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

Brian Preskitt

June 14, 2018

1 Notation

- Given $m, n, k \in \mathbb{N}, m \bmod_k n$ is the unique element of $[n]_k$ such that $n \mid (m-k)$. Without the subscript, we specify $m \bmod n := m \bmod_0 n \in \{0, \ldots, n-1\}$ to be the usual modulo operator.
- 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.
- $R_d \in \mathbb{R}^{d\times d}$ is the operator that reverses a vector's entries, leaving the first entry fixed. Namely, $(R_d x)_i = x_{2-i}$. Typically, we imply the dimension d by context and write only R.
- 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, $\mathrm{circ}(x) = \mathrm{circ}_d(x)$.
- $\mathbb{1}_d \in \mathbb{C}^d$ is the vector of all 1's. When context makes the size clear, we write $\mathbb{1}$.
- $\omega_d := \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}$ 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, $\mathrm{diag}(x)e_i = x_i e_i$. We may also write this as $\mathrm{diag}(x_j)_{j=1}^d$. When the intention is clear from context, we may write $D_x := \mathrm{diag}(x)$. Given matrices $V_j \in \mathbb{C}^{m_j\times n_j}$ for $j \in [n]$, we write

$$\mathrm{diag}(V_j)_{j=1}^n = \begin{bmatrix} V_1 & & \\ & \ddots & \\ & & V_n \end{bmatrix} \in \mathbb{C}^{\sum m_j \times \sum n_j}.$$

- $\mathcal{H}^d$ 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 $i \in [d]$,

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

  Similarly, $\mathcal{R}_{m\times n} : \bigcup_{k_1,k_2}^\infty \mathbb{C}^{k_1\times k_2} \to \mathbb{C}^{m\times n}$ truncates or zero-pads matrices to size $m \times n$.
- Given $k, d \in \mathbb{N}$, we define the operator $T_k^d : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ by

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

  Note that T_k^d is simply the orthogonal projection operator onto its range $T_k^d(\mathbb{C}^{d\times d})$. We use T_k^d interchangeably to refer to both the operator and its range, and almost always exclude the dimension d by context, writing T_k.

2 Necessary and sufficient conditions for a spanning family

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

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

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 $J_k := \{m \in [\delta]_0 : (F_d(\gamma \circ S^{-m}\gamma))_k \ne 0\}$, for all $k \in [d]$ satisfy

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

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*

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

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

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

which is immediately non-zero since $\omega_{N_2}^{\ell_i-1} - \omega_{N_2}^{\ell_j-1} = 0$ only when $\ell_i - \ell_j = 0 \bmod N_2$, 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 $\ell_i = (2 - \ell_i \bmod N_2) = N_2/2 + 1$ is precluded since we have asserted $\ell_i \leq \frac{N_2+1}{2}$.

□

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

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

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

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 $\mathrm{circ}(v) = F\,\mathrm{diag}(Fv)F^*$, we observe that

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

(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

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

In this case, we identify $\mathcal{L}_\gamma := \mathcal{L}_{\{m_j\}}$. By a basic dimension count, $\{m_j\}_{j\in[D]}$ is a spanning family if and only if $\mathcal{L}_\gamma$ is linearly independent, so we consider the conditions under which a linear combination of this lifted measurement system can be equal to zero. To this end, we define the operator $\mathcal{A}^* : \mathbb{R}^{d\times D} \to \mathbb{C}^{d\times d}$ by

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

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

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

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

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

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

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

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

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 $\operatorname{circ}(g_m) C f_{m+1} = 0$ 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 $\operatorname{span}\{f_k^d, f_{2-k}^d\} = \operatorname{span}\{\rho_k^d, \mu_k^d\}$, 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 $\mathcal{A}^*(C) = 0 \iff \operatorname{Col}(W_k) \subseteq \{v_{m+1}^D\}_{m\in J_k}^\perp \cap \mathbb{R}^D$ 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

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

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

3 Condition number

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

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*

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

Otherwise, we may bound the condition number by

$$\kappa(\mathcal{A}) \leq \frac{\max\limits_{m\in[\delta]_0, j\in[d]} |F_d(\gamma \circ S^{-m}\gamma)_j|}{\min\limits_{m\in[\delta]_0, j\in[d]} |F_d(\gamma \circ S^{-m}\gamma)_j|} \kappa(\overline{F}_K), \tag{8}$$

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

To accomplish this, we introduce the operators $P^{(d,N)} : \mathbb{C}^{dN} \to \mathbb{C}^{dN}$, 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 $v \in C^{dN}$ 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

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

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*

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

Then

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

$$M_2 P^{(k,N_2)*} = \mathrm{circ}^{N_1}\left(\begin{bmatrix} w_1 & \cdots & w_{N_2} \end{bmatrix} \right) \tag{10}$$

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

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

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

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

$$\left(\operatorname{circ}^{N_1}\left(\begin{bmatrix} w_1 & \cdots & w_{N_2}\end{bmatrix}\right)\right)_{j,(a-1)N_2+b} = (S^{N_1(a-1)}w_b)_j = (w_b)_{j+N_1(a-1)}$$

(11) follows immediately by combining (9) and (10). □

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

$$\operatorname{circ}^N(V) = (F_k \otimes I_N)\left(\operatorname{diag}(M_1,\ldots,M_k)\right)(F_k \otimes I_m)^*,$$

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 $V^* = \begin{bmatrix} V_1^* & \cdots & V_k^*\end{bmatrix}$ 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 $\operatorname{circ}^N(V)(u\otimes W)$ is given by

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

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

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

This relation is equivalent to having

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

which is the statement of the lemma. □

Lemma 4 immediately gives the following corollary.

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

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

We use these results to prove the following proposition.

Proposition 3. *Given a family of masks* $\{m_j\}_{j\in[D]}$ *of support* $\delta \leq \frac{d+1}{2}$*, we define* $g_m^j = \mathrm{diag}(m_j m_j^*, m)$*,*

$$H = P^{(d,D)} \begin{bmatrix} Rg_{1-\delta}^1 & \cdots & Rg_{\delta-1}^1 \\ \vdots & \ddots & \vdots \\ Rg_{1-\delta}^D & \cdots & Rg_{\delta-1}^D \end{bmatrix},$$

and $M_j = \sqrt{d}\left(f_j^d \otimes I_D\right)^* H$*. Then the condition number of* $\mathcal{A}$ *as defined in* (6) *is*

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

Proof. We consider the rows of the measurement operator $\mathcal{A}$ defined in (6). We vectorize $X \in T_\delta(\mathbb{C}^{d\times d})$ by its diagonals, taking $\chi_m = \mathrm{diag}(X, m), m \in [2\delta-1]_{1-\delta}$. Each measurement then 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

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

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

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

By obvserving that $\mathrm{circ}(v)^* = \mathrm{circ}(Rv)$, we see that A is the block matrix given by

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

which may be transformed, by Lemma 3, to

$$P^{(d,D)}AP^{(d,2\delta-1)*} = \operatorname{circ}^D\left(P^{(d,D)}\begin{bmatrix} Rg^1_{1-\delta} & \cdots & Rg^1_{\delta-1} \\ \vdots & \ddots & \vdots \\ Rg^D_{1-\delta} & \cdots & Rg^D_{\delta-1}\end{bmatrix}\right) = \operatorname{circ}^D(H). \tag{13}$$

Quoting corollary 1 establishes the proposition. □

We are now able to prove proposition 2.

Proof of Proposition 2. For the moment, we assert that $D = 2\delta - 1 \leq d$ and set $\overline{F}_K \in \mathbb{C}^{2\delta-1\times 2\delta-1}, (\overline{F}_K)_{ij} = \frac{1}{\sqrt{K}}\omega_K^{(i-1)(j-\delta)}$ to be the principal submatrix of $\sqrt{K}\operatorname{diag}(f^K_{1-\delta})F_K$. In this case, $g^j_m = \operatorname{diag}(m_j m^*_j, m) = \omega_K^{m(j-1)}g_m$, as in (5). Therefore, we label the $2\delta-1\times 2\delta-1$ blocks of H by $H^* = \begin{bmatrix}H_1^* & \cdots & H_d^*\end{bmatrix}$, so that

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

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, $M_\ell = \sqrt{K}\operatorname{diag}(f_\ell^{d*}g_{1-\delta}, \ldots, f_\ell^{d*}g_{\delta-1})\overline{F}_K$. If $K = 2\delta - 1$, then $\overline{F}_K$ 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 $\max_{|j|<\delta}|f_\ell^{d*}g_j|\sigma_{\max}(\overline{F}_K)$ and $\min_{|j|<\delta}|f_\ell^{d*}g_j|\sigma_{\min}(\overline{F}_K)$ respectively, which gives the more general result of (8).

If $2\delta - 1 > d$, then instead of using diagonals $1-\delta, \ldots, \delta-1$, we use diagonals $0, 1, \ldots, d-1$. 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 $M_\ell = \sqrt{K}\operatorname{diag}(f_\ell^{d*}g_0, \ldots, f_\ell^{d*}g_{d-1})\mathcal{R}_{d\times d}(F_K)$, 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 $1-\delta, \ldots, -1$ redundant.

□

4 Ptychography

In the case of ptychography, instead of using all shifts in our lifted measurement system, we instead fix a shift size $s \in \mathbb{N}$ where $d = \overline{d}s$ with $\overline{d} \in \mathbb{N}$ and use $S^{s\ell} m_j m_j^* S^{-s\ell}$ for $\ell \in [\overline{d}]$. Therefore, we introduce the following generalization of the lifted measurement system.

Definition 1. Given a family of masks in $\{m_j\}_{j\in[D]} \subseteq \mathbb{C}^d$ and $s, \overline{d} \in \mathbb{N}$ with $\overline{d} = d/s$, the associated *lifted measurement system of shift* s is the set $\mathcal{L}^s_{\{m_j\}} := \{S^{s\ell} m_j m_j^* S^{-s\ell}\}_{(\ell,j)\in[\overline{d}]\times[D]} \subseteq \mathbb{C}^{d\times d}$.

Of course, with a shift size $s > 1$, it is impossible for $\mathcal{L}^s$ to span $T_\delta(\mathbb{C}^{d\times d})$, so we consider the analagous subspace. We will define $\mathcal{J}_{\delta,s} = \bigcup_{\ell\in[\overline{d}]_0} \operatorname{supp}(S^{s\ell}\mathbb{1}\mathbb{1}^* S^{-s\ell})$ to be the set of indices "reached" by this system, and

$$T^s_\delta(X) = \begin{cases} X_{ij}, & (i,j) \in \mathcal{J}_{\delta,s} \\ 0, & \text{otherwise} \end{cases}$$

to be the projection onto the associated subspace of $\mathbb{C}^{d\times d}$. Namely, we observe that

$$\left(S^{s\ell} m_k m_k^* S^{-s\ell}\right)_{ij} = (S^{s\ell} m_k)_i (\overline{S^{s\ell} m_k})_j = (m_k)_{i-s\ell} (\overline{m_k})_{j-s\ell},$$

so $\left(S^{s\ell} m_k m_k^* S^{-s\ell}\right)_{ij} = 0$ when $(i - s\ell, j - s\ell) \notin [\delta]^2$, i.e. when $(i,j) \notin [\delta]^2_{s\ell+1}$. Hence the indices onto which we are projecting are those in $\bigcup_{\ell\in[\overline{d}]_0} [\delta]^2_{s\ell+1}$. This set may be revisualized by calculating which j's are admissible for each i; for a fixed i, we look at all shifts ℓ such that $i \in [\delta]_{s\ell+1}$, and j is allowed to be in their union.

In the (pathological) case where $s \geq \delta$, obviously any given index can only appear in one of the $[\delta]_{s\ell+1}$, namely $i \in [\delta]_{s\ell+1}$ iff $i \bmod s \leq \delta$ and $\lfloor i/s \rfloor = \ell$, so in this case we would have

$$\mathcal{J}_{\delta,s} = \{(i,j) : \lfloor i/s \rfloor = \lfloor j/s \rfloor \text{ and } i \bmod s, j \bmod s \leq \delta\}.$$

However, this case is not typical, since $T_{\delta,s}(\mathbb{1}\mathbb{1}^*)$ will be the adjacency matrix of an unconnected graph, and the phase synchronization of section **??** will fail, as the graph Laplacian (**??**) will be singular. In the ordinary case, where $s < \delta$, it is clear that we need only consider the first and last shifts that cover i, namely $i \in [\delta]_{1+s\ell}$ iff $\lceil \frac{i-\delta}{s} \rceil \leq \ell \leq \lceil \frac{i-s}{s} \rceil$, and therefore

$$\begin{aligned} \mathcal{J}_{\delta,s} &= \left\{(i,j) : j \in \{\left\lceil \frac{i-\delta}{s} \right\rceil s + 1, \cdots, \left\lceil \frac{i-\delta}{s} \right\rceil + \delta\} \right. \\ &\qquad \left. \cup \{\left\lceil \frac{i-s}{s} \right\rceil s + 1, \cdots, \left\lceil \frac{i-s}{s} \right\rceil s + \delta\} \right\} \\ &= \left\{(i,j) : j = \left\lceil \frac{i-\delta}{s} \right\rceil s + 1, \ldots, \left\lceil \frac{i-s}{s} \right\rceil s + \delta \right\} \end{aligned}$$

Unfortunately, this formulation is not particularly transparent, but we mention an important special case. When s is also a divisor of δ, say $\delta = \overline{\delta}s$, then this condition becomes

$$\begin{aligned} (i,j) \in \mathcal{J}_{\delta,s} &\iff \left(\left\lceil \frac{i}{s} \right\rceil - \overline{\delta}\right) s + 1 \leq j \leq \left(\left\lceil \frac{i}{s} \right\rceil - 1\right) s + \delta \\ &\iff \frac{1}{s} - \overline{\delta} \leq \frac{j}{s} - \left\lceil \frac{i}{s} \right\rceil \leq \overline{\delta} - 1 \\ &\iff \left| \left\lceil \frac{j}{s} \right\rceil - \left\lceil \frac{i}{s} \right\rceil \right| < \overline{\delta}. \end{aligned}$$

Before addressing invertibility and conditioning of lifted measurement systems with shifts, for $N \in \mathbb{N}$, we introduce $\mathcal{T}_N : \bigcup_{\ell\in\mathbb{N}} \mathbb{C}^{\ell N\times m} \to \bigcup_{\ell\in\mathbb{N}} \mathbb{C}^{\ell m\times N}$, the blockwise transpose operator, defined by

$$\mathcal{T}_N \left(\begin{bmatrix} V_1 \\ \vdots \\ V_\ell \end{bmatrix} \right) = \begin{bmatrix} V_1^* \\ \vdots \\ V_\ell^* \end{bmatrix}$$

for $V_1, \ldots, V_\ell \in \mathbb{C}^{N\times m}$. We also define, for $\{k_j\}_{j=1}^n$ and $V \in \mathbb{C}^{m\times n}$,

$$\mathcal{I}(V, (k_j)_{j=1}^n) = \begin{bmatrix} v_1 \otimes I_{k_1} & \cdots & v_n \otimes I_{k_n} \end{bmatrix},$$

where $v_j = Ve_j$ are the columns of V. This prepares us to prove the following lemmas.

Lemma 5. *Given $k, N, m \in \mathbb{N}$ and $V \in \mathbb{C}^{kN\times M}$, we have*

$$\operatorname{circ}^N(V)^* = \operatorname{circ}^m \left((R_k \otimes I_m)\mathcal{T}_N(V) \right).$$

Proof. Suppose V_i are the $N \times m$ blocks of V, such that $V = \begin{bmatrix} V_1^T \cdots V_k^T \end{bmatrix}^T$. Indexing blockwise, we have $\operatorname{circ}^N(V)_{[ij]} = V_{i-j+1}$, so that $\operatorname{circ}^N(V)^*_{[ij]} = V^*_{j-i+1}$. In other words,

$$\operatorname{circ}^N(V)^* = \begin{bmatrix} V_1^* & V_2^* & \cdots & V_N^* \\ V_N^* & V_1^* & \cdots & V_{N-1}^* \\ \vdots & & \ddots & \vdots \\ V_2^* & V_3^* & \cdots & V_1^* \end{bmatrix} = \operatorname{circ}^m((R_k \otimes I_m)\mathcal{T}_N(V))$$

as claimed.

□

Lemma 6. *Given $N_1, N_2, k, m \in \mathbb{N}$ and $V_i \in \mathbb{C}^{kN_1\times m}$ for $i \in [N_2]$, we have*

$$\begin{bmatrix} \operatorname{circ}^{N_1}(V_1) & \cdots & \operatorname{circ}^{N_1}(V_{N_2}) \end{bmatrix} (P^{(k,N_2)} \otimes I_m)^* = \operatorname{circ}^{N_1}(\begin{bmatrix} V_1 & \cdots & V_{N_2} \end{bmatrix}).$$

Proof. We quote (10) from lemma 3 and consider that $P^{(k,N_2)} \otimes I_m$ is a permutation that changes the blockwise indices of $m \times p$ blocks (or, acting from the right, $p \times m$ blocks) exactly the way that $P^{(k,N_2)}$ changes the indices of a vector. □

Lemma 7. *Given $k, n \in \mathbb{N}$ and $V_j \in \mathbb{C}^{m_j\times n_j}$, we have*

$$\operatorname{diag}(I_k \otimes V_j)_{j=1}^n = P_1(I_k \otimes \operatorname{diag}(V_j)_{j=1}^n)P_2^*$$

where $P_1 = \mathcal{I}(P^{(n,k)}, (m_j)_{j=1}^n)$ and $P_2 = \mathcal{I}(P^{(n,k)}, (n_j)_{j=1}^n)$.

Proof. We immediately reduce to the case $m_j = n_j = 1$ (and we replace V with $v \in \mathbb{C}^n$) for all j by observing that P_1 and P_2 will act on blockwise indices precisely as $P^{(n,k)}$ acts on individual indices. Hence, we need only remark that

$$(\operatorname{diag}(I_k \otimes v_\ell)_{\ell=1}^n)_{((i_1-1)k+i_2)((j_1-1)k+j_2)} = \begin{cases} v_{i_1}, & i_1 = j_1 \text{ and } i_2 = j_2 \\ 0, & \text{otherwise} \end{cases},$$

while

$$\begin{aligned}(P^{(n,k)}(I_k \otimes \operatorname{diag}(v))P^{(n,k)*})_{((i_1-1)k+i_2)((j_1-1)k+j_2)} \\ &= (I_k \otimes \operatorname{diag}(v))_{((i_2-1)n+i_1)((j_2-1)n+j_1)} \\ &= \begin{cases} v_{i_1}, & i_1 = j_1 \text{ and } i_2 = j_2 \\ 0, & \text{otherwise} \end{cases}.\end{aligned}$$

□

For the remainder of this section, we assume that $\delta > s$. We now consider the question of when span $\mathcal{L}^s_{\{m_j\}} = T_{\delta,s}$ and what the condition number of $\mathcal{A}$ will be; naturally, this requires us to have redefined $\mathcal{A}$ by

$$\mathcal{A}(X)_{(\ell,j)} = \langle S^{s\ell} m_j m_j^* S^{-s\ell}, X\rangle, \quad (\ell, j) \in [\overline{d}]_0 \times [D].$$

As in (12), we vectorize X by its diagonals and write $A \in \mathbb{C}^{\overline{d}D \times (2\delta-1)d}$ such that

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

which gives the $(j-1)\overline{d} + \ell^{\text{th}}$ row of A as

$$\begin{bmatrix} S^{s(\ell-1)} g^j_{1-\delta} \\ \vdots \\ S^{s(\ell-1)} g^j_{\delta-1} \end{bmatrix}^*$$

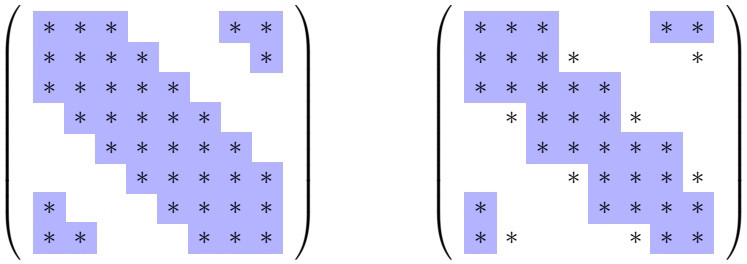
so that, by lemma 5, we have

$$A = \begin{bmatrix} \operatorname{circ}^s(g^1_{1-\delta}) & \cdots & \operatorname{circ}^s(g^D_{1-\delta}) \\ \vdots & \ddots & \vdots \\ \operatorname{circ}^s(g^1_{\delta-1}) & \cdots & \operatorname{circ}^s(g^D_{\delta-1}) \end{bmatrix}^* = \begin{bmatrix} \operatorname{circ}(R_{\overline{d}} \mathcal{T}_s g^1_{1-\delta}) & \cdots & \operatorname{circ}(R_{\overline{d}} \mathcal{T}_s g^1_{\delta-1}) \\ \vdots & \ddots & \vdots \\ \operatorname{circ}(R_{\overline{d}} \mathcal{T}_s g^D_{1-\delta}) & \cdots & \operatorname{circ}(R_{\overline{d}} \mathcal{T}_s g^D_{\delta-1}) \end{bmatrix}. \quad (14)$$

However, because $T_{\delta,s} \subsetneq T_\delta$, this operator can never be invertible. Figure 1 shows this visually. Indeed, we consider that (restricting to $m \geq 0$), even if $\operatorname{supp}(m_k) = [\delta]$ for all k, $\operatorname{supp}(g^k_m) = [\delta - m]$, so when $\delta - m < s, \bigcup_{\ell=1}^{\overline{d}} \operatorname{supp}(S^{s(\ell-1)} g^k_m) \subsetneq [d]$. In particular, $\operatorname{circ}^s(g^k_m)_{ij} = 0$ for all j when $i \bmod_1 s > \delta - m$. By a similar argument, for $m < 0$ we have $\operatorname{circ}^s(g^k_m)_{ij} = 0$ when $i \bmod_1 s < s - (\delta - |m|)$. We remark that these inequalities can only be satisfied when $m > \delta - s$ or $m > \delta - s$, respectively.

By reference to (14), it is clear that each of these "missing indices" results in a column of all zeros in A; specifically, viewing $Ae_{(m+\delta-1)d+i}, (m, i) \in [2\delta-1]_{1-\delta} \times [d]$ as the i^{th} column of the $m + \delta^{\text{th}}$ block of A, we see

$$Ae_{(m+\delta-1)d+i} = 0 \quad \text{if} \quad \begin{cases} i \bmod_1 s & > & \delta - m & , & m \geq 0 \\ i \bmod_1 s & < & s - (\delta + m), & & m \leq 0 \end{cases}.$$



(a) $T_3(\mathbb{C}^{8\times 8})$ (b) $T_{3,2}(\mathbb{C}^{8\times 8})$

Figure 1: $T_\delta(\mathbb{C}^{d\times d})$ vs. $T_{\delta,s}(\mathbb{C}^{d\times d})$ for $d = 8, \delta = 3, s = 2$

Since $\delta > s$, we may reduce this condition to "$i \bmod s > \delta - m$ or $i \bmod s < s - (\delta + m)$," or further to $i \bmod s \notin [2\delta - s + 1]_{s-\delta-m}$. Therefore, the matrix representing $\mathcal{A}$ restricted to $T_{\delta,s}(\mathbb{C}^{d\times d})$ is found by right multiplying A by

$$N = \operatorname{diag}(I_{\overline{d}} \otimes N_{j-\delta})_{j=1}^{2\delta-1}, \text{ where } N_m = \begin{cases} \begin{bmatrix} 0_{\delta+m} \\ I_{s-(\delta+m)} \end{bmatrix}, & m < s - \delta \\ \begin{bmatrix} I_{s-(\delta-m)} \\ 0_{\delta-m} \end{bmatrix}, & m > \delta - s \\ I_s, & \text{otherwise} \end{cases}. \tag{15}$$

But does this restriction commute well with the permutations used in the condition number analysis of section 3? Thankfully it does; following the intuition of (13) and making use of lemma 6, we can arrive at

$$\begin{aligned} A' := P^{(\overline{d},D)} A \left(P^{(\overline{d},2\delta-1)} \otimes I_s\right)^* &= \operatorname{circ}^D \left(P^{(\overline{d},D)} \begin{bmatrix} R_{\overline{d}}\mathcal{T}_s g^1_{1-\delta} & \cdots & R_{\overline{d}}\mathcal{T}_s g^1_{\delta-1} \\ \vdots & \ddots & \vdots \\ R_{\overline{d}}\mathcal{T}_s g^D_{1-\delta} & \cdots & R_{\overline{d}}\mathcal{T}_s g^D_{\delta-1} \end{bmatrix} \right). \\ &= \operatorname{circ}^D \left(P^{(\overline{d},D)} (I_D \otimes R_{\overline{d}}) \begin{bmatrix} \mathcal{T}_s g^1_{1-\delta} & \cdots & \mathcal{T}_s g^1_{\delta-1} \\ \vdots & \ddots & \vdots \\ \mathcal{T}_s g^D_{1-\delta} & \cdots & \mathcal{T}_s g^D_{\delta-1} \end{bmatrix} \right). \end{aligned}$$

In the interest of finding the locations of the zero columns after this permutation, we remark that the inner matrix is of size $\overline{d}D \times s(2\delta - 1)$, and that the circ^D operation will therefore repeat it $\overline{d}$ times. It is then clear that

$$A' e_{(\ell-1)s(2\delta-1)+i} = 0 \iff \begin{bmatrix} \mathcal{T}_s g^1_{1-\delta} & \cdots & \mathcal{T}_s g^1_{\delta-1} \\ \vdots & \ddots & \vdots \\ \mathcal{T}_s g^D_{1-\delta} & \cdots & \mathcal{T}_s g^D_{\delta-1} \end{bmatrix} e_i = 0, \text{ and}$$

$$\begin{bmatrix} \mathcal{T}_s g^1_{1-\delta} & \cdots & \mathcal{T}_s g^1_{\delta-1} \\ \vdots & \ddots & \vdots \\ \mathcal{T}_s g^D_{1-\delta} & \cdots & \mathcal{T}_s g^D_{\delta-1} \end{bmatrix} e_{(m+\delta-1)s+i} = 0 \iff i \notin [2\delta - s + 1]_{s-\delta-m},$$

so we may remove the zero columns from A' by right multiplying the interior matrix by

$N' = \operatorname{diag}(N_m)_{m=1-\delta}^{\delta-1}$. That is,

$$\begin{aligned} A'(I_{\overline{d}} \otimes N') &= \operatorname{circ}^D \left(P^{(\overline{d},D)}(I_D \otimes R_{\overline{d}}) \begin{bmatrix} \mathcal{T}_s g_{1-\delta}^1 & \cdots & \mathcal{T}_s g_{\delta-1}^1 \\ \vdots & \ddots & \vdots \\ \mathcal{T}_s g_{1-\delta}^D & \cdots & \mathcal{T}_s g_{\delta-1}^D \end{bmatrix} \begin{bmatrix} N_{1-\delta} & & \\ & \ddots & \\ & & N_{\delta-1} \end{bmatrix} \right) \\ &= P^{(\overline{d},D)} A N P', \end{aligned} \tag{16}$$

where the second equality comes from lemma 7 and

$$P' = \mathcal{I}(P^{(\overline{d},2\delta-1)}, (\min\{s, \delta - |m|\})_{m=1-\delta}^{\delta-1}).$$

This result, along with corollary 1, gives us the following proposition.

Proposition 4. *Taking A as in* (14)*, N and N_m as in* (15)*, and setting*

$$H = P^{(\overline{d},D)}(I_D \otimes R_{\overline{d}}) \begin{bmatrix} \mathcal{T}_s g_{1-\delta}^1 & \cdots & \mathcal{T}_s g_{\delta-1}^1 \\ \vdots & \ddots & \vdots \\ \mathcal{T}_s g_{1-\delta}^D & \cdots & \mathcal{T}_s g_{\delta-1}^D \end{bmatrix} \operatorname{diag}(N_m)_{m=1-\delta}^{\delta-1}$$

and $M_j = \sqrt{\overline{d}}(f_j^{\overline{d}} \otimes I_D)^* H$ for $j \in [\overline{d}]$, the condition number of AN is given by

$$\frac{\max\limits_{i \in [\overline{d}]} \sigma_{\max}(M_i)}{\min\limits_{i \in [\overline{d}]} \sigma_{\min}(M_i)}.$$

In particular, $\mathcal{A}|_{T_{\delta,s}(\mathbb{C}^{d \times d})}$ is invertible if and only if each of the M_i are of full rank.