min}(\bar{F}_K)$ respectively, which gives the more general result of (8).

If $2\delta - 1 > d$, then instead of using diagonals $1 - \delta, \dots, \delta - 1$, we use diagonals $0, 1, \dots, d - 1$. This change propagates from (12) to (13), so that

$$(H_\ell)_{ij} = \omega_K^{(i-1)(j-1)} (Rg_{j-1})_\ell \quad \text{and} \quad (M_\ell)_{ij} = \omega_K^{(i-1)(j-1)} (F_d^* g_{j-1})_\ell,$$

giving $M_\ell = \sqrt{K} \text{diag}(f_\ell^{d*} g_0, \dots, f_\ell^{d*} g_{d-1}) \mathcal{R}_{d \times d}(F_K)$, which immediately gives us (8). We remark that indexing only over the diagonals $m \in [\delta]_0$ in (8) suffices, again because $S^j g_j = g_{-j}$, so having $2\delta - 1 > d$ makes $1 - \delta, \dots, -1$ redundant.

□