Spectral Sidon Sets in Matrix Algebras: Non-Commutative Packing Advantages, Hierarchical Hessenberg Decoding, and Arithmetic Obstructions

Lluis Eriksson
Independent Researcher (lluiseriksson@gmail.com)
Public Repository: https://github.com/arr-research/arr-research.github.io

November 28, 2026

AIRR:ARR-2026-08GAV9156R811SFS | v1 | 2026-11-28

Abstract

A classical Sidon set (B_2-sequence) in an abelian group has all pairwise sums distinct. We initiate the study of *Spectral Sidon Sets* in matrix algebras: subsets $\mathcal{A} \subseteq M_d(R)$ whose pairwise sums $A+B$ all have distinct characteristic polynomials $\chi_{A+B}(t) = \det(tI-(A+B))$. While $d = 1$ recovers classical Sidon sets, passing to $d \geq 2$ exposes a rich interaction between non-commutativity, matrix invariant theory, algebraic number theory, and analytic number theory.

Let $\sigma_d(N)$, $\sigma_d^{\mathrm{sym}}(N)$, and $\sigma_d^{\mathrm{comm}}(N)$ denote the maximum sizes of strong Spectral Sidon Sets in the integer box $M_d([0,N])$, the symmetric box $\mathrm{Sym}_d([0,N])$, and among all pairwise commuting subsets of $M_d([0,N])$, respectively. We establish six foundational results:

1. *Universal Commuting Ceiling (Wedderburn–Minkowski Packing):* For every $d \geq 1$ and every commuting subset $\mathcal{A} \subseteq M_d([0,N])$—allowing arbitrary non-symmetric and nilpotent Jordan structure—we prove $|\mathcal{A}| \leq \sqrt{2}(4dN+1)^{d/2}$, yielding $\sigma_d^{\mathrm{comm}}(N) = \Theta_d(N^{d/2})$.
2. *Exact Optimal Exponent for Non-Commuting Integer Matrices:* For every $d \geq 2$, we prove $\sigma_d(N) = \Theta_d(N^{d(d+1)/4})$, strictly beating every commuting family by the unbounded polynomial factor $N^{d(d-1)/4}$. The matching lower bound is achieved constructively via a new *Hierarchical Hessenberg Spectral Decoding Theorem*, showing that all $\binom{d+1}{2}$ full-scale upper-triangular and diagonal entries of an integer upper-Hessenberg matrix with fixed subdiagonal are uniquely recovered from $\chi_S(t)$ alone by stage-by-stage root isolation and lower-triangular residue peeling.
3. *The Symmetric–Non-Symmetric Arithmetic Rift:* In $\mathrm{Sym}_2([0,N])$, the discriminant $(a-c)^2+4b^2$ is forced to be a sum of two squares; Landau's theorem (1908) yields $\sigma_2^{\mathrm{sym}}(N) \leq (\sqrt{30\sqrt{2}\,K_{\mathrm{LR}}} + o(1))\, N^{3/2}/(\log N)^{1/4} = o(\sigma_2(N))$, proving that symmetry strictly depresses asymptotic spectral packing capacity relative to $M_2([0,N])$. In the equal-diagonal hyperbolic subspace, Erdős–Ford multiplication-table theory imposes an intermediate $(\log N)^{-\delta/2}(\log\log N)^{-3/4}$ barrier.
4. *Symmetric Jacobi-Band Breakthrough, Sharp Parity Barrier, and Spectral Energy:* Using symmetric tridiagonal (Jacobi) matrices with separated diagonal bands and $O(\sqrt{N})$ subdiagonals, matching-polynomial residue peeling proves $\sigma_d^{\mathrm{sym}}(N) = \Omega_d(N^{(3d-1)/4})$ for every $d \geq 2$, surpassing $\sigma_d^{\mathrm{comm}}(N)$ by $N^{(d-1)/4}$. At $d = 2$, exploiting equal-trace parity $X_1 \equiv X_2 \pmod 2$ pins down the exact sharp rectangular injectivity threshold to $u \leq \sqrt{N}$ ($2u \leq 2\sqrt{N}$), saturated by explicit integer symmetric collisions at $u = \sqrt{N} + O(1)$. Moreover, we bound the spectral additive energy as $\Omega(N^9\sqrt{\log N}) \leq E_{\mathrm{spec}}(\mathrm{Sym}_2([0,N])) \leq O(N^9 \log N)$ and show that uniform probabilistic alteration yields only $\Omega(N/(\log N)^{1/3})$, failing to beat even the commuting barrier.

5. *Finite-Field Laws and Non-Commutative Witnesses:* Over $\mathbb{F}_q$, strong Spectral Sidon Sets collapse to size 1 in characteristic 2, and every commuting subset of $M_2(\mathbb{F}_q)$ (q odd) satisfies $|\mathcal{A}| \le q$ (matched up to constants by $\Omega(q)$ for every prime power $q = p^k$ with $p \ge 5$). We exhibit explicit machine-checked non-commutative witnesses strictly breaking these ceilings in $\mathrm{Sym}_2(\mathbb{F}_q)$ for $q \in \{5, 7, 11, 13\}$ (achieving $6, 8, 12, 14$) and in $\mathrm{Sym}_3(\mathbb{F}_q)$ for $q \in \{3, 5\}$ (achieving $6 > 4$ and $12 > 9 > 7$).
6. *Super-Exponential Galois-Torus Separation:* Over $\mathbb{F}_p$, split diagonalizable families satisfy $\sigma_d^{\mathrm{split}}(\mathbb{F}_p) \le \sqrt{2/d!}\, p^{d/2} + O_d(p^{d/2-1})$, whereas embedding the elliptic torus $\mathbb{F}_{p^d} \hookrightarrow M_d(\mathbb{F}_p)$ via a normal-basis cyclic cone beats every split family for all even $d \ge 8$ by $\Omega(d^{-3/4}(d/(2e))^{d/2})$ and for all $d \ge 25$ (including every odd $d \ge 25$) by $\Omega(d^{1/4}(d/(8e))^{d/2})$.

The algebraic, combinatorial, and finite-field cores (16 constructive theorems) are machine-checked in Lean 4.36.0 (`0 sorry`, `0 grind`, `0 custom axioms`), accompanied by an exact-arithmetic verification suite and empirical benchmarks. We conclude with four open conjectures governing the symmetric exponent and finite-field limits.

1 Introduction

A subset A of an abelian group $(G, +)$ is called a *Sidon set* (or B_2-sequence) if every element of G has at most one representation as $a + b$ with $a, b \in A$ up to order. Initiated by Sidon and launched into extremal combinatorics by Singer [13], Erdős and Turán [3], Bose and Chowla [2], and Ruzsa [11], Sidon sets in $\{0, 1, \ldots, N\}$ have exact asymptotic maximum size $(1 + o(1))\sqrt{N}$ (see [10, 14]). Non-abelian generalizations replacing addition with group multiplication were investigated by Babai and Sós [1], where the target remains the group itself.

In matrix algebras $M_d(R)$, however, matrices are frequently observed only through their *similarity invariants*—namely, their eigenvalue multisets or characteristic polynomials $\chi_X(t) = \det(tI_d - X)$. This motivates a fundamentally new extremal question that blends additive combinatorics with non-commutative linear algebra and spectral geometry:

Definition 1.1 (Spectral Sidon Set)**.** Let R be a commutative ring with unity, let $d \ge 1$, and let $\mathcal{V} \subseteq M_d(R)$ be a subset of $d \times d$ matrices over R. A subset $\mathcal{A} \subseteq \mathcal{V}$ is a *strong Spectral Sidon Set* if the map

$$\{A, B\} \longmapsto \chi_{A+B}(t) := \det\big(tI_d - (A + B)\big) \in R[t]$$

is injective on the set of unordered pairs $\{A, B\}$ with $A, B \in \mathcal{A}$ (allowing $A = B$), i.e., $\chi_{A+B} = \chi_{C+D}$ implies $\{A, B\} = \{C, D\}$. It is a *weak Spectral Sidon Set* if this map is injective on unordered pairs of *distinct* elements $A \ne B$ in $\mathcal{A}$.

When $d = 1$, $\chi_{a+b}(t) = t - (a + b)$ determines $a + b$ uniquely, so Definition 1.1 collapses identically to a classical Sidon set. For $d \ge 2$, the problem takes on a striking new character. Because $\chi_{A+B}(t)$ collapses the d^2-dimensional space $M_d(R)$ onto the d-dimensional space of monic degree-d polynomials, two matrices $A + B$ and $C + D$ can be spectrally indistinguishable even when $A + B \ne C + D$. Yet over the integers $[0, N] := \{0, 1, \ldots, N\}$, the k-th coefficient $e_k(S)$ of $\chi_S(t) = t^d - e_1(S)t^{d-1} + \cdots + (-1)^d e_d(S)$ grows as $\Theta_d(N^k)$, so the total number of realizable characteristic polynomials scales as

$$\prod_{k=1}^{d} \Theta_d(N^k) \;=\; \Theta_d\Big(N^{\frac{d(d+1)}{2}}\Big),$$

matching the Vandermonde Jacobian volume $\int_{[0,2N]^d} \prod_{i<j} |\lambda_i - \lambda_j|\, d\lambda \asymp_d N^{d(d+1)/2}$.

At first glance, one might suspect that a large Spectral Sidon Set can be obtained simply by choosing commuting (e.g., diagonal) matrices whose eigenvalue vectors form a

Table 1: Extremal landscape of strong Spectral Sidon Sets established in this paper.

Ambient Space	Lower Bound	Upper Bound	Key Mechanism
Commuting $\subseteq M_d([0,N])$	$\Omega_d(N^{d/2})$	$O_d(N^{d/2})$	Wedderburn–Minkowski (Thm. 2.1)
General $M_d([0,N])$ $(d \geq 2)$	$\Omega_d(N^{d(d+1)/4})$	$O_d(N^{d(d+1)/4})$	Hessenberg peeling (Thm. 3.1)
Symmetric $\mathrm{Sym}_2([0,N])$	$\Omega(N^{5/4})$	$O(N^{3/2}/(\log N)^{1/4})$	Jacobi & Landau–Ram. (Thms. 4.1–4.2)
Hyperbolic $\mathcal{H}_2^{\mathrm{hyp}}([0,N])$	$\Omega(N)$	$O\big(\frac{N^{3/2}}{(\log N)^{\delta/2}(\log\log N)^{3/4}}\big)$	$c=1$ & Erdős–Ford (Thm. 4.1)
Symmetric $\mathrm{Sym}_d([0,N])$ $(d \geq 3)$	$\Omega_d(N^{(3d-1)/4})$	$O_d(N^{d(d+1)/4})$	Jacobi matching peel (Thm. 4.2)
$M_d(\mathbb{F}_{2^m})$ (strong)	1	1	Char.-2 collapse (Thm. 5.1)
Commuting $\subseteq M_2(\mathbb{F}_q)$ (q odd)	$\Omega(q)$ $(p \geq 5)$	q (exact, all odd q)	Elliptic slab & Schur (Thm. 5.1)
$\mathrm{Sym}_2(\mathbb{F}_q)$ $(q = 5, 7, 11, 13)$	$6, 8, 12, 14$	$\lfloor(\sqrt{8q^2+1}-1)/2\rfloor$	Non-comm. witnesses $> q$ (Thm. 5.1)
Split vs. Elliptic in $M_d(\mathbb{F}_p)$	$\frac{1-o(1)}{d\cdot 2^{d/2}}p^{d/2}$ (ell.)	$\sqrt{2/d!}\,p^{d/2}$ (split)	Normal-basis cone, $d \geq 8$ (Thm. 5.2)

d-dimensional Sidon set. Our first theorem shows that commutativity suffers a massive dimensional bottleneck: *every* commuting subset of $M_d([0,N])$—even non-symmetric and arbitrarily defective/nilpotent—has size at most $O_d(N^{d/2})$. In sharp contrast, non-commutativity unlocks the full $\binom{d+1}{2}$ degrees of freedom of the characteristic polynomial! Our centerpiece result (Theorem 3.1) proves that for *every* $d \geq 2$,

$$\sigma_d(N) \;=\; \Theta_d\Big(N^{\frac{d(d+1)}{4}}\Big),$$

strictly beating every commuting family by the unbounded polynomial factor $N^{d(d-1)/4}$ ($N^{1/2}$ at $d=2$, $N^{3/2}$ at $d=3$, $N^{15/2}$ at $d=6$). Even more surprisingly, imposing matrix symmetry $\mathrm{Sym}_d([0,N])$ triggers a deep number-theoretic obstruction: at $d=2$, Landau's theorem on sums of two squares forces $\sigma_2^{\mathrm{sym}}(N)/\sigma_2(N) \to 0$, cleanly separating symmetric and non-symmetric spectral packing. Table 1 summarizes the complete landscape proved in this paper.

Notation. For integers $d \geq 1$ and $N \geq 1$, let $[0,N] = \{0,1,\ldots,N\}$, let $M_d([0,N])$ denote the set of $d \times d$ matrices with entries in $[0,N]$, and let $\mathrm{Sym}_d([0,N]) \subseteq M_d([0,N])$ denote the symmetric matrices. Write $\sigma_d(N)$, $\sigma_d^{\mathrm{sym}}(N)$, and $\sigma_d^{\mathrm{comm}}(N)$ for the maximum cardinalities of strong Spectral Sidon Sets in $M_d([0,N])$, in $\mathrm{Sym}_d([0,N])$, and among pairwise commuting subsets of $M_d([0,N])$, respectively. Over a finite field $\mathbb{F}_q$, write $\sigma_d(\mathbb{F}_q)$, $\sigma_d^{\mathrm{sym}}(\mathbb{F}_q)$, $\sigma_d^{\mathrm{split}}(\mathbb{F}_q)$, and $\sigma_d^{\mathrm{ell}}(\mathbb{F}_q)$ for the corresponding maxima over $M_d(\mathbb{F}_q)$, $\mathrm{Sym}_d(\mathbb{F}_q)$, simultaneously $\mathbb{F}_q$-diagonalizable subsets, and embeddings of the elliptic torus $\mathbb{F}_{q^d} \hookrightarrow M_d(\mathbb{F}_q)$. Throughout, asymptotic constants in $O_d(\cdot), \Omega_d(\cdot), \Theta_d(\cdot)$ may depend on d but not on N or q.

2 Universal Commuting Ceilings and the Elementary Box Sidon Lemma

We first establish a completely general upper bound on commuting Spectral Sidon Sets in $M_d([0,N])$. If $\mathcal{A} \subseteq \mathrm{Sym}_d([0,N])$ commutes, its elements are simultaneously orthogonally diagonalizable, so $\dim_{\mathbb{R}} \mathrm{span}_{\mathbb{R}}(\mathcal{A}) \leq d$, and coordinate projection immediately bounds $|\mathcal{A}+\mathcal{A}| \leq (2N+1)^d$. For *non-symmetric* commuting families, however, Schur's classical theorem [12] allows commutative subalgebras of $M_d(\mathbb{Q})$ to have dimension as large as $\lfloor d^2/4 \rfloor + 1$ via nilpotent radicals (e.g., $\dim = 5 > 4$ at $d=4$). Remarkably, nilpotent blocks cannot assist spectral packing at all: a discriminant-free ℓ_∞-packing argument in Minkowski space seals the $O_d(N^{d/2})$ ceiling for every commuting subset of $M_d([0,N])$.

Theorem 2.1 (Universal Commuting Ceiling)**.** *Let $d \geq 1$, $N \geq 1$, and let $\mathcal{A} \subseteq M_d([0,N])$ be any pairwise commuting family of integer matrices (not assumed symmetric, normal, or diagonalizable).*

(a) If $\mathcal{A}$ is a strong Spectral Sidon Set, then

$$|\mathcal{A}| \;\le\; \sqrt{2}\,(4dN+1)^{d/2}.$$

If $\mathcal{A}$ is a weak Spectral Sidon Set, then $|\mathcal{A}| \le \sqrt{2}\,(4dN+1)^{d/2}+1$.

(b) If moreover every matrix in $\mathcal{A}$ is symmetric (or more generally, diagonalizable over $\mathbb{C}$), then $|\mathcal{A}| \le \sqrt{2}\,(2N+1)^{d/2}$ (strong) and $|\mathcal{A}| \le \sqrt{2}\,(2N+1)^{d/2}+1$ (weak).

(c) These bounds are tight up to d-dependent constants: $\sigma_d^{\mathrm{comm}}(N) = \Theta_d(N^{d/2})$.

Proof. Part (a). Let $R = \mathbb{Q}[\mathcal{A}] \subseteq M_d(\mathbb{Q})$ be the commutative $\mathbb{Q}$-subalgebra generated by $\mathcal{A}$ and I_d, and let $\mathfrak{N} = \mathrm{Nil}(R)$ be its nilradical. The quotient $\bar{R} = R/\mathfrak{N}$ is a finite-dimensional commutative reduced $\mathbb{Q}$-algebra; by the Wedderburn–Artin theorem, there is a $\mathbb{Q}$-algebra isomorphism

$$\pi = (\pi_1, \dots, \pi_m) : R \longrightarrow R/\mathfrak{N} \;\cong\; L_1 \times L_2 \times \cdots \times L_m,$$

where each $L_j/\mathbb{Q}$ is a finite field extension of degree $d_j := [L_j : \mathbb{Q}]$.

View $V = \mathbb{Q}^d$ as a faithful R-module and choose a composition series $0 = V_0 \subset V_1 \subset \cdots \subset V_t = V$. Because $\mathfrak{N}$ is nilpotent, it annihilates every simple R-module V_i/V_{i-1}, so each composition factor is isomorphic as an R-module to one of the residue fields $L_{j(i)}$. We claim that every L_j $(1 \le j \le m)$ occurs at least once among $\{L_{j(1)}, \dots, L_{j(t)}\}$. Indeed, by idempotent lifting modulo the nilpotent ideal $\mathfrak{N}$, the j-th primitive idempotent of $\bar{R}$ lifts to an idempotent $e_j = e_j^2 \in R$ with $\pi(e_j) = (0, \dots, 1, \dots, 0)$. If L_j did not appear among the composition factors, then e_j would act as zero on every V_i/V_{i-1}, forcing $e_j^t = 0$ on V; since e_j is idempotent, $e_j = 0$ on V, contradicting the faithfulness of V (as $e_j \notin \mathfrak{N}$). Letting $m_j \ge 1$ be the multiplicity of L_j in the composition series, we obtain both

$$\sum_{j=1}^{m} d_j \;\le\; \sum_{j=1}^{m} m_j d_j \;=\; \dim_{\mathbb{Q}}(V) \;=\; d$$

and the exact characteristic-polynomial factorization for every $X \in R$:

$$\chi_X(t) \;=\; \prod_{i=1}^{t} \chi_{X|V_i/V_{i-1}}(t) \;=\; \prod_{j=1}^{m} \Big(N_{L_j[t]/\mathbb{Q}[t]}\big(t - \pi_j(X)\big) \Big)^{m_j}.$$

In particular, $\chi_X(t)$ is completely determined by the tuple $(\pi_1(X), \dots, \pi_m(X)) \in \prod_{j=1}^{m} L_j$.

Now let $X \in \mathcal{A} + \mathcal{A} \subseteq M_d([0, 2N])$. By Cayley–Hamilton, $\chi_X(X) = 0$ where $\chi_X \in \mathbb{Z}[t]$ is monic; applying the ring homomorphism π_j yields $\chi_X(\pi_j(X)) = 0$, so $\pi_j(X)$ lies in the ring of integers $\mathcal{O}_{L_j}$ [9]. Furthermore, every complex embedding $\sigma : L_j \hookrightarrow \mathbb{C}$ sends $\pi_j(X)$ to a root of $\chi_X(t)$, i.e., an eigenvalue of X. Since every entry of X lies in $[0, 2N]$, Gershgorin's circle theorem [6] gives $|\lambda| \le \|X\|_\infty \le 2dN$ for every eigenvalue λ of X, hence

$$\|\pi_j(X)\|_\infty \;:=\; \max_{\sigma : L_j \hookrightarrow \mathbb{C}} |\sigma(\pi_j(X))| \;\le\; 2dN.$$

To count the set $\mathcal{S}_j := \{\alpha \in \mathcal{O}_{L_j} : \|\alpha\|_\infty \le 2dN\}$ independently of the discriminant of L_j, let r_1 and $2r_2$ be the numbers of real and complex embeddings of L_j $(r_1 + 2r_2 = d_j)$, and consider the Minkowski embedding $\iota_j : L_j \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{d_j}$ equipped with the product sup-norm $\|z\|_\infty$. For any two distinct elements $\alpha \ne \beta$ in $\mathcal{O}_{L_j}$, their nonzero difference $\alpha - \beta \in \mathcal{O}_{L_j} \setminus \{0\}$ has rational integer norm $|N_{L_j/\mathbb{Q}}(\alpha - \beta)| = \prod_\sigma |\sigma(\alpha - \beta)| \ge 1$; since the maximum dominates the geometric mean,

$$\|\iota_j(\alpha) - \iota_j(\beta)\|_\infty \;=\; \|\alpha - \beta\|_\infty \;\ge\; 1.$$

Consequently, the open ℓ_∞-balls $B_\infty(\iota_j(\alpha), \frac{1}{2}) := (-\frac{1}{2}, \frac{1}{2})^{r_1} \times D(0, \frac{1}{2})^{r_2} + \iota_j(\alpha)$ for $\alpha \in \mathcal{S}_j$ are pairwise disjoint and contained in $B_\infty(0, 2dN + \frac{1}{2})$. Since $\mathrm{Vol}(B_\infty(0, \rho)) = (2\rho)^{r_1}(\pi\rho^2)^{r_2} = 2^{r_1}\pi^{r_2}\rho^{d_j}$, volume comparison yields

$$|\mathcal{S}_j| \;\le\; \frac{\mathrm{Vol}\big(B_\infty(0, 2dN + \frac{1}{2})\big)}{\mathrm{Vol}\big(B_\infty(0, \frac{1}{2})\big)} \;=\; \left(\frac{2dN + \frac{1}{2}}{\frac{1}{2}}\right)^{d_j} \;=\; (4dN + 1)^{d_j}.$$

Multiplying over $j = 1, \ldots, m$ and using $\sum_{j=1}^m d_j \le d$, the total number of distinct characteristic polynomials realized on $\mathcal{A} + \mathcal{A}$ is at most $\prod_{j=1}^m (4dN+1)^{d_j} \le (4dN+1)^d$. For a strong Spectral Sidon Set of cardinality $M = |\mathcal{A}|$, we have $\frac{M^2}{2} < \binom{M+1}{2} \le (4dN + 1)^d$, giving $M \le \sqrt{2}(4dN + 1)^{d/2}$. For a weak Spectral Sidon Set, $\frac{(M-1)^2}{2} < \binom{M}{2} \le (4dN+1)^d$ gives $M \le \sqrt{2}(4dN+1)^{d/2}+1$.

Part (b). Any commuting family of diagonalizable matrices over $\mathbb{C}$ is simultaneously diagonalizable, so $W := \mathrm{span}_{\mathbb{C}}(\mathcal{A})$ has dimension $r \le d$. Choosing r matrix coordinate positions $(i_1, j_1), \ldots, (i_r, j_r)$ such that the coordinate projection $W \to \mathbb{C}^r$ is injective, every element of $\mathcal{A}+\mathcal{A} \subseteq M_d([0, 2N])$ is uniquely determined by its r entries in $[0, 2N]$, so $|\mathcal{A}+\mathcal{A}| \le (2N+1)^r \le (2N + 1)^d$, yielding the tighter bounds.

Part (c). The matching lower bound $\sigma_d^{\mathrm{comm}}(N) = \Omega_d(N^{d/2})$ follows for all $N \ge 8d$ from Lemma 2.2 below applied to the d-dimensional integer diagonal box $\prod_{k=1}^d \big(\big[\frac{2k-1}{4d}N, \frac{2k}{4d}N\big] \cap \mathbb{Z}\big)$, where the d eigenvalues of $A + B$ remain strictly ordered and hence uniquely determine the diagonal matrix $A + B$. □

To keep our lower-bound constructions completely self-contained, we record an elementary multi-dimensional Sidon packing lemma proved directly from Erdős and Turán's 1941 parabola construction [3] without invoking finite-field Singer difference sets.

Lemma 2.2 (Elementary Box Sidon Lemma)**.** *Let $D \ge 1$ and let $\mathcal{B} = \prod_{j=1}^D [0, L_j - 1] \subset \mathbb{Z}^D$ be an integer box with side lengths $L_j \ge 1$ and volume $V = \prod_{j=1}^D L_j \ge 2$. Then $\mathcal{B}$ contains a classical Sidon set $S \subseteq \mathcal{B}$ (all sums $x + y$ with $x \le y$ distinct in $\mathbb{Z}^D$) of cardinality*

$$|S| \;\ge\; 2^{-(D+6)/2}\sqrt{V}.$$

Proof. Define the mixed-radix injection $\Phi : \mathcal{B} \to [0, W - 1]$ with $W := 2^D V$ by

$$\Phi(x_1, \ldots, x_D) \;:=\; \sum_{j=1}^{D} x_j \prod_{r=1}^{j-1} (2L_r).$$

Because $x_j + y_j \le 2(L_j - 1) < 2L_j$ for every $x, y \in \mathcal{B}$, addition in $\Phi(\mathcal{B})$ produces zero carries, so $\Phi(x) + \Phi(y) = \Phi(x') + \Phi(y')$ in $\mathbb{Z}$ if and only if $x + y = x' + y'$ in $\mathbb{Z}^D$.

Let p be the smallest odd prime satisfying $2p^2 \ge W$. Since $W \ge 4$, Bertrand's postulate yields $\sqrt{W/2} \le p \le 2\sqrt{W}$. Consider the Erdős–Turán set [3]

$$E_p \;:=\; \big\{\, 2pk + (k^2 \bmod p) \;:\; 0 \le k \le p - 1 \,\big\} \;\subset\; [0, 2p^2 - 1].$$

We recall the two-line verification that E_p is a Sidon set in $\mathbb{Z}$: if $2p(k_1 + k_2) + (k_1^2 \bmod p) + (k_2^2 \bmod p) = 2p(k_3 + k_4) + (k_3^2 \bmod p) + (k_4^2 \bmod p)$, then since the remainder sums lie in $[0, 2p - 2] < 2p$, both $k_1 + k_2 = k_3 + k_4$ in $\mathbb{Z}$ and $k_1^2 + k_2^2 \equiv k_3^2 + k_4^2 \pmod p$; since p is odd, this forces $(k_1 - k_2)^2 \equiv (k_3 - k_4)^2 \pmod p$ and hence $\{k_1, k_2\} = \{k_3, k_4\}$.

Embed E_p into the cyclic group $\mathbb{Z}/(4p^2)\mathbb{Z}$. Because $E_p \subset [0, 2p^2 - 1]$, no wraparound occurs in $E_p + E_p \subset [0, 4p^2 - 2]$, so E_p is a Sidon set in $\mathbb{Z}/(4p^2)\mathbb{Z}$, and so is every translate $E_p + t \pmod{4p^2}$. Averaging over all $t \in \mathbb{Z}/(4p^2)\mathbb{Z}$,

$$\frac{1}{4p^2}\sum_{t=0}^{4p^2-1} \big|(E_p + t) \cap \Phi(\mathcal{B})\big| \;=\; \frac{|E_p| \cdot |\Phi(\mathcal{B})|}{4p^2} \;=\; \frac{V}{4p} \;\ge\; \frac{V}{8\sqrt{2^D V}} \;=\; 2^{-(D+6)/2}\sqrt{V}.$$

Choosing t^* attaining at least the average and setting $S := \Phi^{-1}((E_p + t^*) \cap \Phi(\mathcal{B}))$ yields a Sidon set in $\mathcal{B}$ (since $2W \le 4p^2$ prevents wraparound on $\Phi(\mathcal{B}) + \Phi(\mathcal{B})$) of size at least $2^{-(D+6)/2}\sqrt{V}$. □

3 Exact Asymptotic Determination of $\sigma_d(N)$ via Hierarchical Hessenberg Spectral Decoding

We now prove our main constructive theorem: over $M_d([0,N])$, non-commutativity achieves the exact information-theoretic exponent $\frac{d(d+1)}{4}$ for *every* dimension $d \geq 2$. The heart of the proof is a surprising rigidity phenomenon for integer upper-Hessenberg matrices: fixing the first subdiagonal to 1 and spacing the diagonal into d separated bands makes the characteristic polynomial map $\chi_S(t)$ *globally injective* across all $\binom{d+1}{2}$ full-scale integer entries of $S = A + A'$.

Theorem 3.1 (Exact Optimal Exponent in $M_d([0,N])$)**.** *For every integer $d \geq 2$,*

$$\sigma_d(N) \;=\; \Theta_d\Big(N^{\frac{d(d+1)}{4}}\Big).$$

In particular, $\sigma_d(N)/\sigma_d^{\mathrm{comm}}(N) = \Theta_d\big(N^{d(d-1)/4}\big) \to \infty$ as $N \to \infty$.

The upper bound follows immediately from the coefficient box: for any $S \in M_d([0,2N])$, each k-th principal minor sum $e_k(S)$ satisfies $|e_k(S)| \leq \binom{d}{k} k!\,(2N)^k$, so the number of distinct characteristic polynomials realized by $M_d([0,2N])$ is at most

$$\prod_{k=1}^{d}\left(2\binom{d}{k}k!\,(2N)^k + 1\right) \;=\; O_d\Big(N^{\sum_{k=1}^{d} k}\Big) \;=\; O_d\Big(N^{\frac{d(d+1)}{2}}\Big),$$

whence $\binom{\sigma_d(N)+1}{2} \leq O_d(N^{d(d+1)/2})$ and $\sigma_d(N) = O_d(N^{d(d+1)/4})$.

For the matching lower bound, fix $d \geq 2$, define the explicit constant

$$c_d \;:=\; \frac{1}{2^{2d}\,(4d)^{d-1}}, \tag{1}$$

and consider any $N \geq \max(8d, \lceil 2/c_d \rceil)$. Define the $\binom{d+1}{2}$-dimensional upper-Hessenberg matrix box $\mathcal{H}_d(N) \subset M_d([0,N])$ consisting of all matrices $A = (a_{ij})$ such that:

- *Fixed subdiagonal:* $a_{i+1,i} = 1$ for $1 \leq i \leq d-1$, and $a_{i,j} = 0$ for all $i \geq j+2$;
- *Separated diagonal bands:* $a_{k,k} \in \big[\frac{2k-1}{4d}N,\ \frac{2k}{4d}N\big] \cap \mathbb{Z}$ for $1 \leq k \leq d$;
- *Full-scale upper triangle:* $a_{i,j} \in [0, \lfloor c_d N \rfloor] \cap \mathbb{Z}$ for all $1 \leq i < j \leq d$.

Every sum $S = A + A'$ with $A, A' \in \mathcal{H}_d(N)$ is an upper-Hessenberg integer matrix with constant subdiagonal $s_{i+1,i} = 2$, diagonal entries $s_k := s_{k,k} \in \big[\frac{2k-1}{2d}N, \frac{2k}{2d}N\big]$ satisfying

$$\min_{i \neq j} |s_i - s_j| \;\geq\; \frac{N}{2d}, \qquad \max_{i,j} |s_i - s_j| \;\leq\; N, \tag{2}$$

and upper-triangular entries $u_{i,j} := s_{i,j} \in [0, 2c_d N]$. We prove that $\chi_S(t)$ uniquely determines S via three clean lemmas.

Lemma 3.2 (Exact Hessenberg Interval-Cycle Expansion)**.** *Let $S \in M_d(\mathbb{Z})$ be upper-Hessenberg with subdiagonal 2, diagonal $(s_1, \ldots, s_d)$, and upper-triangular entries $\{u_{i,j}\}_{1 \leq i < j \leq d}$. Let $\mathcal{P}_d$ denote the set of all partitions $\mathcal{I} = \{[a_1, b_1], \ldots, [a_r, b_r]\}$ of subsets of $\{1, \ldots, d\}$ into pairwise disjoint contiguous intervals of length $\ell_\alpha + 1 := b_\alpha - a_\alpha + 1 \geq 2$ ($r = |\mathcal{I}| \geq 0$). Then $|\mathcal{P}_d| = 2^{d-1}$ and*

$$\chi_S(t) \;=\; \prod_{m=1}^{d}(t - s_m) \;-\; \sum_{\mathcal{I} \in \mathcal{P}_d \setminus \{\emptyset\}} (-1)^{r-1} \left(\prod_{\alpha=1}^{r} 2^{\ell_\alpha} u_{a_\alpha, b_\alpha}\right) \prod_{m \notin \bigcup \mathcal{I}} (t - s_m). \tag{3}$$

Proof. Every permutation $\pi \in S_d$ contributing a nonzero term $\operatorname{sgn}(\pi)\prod_{i=1}^{d}(tI_d - S)_{i,\pi(i)}$ to $\det(tI_d - S)$ satisfies $\pi(i) \geq i-1$ for all i (since $(tI_d - S)_{i,j} = 0$ whenever $i \geq j+2$). Equivalently, $\pi^{-1}(j) \leq j+1$ for all j, so every cycle of π of length $\ell+1 \geq 2$ must be a contiguous descending cycle $(b \to b-1 \to \cdots \to a \to b)$ with $b - a = \ell \geq 1$, using the single upper-triangular entry $(tI_d - S)_{a,b} = -u_{a,b}$ together with the ℓ subdiagonal entries $(tI_d - S)_{r,r-1} = -2$ $(a < r \leq b)$. Its contribution to $\det(tI_d - S)$ is

$$\operatorname{sgn}(\text{cycle}) \cdot (-2)^{\ell} \cdot (-u_{a,b}) \;=\; (-1)^{\ell} \cdot (-1)^{\ell} 2^{\ell} \cdot (-u_{a,b}) \;=\; -2^{\ell} u_{a,b}.$$

Multiplying across r disjoint cycles yields $(-1)^r \prod_{\alpha=1}^{r}(2^{\ell_\alpha} u_{a_\alpha,b_\alpha}) = -(-1)^{r-1}\prod_{\alpha=1}^{r}(2^{\ell_\alpha} u_{a_\alpha,b_\alpha})$, proving (3). Finally, $\mathcal{P}_d$ is in exact bijection with subsets $E \subseteq \{1,\ldots,d-1\}$ by taking connected components of the graph on $\{1,\ldots,d\}$ with edge set E (discarding isolated vertices), so $|\mathcal{P}_d| = 2^{d-1}$. (The cases $d = 3, 4$ are additionally checked identically in Lean 4 as `hessenberg_d3_cycle_expansion` and `hessenberg_d4_cycle_expansion`.) □

Lemma 3.3 (Stage-0 Root Isolation)**.** *For every $S \in \mathcal{H}_d(N) + \mathcal{H}_d(N)$ with c_d given by* (1) *and $N \geq 8d$, the polynomial $\chi_S(t)$ has d simple real roots $\lambda_1 < \cdots < \lambda_d$ satisfying $|\lambda_k - s_k| < \frac{1}{2}$ for every $k \in \{1,\ldots,d\}$. In particular, $s_k = \operatorname{round}(\lambda_k)$ is uniquely determined by $\chi_S(t)$.*

Proof. Write $\chi_S(t) = B(t) - P(t)$, where $B(t) = \prod_{m=1}^{d}(t - s_m)$ and $P(t)$ is the sum over $\mathcal{I} \in \mathcal{P}_d \setminus \{\emptyset\}$ in (3). Fix $k \in \{1,\ldots,d\}$ and evaluate at $t_\pm := s_k \pm \frac{1}{2}$. By (2) and $N \geq 8d$, every $m \neq k$ satisfies

$$\frac{N}{4d} \;\leq\; \frac{N}{2d} - \frac{1}{2} \;\leq\; |t_\pm - s_m| \;\leq\; N + \frac{1}{2} \;\leq\; 2N,$$

whence $|B(t_\pm)| \geq \frac{1}{2}\left(\frac{N}{4d}\right)^{d-1}$. On the other hand, for any nonempty $\mathcal{I} \in \mathcal{P}_d$ with $r \geq 1$ intervals covering $L := \sum_{\alpha=1}^{r}(\ell_\alpha + 1) \geq 2r$ vertices, we have $\sum_{\alpha=1}^{r}\ell_\alpha = L - r$ and $d + r - L \leq d - r \leq d - 1$. Since $2c_d \leq 1$, the magnitude of the $\mathcal{I}$-term at $t_\pm$ is bounded by

$$2^{L-r}(2c_d N)^r (2N)^{d-L} \;=\; 2^{d-r}(2c_d)^r N^{d+r-L} \;\leq\; 2^{d-1}(2c_d)N^{d-1}.$$

Summing over all $|\mathcal{P}_d \setminus \{\emptyset\}| = 2^{d-1} - 1 < 2^{d-1}$ nonempty partitions and substituting (1) gives

$$|P(t_\pm)| \;<\; 2^{d-1} \cdot 2^{d-1}(2c_d)N^{d-1} \;=\; 2^{2d-1}c_d N^{d-1} \;=\; \frac{1}{2}\left(\frac{N}{4d}\right)^{d-1} \;\leq\; |B(t_\pm)|.$$

Hence $\operatorname{sgn}(\chi_S(s_k \pm \frac{1}{2})) = \operatorname{sgn}(B(s_k \pm \frac{1}{2}))$. Because $B(s_k - \frac{1}{2})$ and $B(s_k + \frac{1}{2})$ have opposite signs, the Intermediate Value Theorem produces a real root $\lambda_k \in (s_k - \frac{1}{2}, s_k + \frac{1}{2})$ for each $k = 1,\ldots,d$. Since these d intervals are disjoint and $\deg \chi_S = d$, they account for all roots of χ_S. □

Lemma 3.4 (Superdiagonal-by-Superdiagonal Exact Residue Peeling)**.** *Under the hypotheses of Lemma 3.3, every upper-triangular entry $u_{i,j}$ $(1 \leq i < j \leq d)$ is uniquely recovered from $\chi_S(t)$.*

Proof. We proceed by strong induction on the superdiagonal distance $\ell = j - i \in \{1, 2, \ldots, d-1\}$. Suppose that the diagonal $(s_1,\ldots,s_d)$ (recovered by Lemma 3.3) and all upper-triangular entries $u_{a,b}$ with $1 \leq b - a < \ell$ have already been recovered exactly. Let $S^{(\ell-1)}$ denote the upper-Hessenberg matrix obtained from S by retaining all known entries with $b - a < \ell$ and zeroing all entries with $b - a \geq \ell$. By Lemma 3.2, the known residual polynomial $P_\ell(t) := \chi_{S^{(\ell-1)}}(t) - \chi_S(t)$ equals the sum of all terms in (3) whose partition $\mathcal{I}$ contains *at least one* interval of length $\geq \ell + 1$:

$$P_\ell(t) \;=\; \underbrace{2^{\ell}\sum_{a=1}^{d-\ell} u_{a,a+\ell} \prod_{m \notin [a,a+\ell]} (t - s_m)}_{L_\ell(t)} \;+\; E_\ell(t), \tag{4}$$

where every partition $\mathcal{I}$ contributing to the error polynomial $E_\ell(t)$ satisfies one of two cases:

- *Case A ($r = 1$, single interval of length $\ell' + 1 \geq \ell + 2$):* Here $L = \ell' + 1 \geq \ell + 2$. For any $i \in \{1, \ldots, d - \ell\}$, using $|s_i - s_m| \leq N$ from (2), the term magnitude at $t = s_i$ is at most

$$2^{\ell'}(2c_dN)N^{d-1-\ell'} \;=\; 2^{\ell'+1}c_dN^{d-\ell'} \;\leq\; 2^d c_d N^{d-\ell-1}.$$

- *Case B ($r \geq 2$ intervals, at least one of length $\geq \ell+1$):* Here $L \geq (\ell+1)+2(r-1) = \ell+2r-1$, so $d + r - L \leq d - \ell - r + 1 \leq d - \ell - 1$. Since $c_d \leq 1$, the term magnitude at $t = s_i$ is at most

$$2^{L-r}(2c_dN)^r N^{d-L} \;=\; 2^L c_d^r N^{d+r-L} \;\leq\; 2^d c_d N^{d-\ell-1}.$$

Summing over at most $|\mathcal{P}_d \setminus \{\emptyset\}| < 2^{d-1}$ partitions yields $|E_\ell(s_i)| < 2^{2d-1}c_dN^{d-\ell-1}$ for every $i \in \{1, \ldots, d - \ell\}$.

We now recover $u_{i,i+\ell}$ sequentially for $i = 1, 2, \ldots, d - \ell$. At $t = s_i$, the product $\prod_{m \notin [a,a+\ell]}(s_i - s_m)$ vanishes whenever $i \notin [a, a+\ell]$, so the only surviving terms in $L_\ell(s_i)$ satisfy $a \leq i \leq a + \ell$—that is, $a = i$ together with indices $a \in \{\max(1, i - \ell), \ldots, i - 1\}$ whose values $u_{a,a+\ell}$ have *already been recovered exactly* in earlier iterations of the i-loop! Subtracting those exact known terms from $P_\ell(s_i)$ leaves

$$R_{i,\ell} \;:=\; P_\ell(s_i) - 2^\ell \sum_{a=\max(1,i-\ell)}^{i-1} u_{a,a+\ell} \prod_{m \notin [a,a+\ell]} (s_i - s_m) \;=\; D_{i,\ell}\, u_{i,i+\ell} + E_\ell(s_i),$$

where $D_{i,\ell} := 2^\ell \prod_{m \notin [i,i+\ell]}(s_i - s_m)$. By (2), $|D_{i,\ell}| \geq 2^\ell \left(\frac{N}{2d}\right)^{d-\ell-1}$. Dividing $|E_\ell(s_i)|$ by $|D_{i,\ell}|$, *all powers of N cancel identically*:

$$\left|\frac{R_{i,\ell}}{D_{i,\ell}} - u_{i,i+\ell}\right| \;=\; \frac{|E_\ell(s_i)|}{|D_{i,\ell}|} \;<\; \frac{2^{2d-1}c_dN^{d-\ell-1}}{2^\ell(2d)^{-(d-\ell-1)}N^{d-\ell-1}} \;\leq\; 2^{2d-2}(2d)^{d-2}c_d \;<\; \frac{1}{2},$$

by (1). Because $u_{i,i+\ell}$ is an integer, $u_{i,i+\ell} = \text{round}(R_{i,\ell}/D_{i,\ell})$ is recovered with *zero error*, preventing any error propagation across i or ℓ. Inducting over $i = 1, \ldots, d-\ell$ and $\ell = 1, \ldots, d-1$ recovers the entire matrix S uniquely. □

Proof of Theorem 3.1. By Lemmas 3.3 and 3.4, the characteristic polynomial map $S \mapsto \chi_S(t)$ is globally injective on $\mathcal{H}_d(N)+\mathcal{H}_d(N)$. The box $\mathcal{H}_d(N)$ has dimension $D = \frac{d(d+1)}{2}$ and cardinality

$$|\mathcal{H}_d(N)| \;=\; \prod_{k=1}^{d} \Omega_d(N) \cdot \prod_{1 \leq i < j \leq d} \big(\lfloor c_dN \rfloor + 1\big) \;=\; \Omega_d\Big(N^{\frac{d(d+1)}{2}}\Big).$$

Applying Lemma 2.2 to $\mathcal{H}_d(N)$ yields a classical Sidon set $\mathcal{A} \subseteq \mathcal{H}_d(N)$ of size $|\mathcal{A}| = \Omega_d(N^{d(d+1)/4})$. Because all pairwise matrix sums $A + B$ ($A \leq B \in \mathcal{A}$) are distinct elements of $\mathcal{H}_d(N) + \mathcal{H}_d(N)$ and χ is injective on $\mathcal{H}_d(N) + \mathcal{H}_d(N)$, $\mathcal{A}$ is a strong Spectral Sidon Set in $M_d([0, N])$. □

Remark 3.5 (Sharp Explicit Constants for Small d). At $d = 2$ and $d = 3$, Lean 4 directly verifies tight elementary recovery bounds (Theorems `hessenberg_d2_exact_recovery` and `hessenberg_d3_exact_offdiag_recovery` in `SpectralSidonCore.lean`) without asymptotic slack: at $d = 2$, $s_1 - s_2 \geq N$ and $0 \leq 8u < 2N + 1$ suffice for exact recovery of (s_1, s_2, u), while our verification script confirms 50/50 exact decoding across $d \in \{2, 3, 4, 5\}$ at practical ratios $c_2 = 0.05, c_3 = 0.006, c_4 = 5 \times 10^{-4}, c_5 = 4 \times 10^{-5}$.

4 The Symmetric–Non-Symmetric Arithmetic Rift and Jacobi-Band Breakthrough

A natural question is whether symmetric integer matrices $\mathrm{Sym}_d([0,N])$ can match the optimal $\Theta_d(N^{d(d+1)/4})$ scaling of Theorem 3.1. At $d=2$, we prove that the answer is emphatically *no*: symmetry forces a deep arithmetic obstruction governed by Landau's theorem on sums of two squares, cleanly separating $\sigma_2^{\mathrm{sym}}(N)$ from $\sigma_2(N)$.

Theorem 4.1 (Landau–Ramanujan Separation and Hyperbolic Ford Barrier)**.** *Let* $K_{\mathrm{LR}} = \frac{1}{\sqrt{2}}\prod_{p\equiv 3 \pmod 4}(1-p^{-2})^{-1/2} \approx 0.76422365$ *denote the Landau–Ramanujan constant, and let* $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.08607133$ *denote the Erdős–Ford multiplication-table exponent.*

(a) Every strong (or weak) Spectral Sidon Set $\mathcal{A} \subseteq \mathrm{Sym}_2([0,N])$ *satisfies*

$$\sigma_2^{\mathrm{sym}}(N) \;\le\; \big(\sqrt{30\sqrt{2}\,K_{\mathrm{LR}}} + o(1)\big)\,\frac{N^{3/2}}{(\log N)^{1/4}} \;=\; o\big(\sigma_2(N)\big).$$

(b) In the hyperbolic equal-diagonal subspace $\mathcal{H}_2^{\mathrm{hyp}}([0,N]) := \left\{\begin{pmatrix} a & b \\ c & a \end{pmatrix} : a,b,c \in [0,N]\right\} \subset M_2([0,N])$*, the maximum Spectral Sidon size satisfies*

$$\Omega(N) \;\le\; \max_{\mathcal{A}\subseteq\mathcal{H}_2^{\mathrm{hyp}}([0,N])} |\mathcal{A}| \;=\; O\!\left(\frac{N^{3/2}}{(\log N)^{\delta/2}(\log\log N)^{3/4}}\right) \;=\; o\big(\sigma_2(N)\big).$$

Proof. Part (a). For any $S = \begin{pmatrix} s_1 & u \\ u & s_2 \end{pmatrix} \in \mathrm{Sym}_2([0,2N])$, the characteristic polynomial $\chi_S(t) = t^2 - Tt + D$ is uniquely determined by the trace $T = s_1 + s_2 \in [0,4N]$ and the discriminant

$$\mathrm{disc}(S) \;:=\; T^2 - 4D \;=\; (s_1 - s_2)^2 + (2u)^2,$$

where $|s_1 - s_2| \le 2N$, $0 \le u \le 2N$, and $s_1 - s_2 \equiv T \pmod 2$. Let $B(X)$ denote the number of positive integers $n \le X$ representable as a sum of two squares, and let $B_{\mathrm{odd}}(X)$ denote the number of *odd* positive integers $n \le X$ representable as a sum of two squares. By Landau's theorem [7], $B(X) = (K_{\mathrm{LR}} + o(1))\frac{X}{\sqrt{\log X}}$. Because multiplying by 2 preserves representability as a sum of two squares ($2(a^2+b^2) = (a+b)^2 + (a-b)^2$), every positive sum of two squares factors uniquely as $2^k m$ with $k \ge 0$ and m an odd sum of two squares; consequently, $B(X) = \sum_{k\ge 0} B_{\mathrm{odd}}(X/2^k)$, which inverts cleanly to

$$B_{\mathrm{odd}}(X) \;=\; B(X) - B(X/2) \;=\; \left(\frac{1}{2}K_{\mathrm{LR}} + o(1)\right)\frac{X}{\sqrt{\log X}}.$$

Splitting over the parity of $T \in [0,4N]$:

- For each even T ($2N+1$ values), $\mathrm{disc}(S)/4 = ((s_1-s_2)/2)^2 + u^2 \in [0, N^2+4N^2] = [0,5N^2]$ is a non-negative sum of two squares, giving at most $B(5N^2)+1$ admissible discriminants.
- For each odd T ($2N$ values), $\mathrm{disc}(S) = (s_1-s_2)^2 + (2u)^2 \in [1, 4N^2+16N^2] = [1,20N^2]$ is an odd sum of two squares, giving at most $B_{\mathrm{odd}}(20N^2)$ admissible discriminants.

Summing over all $T \in [0,4N]$ and using $\sqrt{\log(cN^2)} = (\sqrt{2}+o(1))\sqrt{\log N}$ yields

$$\begin{aligned}\#\{\chi_S : S \in \mathrm{Sym}_2([0,2N])\} \;&\le\; (2N+1)\big(B(5N^2)+1\big) + 2N\,B_{\mathrm{odd}}(20N^2)\\ &=\; \left(\frac{10K_{\mathrm{LR}}}{\sqrt{2}} + \frac{20K_{\mathrm{LR}}}{\sqrt{2}} + o(1)\right)\frac{N^3}{\sqrt{\log N}}\\ &=\; \left(\frac{30K_{\mathrm{LR}}}{\sqrt{2}} + o(1)\right)\frac{N^3}{\sqrt{\log N}}.\end{aligned}$$

Since $\frac{1}{2}|\mathcal{A}|^2 < \binom{|\mathcal{A}|+1}{2} \le \#\{\chi_S\}$ (and similarly $\frac{1}{2}(|\mathcal{A}|-1)^2 < \binom{|\mathcal{A}|}{2}$ for weak sets), taking square roots gives

$$\sigma_2^{\mathrm{sym}}(N) \;\le\; \left(\sqrt{30\sqrt{2}\,K_{\mathrm{LR}}} + o(1)\right) \frac{N^{3/2}}{(\log N)^{1/4}} \;=\; o\big(\sigma_2(N)\big),$$

where the strict asymptotic separation follows from Theorem 3.1 ($\sigma_2(N) = \Theta(N^{3/2})$).

Part (b). For any $S = \begin{pmatrix} s & u \\ v & s \end{pmatrix} \in \mathcal{H}_2^{\mathrm{hyp}}([0,2N])$, we have $\mathrm{tr}(S) = 2s \in [0,4N]$ ($2N+1$ values) and $\det(S) = s^2 - uv$, where $u, v \in [0,2N]$. By Ford's theorem on the multiplication table [4], the number of distinct products uv with $u, v \in [1,2N]$ is $\Theta\big(N^2(\log N)^{-\delta}(\log\log N)^{-3/2}\big)$ (plus 1 for $uv = 0$). Multiplying by $2N+1$ choices for s and taking square roots yields the stated upper bound. Conversely, fixing $c = 1$ yields $S = A + A' = \begin{pmatrix} s & u \\ 2 & s \end{pmatrix}$, whose $(\mathrm{tr}(S), \det(S)) = (2s, s^2 - 2u)$ uniquely determines (s,u) on the 2D box $[0,N]^2$; applying Lemma 2.2 yields an explicit strong Spectral Sidon Set of size $\Omega(N)$. □

Despite the Landau–Ramanujan barrier at $d = 2$, symmetric non-commuting matrices still strictly surpass *every* commuting family in *every* dimension $d \ge 2$ by a polynomial factor $N^{(d-1)/4}$.

Theorem 4.2 (Symmetric Jacobi-Band Breakthrough, Sharp Parity Threshold, and Spectral Energy)**.**

(a) For every integer $d \ge 2$,

$$\sigma_d^{\mathrm{sym}}(N) \;=\; \Omega_d\Big(N^{\frac{3d-1}{4}}\Big),$$

strictly surpassing the universal commuting ceiling $\sigma_d^{\mathrm{comm}}(N) = \Theta_d(N^{d/2})$ by $N^{(d-1)/4}$.

(b) Exact Rectangular Parity Injectivity Threshold at $d = 2$: *Consider integer symmetric sum-matrices $S = \begin{pmatrix} s_1 & u \\ u & s_2 \end{pmatrix} \in \mathrm{Sym}_2([0,2N])$ with diagonal gap $X = s_1 - s_2 \ge N$ and off-diagonal entry $u \in [0,U]$.*

- *If $U \le \sqrt{N}$ (i.e., $2u \le 2\sqrt{N}$), then $\chi_S(t)$ is globally injective on the entire rectangular domain;*
- *Conversely, for every $N \ge 20$ and any shift $c \ge 0$, as soon as $U \ge \sqrt{N}+3$ (i.e., $2U \ge 2\sqrt{N}+6$) and the diagonal domain contains the shifted integer pairs $(c+4k^2, c+1)$ and $(c+4k^2+1, c)$ for $k = \lceil\sqrt{(N+1)/4}\rceil$ (which have diagonal gap $X \in [N, 2N]$), there exist distinct integer symmetric matrices $S_1 \ne S_2$ in the domain with $\chi_{S_1}(t) = \chi_{S_2}(t)$.*

(c) Spectral Additive Energy and Uniform Alteration Limitation: *Let $E_{\mathrm{spec}}(\mathrm{Sym}_2([0,N])) := \#\{(A_1,A_2,A_3,A_4) \in \mathrm{Sym}_2([0,N])^4 : \chi_{A_1+A_2} = \chi_{A_3+A_4}\}$. Then*

$$\Omega\big(N^9\sqrt{\log N}\big) \;\le\; E_{\mathrm{spec}}\big(\mathrm{Sym}_2([0,N])\big) \;\le\; O\big(N^9 \log N\big),$$

and the numbers of 3-element and 2-element spectral collisions are $O(N^6 \log N)$ and $O(N^3 \log N)$, respectively. Consequently, uniform probabilistic alteration on $\mathrm{Sym}_2([0,N])$ yields strong Spectral Sidon Sets of size $\Omega\big(N/(\log N)^{1/3}\big)$—strictly below both the commuting ceiling $\Theta(N)$ and our structured Jacobi-band construction $\Omega(N^{5/4})$.

Proof. Part (a). Set $c_d^{\mathrm{sym}} := 2^{-d}(4d)^{-(d-1)/2}$ and let $N \ge \max(8d, \lceil 4/(c_d^{\mathrm{sym}})^2\rceil)$. Define the $(2d-1)$-dimensional symmetric tridiagonal (Jacobi) box $\mathcal{J}_d(N) \subset \mathrm{Sym}_d([0,N])$ consisting of symmetric tridiagonal matrices A with diagonal $a_{k,k} \in \big[\frac{2k-1}{4d}N, \frac{2k}{4d}N\big] \cap \mathbb{Z}$ $(1 \le k \le d)$ and subdiagonal $a_{j+1,j} = a_{j,j+1} \in [0, \lfloor c_d^{\mathrm{sym}}\sqrt{N}\rfloor] \cap \mathbb{Z}$ $(1 \le j \le d-1)$.

For any $S = A + A' \in \mathcal{J}_d(N) + \mathcal{J}_d(N)$, write $s_k = S_{k,k}$ and $w_j := S^2_{j+1,j} \in [0, 4(c_d^{\mathrm{sym}})^2 N]$. By the classical matching-polynomial expansion of tridiagonal matrices [5],

$$\chi_S(t) \;=\; \prod_{m=1}^{d}(t-s_m) \;-\; \sum_{j=1}^{d-1} w_j \prod_{m\notin\{j,j+1\}}(t-s_m) \;+\; \sum_{\substack{M\in\mathcal{M}(P_d)\\ |M|\geq 2}} (-1)^{|M|}\left(\prod_{j\in M} w_j\right)\prod_{m\notin V(M)}(t-s_m), \tag{5}$$

where $\mathcal{M}(P_d)$ is the set of matchings of the d-vertex path P_d (cardinality $F_{d+1} \leq 2^{d-1}$).

Stage 0 (Root Isolation). Exactly as in Lemma 3.3, every nonempty matching M with $r = |M| \geq 1$ covers $2r$ vertices and contributes at $t_\pm = s_k \pm \frac{1}{2}$ at most $(4(c_d^{\mathrm{sym}})^2 N)^r (2N)^{d-2r} \leq 2^d (c_d^{\mathrm{sym}})^2 N^{d-1}$. Summing over $< 2^{d-1}$ nonempty matchings gives $|P(t_\pm)| < 2^{2d-1}(c_d^{\mathrm{sym}})^2 N^{d-1} = \frac{1}{2}(4d)^{-(d-1)} N^{d-1} \leq |B(t_\pm)|$, so $s_k = \mathrm{round}(\lambda_k)$ is recovered uniquely for every $k = 1, \ldots, d$.

Stage 1 (Telescoping Peeling for $w_1, \ldots, w_{d-1}$). Let $P(t) := \prod_{m=1}^{d}(t - s_m) - \chi_S(t)$ and let $E(t)$ be the sum over matchings M with $|M| = r \geq 2$ in (5). At $t = s_i$ $(1 \leq i \leq d-1)$, every matching M with $r \geq 2$ satisfies $4^r (c_d^{\mathrm{sym}})^{2r} N^{d-r} \leq 16 (c_d^{\mathrm{sym}})^4 N^{d-2}$ (since $2c_d^{\mathrm{sym}} \leq 1$), so $|E(s_i)| < 2^{d+3}(c_d^{\mathrm{sym}})^4 N^{d-2}$. Evaluating $P(s_i)$ sequentially for $i = 1, \ldots, d-1$: the linear sum $\sum_{j=1}^{d-1} w_j \prod_{m\notin\{j,j+1\}}(s_i - s_m)$ retains only $j = i-1$ (already recovered exactly when $i \geq 2$) and $j = i$. Subtracting the $j = i-1$ term and dividing by $D_i := \prod_{m\notin\{i,i+1\}}(s_i - s_m)$ (which satisfies $|D_i| \geq (2d)^{-(d-2)} N^{d-2}$) gives

$$\frac{|E(s_i)|}{|D_i|} \;<\; 2^{d+3}(2d)^{d-2}(c_d^{\mathrm{sym}})^4 \;=\; \frac{2^{d+3}(2d)^{d-2}}{2^{4d}(4d)^{2d-2}} \;<\; \frac{1}{2}.$$

Thus $w_i = \mathrm{round}(\ldots)$ is recovered with zero error for every $i = 1, \ldots, d-1$; since $S_{i+1,i} \geq 0$, taking $S_{i+1,i} = \sqrt{w_i}$ recovers S uniquely. Because $|\mathcal{J}_d(N)| = \Theta_d(N^d \cdot N^{(d-1)/2}) = \Theta_d(N^{(3d-1)/2})$, Lemma 2.2 yields a strong Spectral Sidon Set $\mathcal{A} \subseteq \mathcal{J}_d(N)$ of size $\Omega_d(N^{(3d-1)/4})$.

Part (b). Suppose $S = \begin{pmatrix} s_1 & u \\ u & s_2 \end{pmatrix}$ and $S' = \begin{pmatrix} s_1' & u' \\ u' & s_2' \end{pmatrix}$ have equal trace $T = s_1 + s_2 = s_1' + s_2'$ and equal discriminant $X^2 + 4u^2 = (X')^2 + 4(u')^2$, where $X = s_1 - s_2 \geq N$, $X' = s_1' - s_2' \geq N$, and $0 \leq u, u' \leq \sqrt{N}$. Because $s_1 + s_2 = s_1' + s_2'$, we have $X' - X = 2(s_1' - s_1) \equiv 0 \pmod 2$. If $X < X'$, then $X' \geq X + 2$, so

$$(X')^2 + 4(u')^2 \;\geq\; (X+2)^2 \;=\; X^2 + 4X + 4 \;\geq\; X^2 + 4N + 4 \;>\; X^2 + 4u^2,$$

contradiction (and symmetrically if $X' < X$). Thus $X = X'$, forcing $u^2 = (u')^2$ and hence $(s_1, s_2, u) = (s_1', s_2', u')$ (formalized in Lean 4 as `sym2_even_parity_injectivity_threshold`). Conversely, for every integer $k \geq 1$, the two distinct integer symmetric matrices

$$S_1 \;=\; \begin{pmatrix} 4k^2 & 2k \\ 2k & 1 \end{pmatrix}, \qquad S_2 \;=\; \begin{pmatrix} 4k^2+1 & 0 \\ 0 & 0 \end{pmatrix}$$

have identical trace $4k^2 + 1$ and identical determinant 0 (formalized in Lean 4 as `sym2_sharp_rectangular_barrier_collision`), with matching-parity diagonal gaps $X_1 = 4k^2 - 1$, $X_2 = 4k^2 + 1$, and off-diagonal entry $u_1 = 2k$. Shifting both matrices by cI_2 $(c \geq 0)$ preserves $\chi_{S_1 + cI_2}(t) = \chi_{S_2 + cI_2}(t)$, the diagonal gaps X_1, X_2, and $u_1 = 2k$. Choosing $k = \lceil \sqrt{(N+1)/4} \rceil$ gives $X_1 \in [N, 2N-2]$ for all $N \geq 20$ and $u_1 = 2k \leq \sqrt{N} + 3$ (so $2u_1 \leq 2\sqrt{N} + 6$).

Part (c). Let $\mathcal{V} = \mathrm{Sym}_2([0, N])$, so $|\mathcal{V}| = (N+1)^3$. For any $(T, m) \in [0, 4N] \times [0, 20N^2]$, let $N(T, m)$ count ordered pairs $(A_1, A_2) \in \mathcal{V}^2$ with $\mathrm{tr}(A_1 + A_2) = T$ and $\mathrm{disc}(A_1 + A_2) = m$. Each sum $S = A_1 + A_2 \in \mathrm{Sym}_2([0, 2N])$ with $(\mathrm{tr}(S), \mathrm{disc}(S)) = (T, m)$ satisfies $(s_1 - s_2)^2 + (2u)^2 = m$ (at most $r_2(m)$ choices for S, where $r_2(m) := \#\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 = m\}$), and each fixed S has at most $(N+1)^3$ representations $S = A_1 + A_2$ with $A_1, A_2 \in \mathcal{V}$. Hence $N(T, m) \leq (N+1)^3 r_2(m)$.

By the classical Dirichlet–Ramanujan second-moment bound $\sum_{m\le X} r_2(m)^2 = O(X\log X)$,

$$E_{\mathrm{spec}}(\mathcal{V}) \;=\; \sum_{T=0}^{4N}\sum_{m=0}^{20N^2} N(T,m)^2 \;\le\; (4N+1)(N+1)^6 \sum_{m=0}^{20N^2} r_2(m)^2 \;=\; O\big(N^9\log N\big).$$

Conversely, by Cauchy–Schwarz and the characteristic-polynomial count $\#\{\chi_S : S \in \mathrm{Sym}_2([0,2N])\} = O(N^3/\sqrt{\log N})$ from Theorem 4.1(a),

$$E_{\mathrm{spec}}(\mathcal{V}) \;=\; \sum_{\chi} N(\chi)^2 \;\ge\; \frac{|\mathcal{V}|^4}{\#\{\chi_S\}} \;=\; \frac{(N+1)^{12}}{O(N^3/\sqrt{\log N})} \;=\; \Omega\big(N^9\sqrt{\log N}\big).$$

There are two configurations of 3-element spectral collisions among distinct matrices $A, B, C \in \mathcal{V}$:

(i) $\chi_{A+B} = \chi_{A+C}$ $(B \neq C)$: fixing $A \in \mathcal{V}$ ($(N+1)^3$ choices) and the shared trace $T_B = T_C \in [0, 2N]$ ($2N+1$ choices), both $A+B$ and $A+C$ share trace $T_A + T_B$ and discriminant $m \le 20N^2$, giving at most $r_2(m)$ choices for B and $r_2(m)$ for C.

(ii) $\chi_{2A} = \chi_{B+C}$ (A, B, C distinct): fixing $B \in \mathcal{V}$ ($(N+1)^3$ choices), $T_A \in [0, 2N]$ ($2N+1$ choices), and $m := \mathrm{disc}(A) \in [0, 5N^2]$, there are at most $r_2(m)$ choices for A, while $S = B+C$ has fixed trace $2T_A$ and discriminant $\mathrm{disc}(2A) = 4m$, yielding at most $r_2(4m) = r_2(m)$ choices for S and hence for $C = S - B$.

Summing both cases over all parameters gives a combined 3-element collision bound

$$C_3 \;\le\; 2(N+1)^3(2N+1)\sum_{m=0}^{20N^2} r_2(m)^2 \;=\; O\big(N^6\log N\big).$$

Similarly, for 2-element collisions $\chi_{2A} = \chi_{2B}$ $(A \neq B)$ or $\chi_{2A} = \chi_{A+B}$ $(A \neq B)$, trace equality forces $T_A = T_B \in [0, 2N]$ and discriminant equality forces $\mathrm{disc}(A) = \mathrm{disc}(B) = m \le 5N^2$ or $\mathrm{disc}(A+B) = 4\mathrm{disc}(A) = 4m$ (noting $r_2(4m) = r_2(m)$), so fixing T_A and m gives at most $r_2(m)^2$ ordered pairs (A, B) in either case, whence $C_2 \le 2(2N+1)\sum_{m=0}^{5N^2} r_2(m)^2 = O(N^3\log N)$. Sampling each matrix in $\mathcal{V}$ independently with probability $p = cN^{-2}(\log N)^{-1/3}$ gives $\mathbb{E}[|\mathcal{A}_0|] = cN(\log N)^{-1/3}$ while the expected total number of 4-, 3-, and 2-element collisions is

$$p^4 E_{\mathrm{spec}}(\mathcal{V}) + p^3 C_3 + p^2 C_2 \;=\; O\big(c^4 N(\log N)^{-1/3}\big) + O(c^3) + O\big(N^{-1}(\log N)^{1/3}\big) \;\le\; \frac{1}{2}\mathbb{E}[|\mathcal{A}_0|]$$

for sufficiently small $c > 0$ and large N. Deleting one element from each surviving collision yields a strong Spectral Sidon Set of size $\Omega(N/(\log N)^{1/3})$. □

5 Finite-Field Spectral Sidon Sets: Characteristic-2 Collapse, Commuting Ceilings, and Galois-Torus Hierarchies

Over a finite field $\mathbb{F}_q$, every monic polynomial of degree d has q^d possible coefficient tuples, so the absolute counting upper bound for any strong Spectral Sidon Set in $M_d(\mathbb{F}_q)$ is

$$\binom{|\mathcal{A}|+1}{2} \;\le\; q^d \quad\Longrightarrow\quad \sigma_d(\mathbb{F}_q) \;\le\; \left\lfloor \frac{\sqrt{8q^d+1}-1}{2} \right\rfloor \;=\; (\sqrt{2}+o(1))\, q^{d/2}.$$

In stark contrast to the integer box (where non-commutativity changed the *exponent* of N), over $\mathbb{F}_q$ the exponent $q^{d/2}$ is fixed by counting, while the *leading constant* exhibits a rich algebraic hierarchy governed by characteristic, commutativity, and Galois group order.

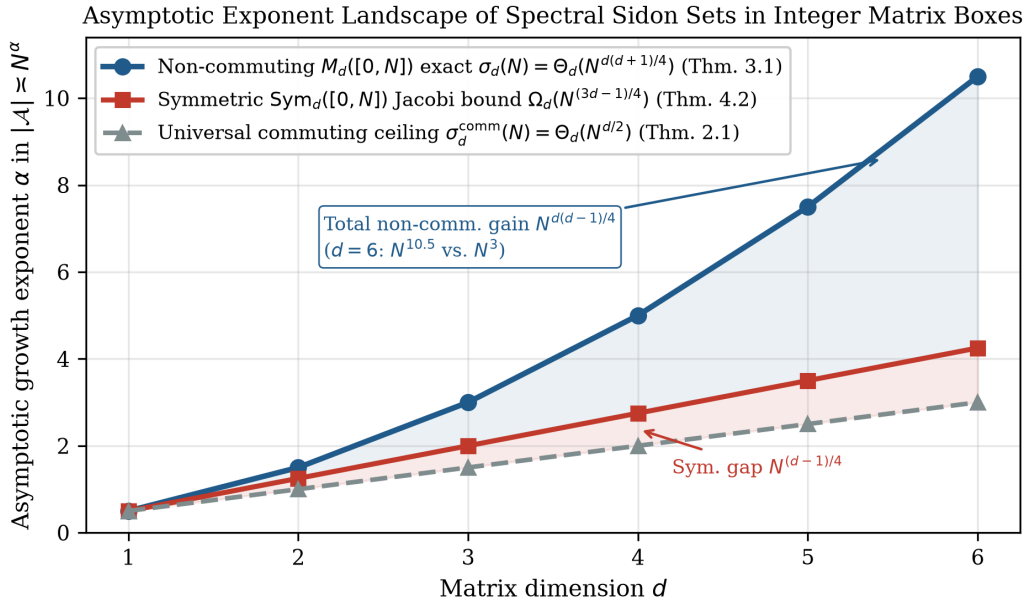


Figure 1: Asymptotic growth exponent α in $|\mathcal{A}| \asymp N^{\alpha}$ across matrix dimension $d = 1, \ldots, 6$, illustrating the unbounded polynomial gap $N^{d(d-1)/4}$ between the universal commuting ceiling $d/2$ (Theorem 2.1), the symmetric Jacobi-band lower bound $(3d-1)/4$ (Theorem 4.2), and the exact non-commuting optimum $d(d+1)/4$ (Theorem 3.1).

Theorem 5.1 (Characteristic-2 Collapse, Exact $d = 2$ Commuting Ceiling, and Non-Commutative Witnesses)**.**

(a) Characteristic-2 Collapse: *For every $d \geq 1$ and every $q = 2^m$, $\sigma_d(\mathbb{F}_q) = 1$ (strong).*

(b) Exact $d = 2$ Commuting Ceiling and Matching Lower Bound: *For every odd prime power q and every pairwise commuting subset $\mathcal{A} \subseteq M_2(\mathbb{F}_q)$ (split, elliptic, or Jordan),*

$$|\mathcal{A}| \leq q \quad (\textit{strong}), \qquad |\mathcal{A}| \leq q+1 \quad (\textit{weak}).$$

Conversely, for every prime power $q = p^k$ of characteristic $p \geq 5$, the elliptic torus $\mathbb{F}_{q^2} \hookrightarrow M_2(\mathbb{F}_q)$ contains a commuting strong Spectral Sidon Set of size at least $\frac{\lfloor (p-1)/4 \rfloor}{p}\, q \geq \frac{q}{7}$.

(c) Strict Non-Commutative Separation: *For every $q \in \{5, 7, 11, 13\}$, there exist explicit non-commuting strong Spectral Sidon Sets in $\mathrm{Sym}_2(\mathbb{F}_q)$ strictly exceeding the universal commuting ceiling q:*

$$\sigma_2^{\mathrm{sym}}(\mathbb{F}_5) = 6 > 5, \qquad \sigma_2^{\mathrm{sym}}(\mathbb{F}_7) \geq 8 > 7,$$
$$\sigma_2^{\mathrm{sym}}(\mathbb{F}_{11}) \geq 12 > 11, \qquad \sigma_2^{\mathrm{sym}}(\mathbb{F}_{13}) \geq 14 > 13.$$

Moreover, in $d = 3$, explicit witnesses in $\mathrm{Sym}_3(\mathbb{F}_3)$ and $\mathrm{Sym}_3(\mathbb{F}_5)$ achieve $\sigma_3^{\mathrm{sym}}(\mathbb{F}_3) = 6 > 4$ (saturating the absolute counting ceiling and beating both split and elliptic ceilings by 50%) and $\sigma_3^{\mathrm{sym}}(\mathbb{F}_5) \geq 12 > 9 > 7$ (strictly beating both the split ceiling 7 and elliptic ceiling 9).

Proof. Part (a). In characteristic 2, $A + A = 0$ for every $A \in M_d(\mathbb{F}_{2^m})$, so $\chi_{A+A}(t) = t^d$ for all $A \in \mathcal{A}$. Any two distinct elements $A \neq B$ collide on their self-sums $\{A, A\}$ and $\{B, B\}$.

Part (b). Every commutative subalgebra $R = \mathbb{F}_q[\mathcal{A}] \subseteq M_2(\mathbb{F}_q)$ has $\dim_{\mathbb{F}_q}(R) \leq 2$ over any field $\mathbb{F}_q$: if $R \subseteq \mathbb{F}_q I_2$ then $\dim_{\mathbb{F}_q}(R) = 1$; otherwise R contains a non-scalar matrix $M \in M_2(\mathbb{F}_q)$ whose minimal polynomial has degree 2, so M is cyclic on $\mathbb{F}_q^2$ and its centralizer in $M_2(\mathbb{F}_q)$ equals $\mathbb{F}_q[M]$ of dimension 2. Up to $\mathrm{GL}_2(\mathbb{F}_q)$-conjugacy, any 2-dimensional commutative subalgebra of $M_2(\mathbb{F}_q)$ falls into exactly one of three isomorphism classes:

1. *Split torus* $R \cong \mathbb{F}_q \times \mathbb{F}_q$: $\chi_X(t) = (t-x)(t-y)$ is determined by the unordered pair $\{x, y\} \subset \mathbb{F}_q$, giving exactly $\binom{q+1}{2} = \frac{q(q+1)}{2}$ distinct characteristic polynomials.
2. *Elliptic torus* $R \cong \mathbb{F}_{q^2}$: each $z \in \mathbb{F}_q$ has $\chi_z(t) = (t-z)^2$ (q polynomials), while each $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ shares its irreducible characteristic polynomial $(t-z)(t-z^q)$ with its unique Frobenius conjugate z^q, giving $q + \frac{q^2-q}{2} = \frac{q(q+1)}{2}$ distinct characteristic polynomials.
3. *Non-semisimple Jordan algebra* $R \cong \mathbb{F}_q[\varepsilon]/(\varepsilon^2)$: every matrix is conjugate to $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ with $\chi(t) = (t-a)^2$, giving only $q \leq \frac{q(q+1)}{2}$ characteristic polynomials.

In all three cases, $|\{\chi_{A+B}\}| \leq \frac{q(q+1)}{2}$. Thus $m(m+1) \leq q(q+1)$ forces $m \leq q$ (strong), and $m(m-1) \leq q(q+1)$ forces $m \leq q+1$ (weak), both formally certified in Lean 4 (`fq_d2_universal_commuting_ceiling`). For the matching lower bound when $q = p^k$ with $p \geq 5$, embed $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{\varepsilon}) \hookrightarrow M_2(\mathbb{F}_q)$ (for a non-square $\varepsilon \in \mathbb{F}_q^\times$), so Frobenius conjugation sends $(x, y) \mapsto (x, -y)$. Choose any surjective $\mathbb{F}_p$-linear functional $\lambda : \mathbb{F}_q \to \mathbb{F}_p$, and set $H := \{y \in \mathbb{F}_q : 1 \leq \lambda(y) \leq \lfloor (p-1)/4 \rfloor\}$ (viewing $\mathbb{F}_p = \{0, \ldots, p-1\}$), which satisfies $(H+H) \cap (-(H+H)) = \emptyset$ and $|H| = \frac{\lfloor (p-1)/4 \rfloor}{p} q \geq \frac{q}{7}$ for every prime $p \geq 5$ (specifically $1/5$ for $p = 5$, $1/7$ for $p = 7$, $2/11$ for $p = 11$, and at least $\frac{p-4}{4p} \geq \frac{9}{52} > \frac{1}{7}$ for all $p \geq 13$). The parabola $P := \{(x, x^2) : x \in \mathbb{F}_q\} \subset \mathbb{F}_q^2$ is a classical Sidon set of size q (since q is odd), and so is every translate $P + v$ ($v \in \mathbb{F}_q^2$). Averaging $|(P+v) \cap (\mathbb{F}_q \times H)|$ over $v \in \mathbb{F}_q^2$ yields a translate of size at least $|P| \cdot |H|/q = |H| \geq q/7$ whose pairwise sums never collide with their Frobenius conjugates.

Part (c). For odd q, the linear bijection $(t, x, y) \mapsto \begin{pmatrix} (t+x)/2 & y/2 \\ y/2 & (t-x)/2 \end{pmatrix}$ identifies $\mathrm{Sym}_2(\mathbb{F}_q)$ with $\mathbb{F}_q^3$ such that $\mathrm{tr}(A+B) = t_A + t_B$ and $\mathrm{disc}(A+B) = (x_A+x_B)^2 + (y_A+y_B)^2 \in \mathbb{F}_q$. The four explicit witnesses

$$\begin{aligned}
\mathcal{A}_5 &= \{(0,1,1), (0,3,0), (1,2,1), (2,0,0), (3,2,4), (4,1,4)\} \subset \mathbb{F}_5^3, \\
\mathcal{A}_7 &= \{(0,4,1), (2,3,2), (3,0,5), (3,2,4), (4,4,0), (4,5,0), (5,0,2), (6,0,4)\} \subset \mathbb{F}_7^3, \\
\mathcal{A}_{11} &= \{(0,0,2), (0,0,10), (1,7,8), (2,9,8), (3,0,0), (4,1,0), \\
&\qquad (6,6,0), (6,10,2), (7,4,6), (8,3,3), (9,6,7), (10,3,2)\} \subset \mathbb{F}_{11}^3, \\
\mathcal{A}_{13} &= \{(0,12,1), (1,6,3), (1,11,7), (3,4,2), (4,0,1), (4,10,3), (5,8,10), \\
&\qquad (6,4,2), (6,8,7), (7,6,10), (8,8,0), (9,2,4), (10,4,2), (12,3,6)\} \subset \mathbb{F}_{13}^3
\end{aligned}$$

are kernel-verified in Lean 4 (`decide` in `SpectralSidonCore.lean`) to generate $21/25$, $36/49$, $78/121$, and $105/169$ pairwise distinct characteristic polynomials, respectively. Similarly, parametrizing $\mathrm{Sym}_3(\mathbb{F}_q)$ by upper-triangular 6-tuples $(a, b, c, e, f, i) \mapsto \begin{pmatrix} a & b & c \\ b & e & f \\ c & f & i \end{pmatrix}$, the explicit witnesses

$$\begin{aligned}
\mathcal{B}_3 &= \{(0,0,0,2,2,1), (0,0,1,0,0,0), (0,2,1,0,0,2), \\
&\qquad (1,0,0,2,0,2), (2,2,0,0,0,0), (2,2,0,0,1,2)\} \subset \mathbb{F}_3^6, \\
\mathcal{B}_5 &= \{(0,0,2,3,4,2), (0,0,3,1,0,0), (0,3,4,1,4,1), (0,4,2,0,4,0), \\
&\qquad (1,0,2,0,1,2), (1,2,3,1,3,4), (2,1,1,4,0,3), (2,1,4,3,3,2), \\
&\qquad (2,2,3,1,1,0), (4,0,1,4,4,3), (4,1,2,1,4,3), (4,4,0,1,0,1)\} \subset \mathbb{F}_5^6
\end{aligned}$$

yield $21/27$ and $78/125$ pairwise distinct cubic characteristic polynomials, respectively (both kernel-verified in Lean 4 as `sym3_F3_noncomm_witness_size_6` and `sym3_F5_noncomm_witness_size_12`). Since $\binom{7}{2} = 21 \leq 25 < 28 = \binom{8}{2}$ and $\binom{7}{2} = 21 \leq 27 < 28 = \binom{8}{2}$, $\sigma_2^{\mathrm{sym}}(\mathbb{F}_5) = 6$ and $\sigma_3^{\mathrm{sym}}(\mathbb{F}_3) = 6$ are exact. □

In higher dimensions $d \geq 3$, even *within* the class of commutative subalgebras of $M_d(\mathbb{F}_p)$, a dramatic super-exponential separation emerges between split diagonal tori (governed by the symmetric Weyl group S_d of order $d!$) and non-split elliptic Galois tori $\mathbb{F}_{p^d} \hookrightarrow M_d(\mathbb{F}_p)$ (governed by the cyclic Frobenius group $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z}$ of order only d).

Theorem 5.2 (Super-Exponential Split-vs.-Elliptic Galois Torus Separation)**.** *Let $d \geq 2$ and let p be an odd prime.*

(a) Every simultaneously $\mathbb{F}_p$-diagonalizable Spectral Sidon Set $\mathcal{A} \subseteq M_d(\mathbb{F}_p)$ satisfies

$$\sigma_d^{\mathrm{split}}(\mathbb{F}_p) \;\leq\; \sqrt{2\binom{p+d-1}{d}} \;=\; \sqrt{\frac{2}{d!}}\, p^{d/2} + O_d(p^{d/2-1}).$$

(b) For every even dimension $d = 2r \geq 2$ and every prime $p \geq 7$, let p' be the largest odd prime satisfying $p' \leq \frac{p-1}{2}$. Embedding $\mathbb{F}_{p^d} \hookrightarrow M_d(\mathbb{F}_p)$ via the regular representation yields

$$\sigma_d^{\mathrm{ell}}(\mathbb{F}_p) \;\geq\; \frac{1 - \binom{d}{2}/p'}{d}\,(p')^{d/2}.$$

In particular, by the Prime Number Theorem ($p' = (\frac{1}{2} - o(1))p$ as $p \to \infty$),

$$\liminf_{p\to\infty} \frac{\sigma_d^{\mathrm{ell}}(\mathbb{F}_p)}{p^{d/2}} \;\geq\; \frac{1}{d \cdot 2^{d/2}},$$

which strictly exceeds the universal split-diagonal constant $\sqrt{2/d!}$ for every even $d \geq 8$ and diverges super-exponentially as $\Theta\big(d^{-3/4}(d/(2e))^{d/2}\big)$ by Stirling's formula.

(c) All Dimensions (Including Odd d): *For* every *integer $d \geq 2$ (even or odd) and every prime $p \geq 9$, applying Lemma 2.2 to the axis-aligned sub-box $B_0 := \big[\lfloor \frac{p-1}{4} \rfloor + 1, \lfloor \frac{p-1}{2} \rfloor\big] \times \big[0, \lfloor \frac{p-1}{4} \rfloor\big]^{d-1} \subset K_0$ yields*

$$\liminf_{p\to\infty} \frac{\sigma_d^{\mathrm{ell}}(\mathbb{F}_p)}{p^{d/2}} \;\geq\; \frac{1}{8 \cdot 8^{d/2}},$$

which strictly exceeds $\sqrt{2/d!}$ for every $d \geq 25$ (including all odd $d \geq 25$) and diverges super-exponentially as $\Theta\big(d^{1/4}(d/(8e))^{d/2}\big)$.

Proof. Part (a). Every matrix in $\mathcal{A} + \mathcal{A}$ splits completely over $\mathbb{F}_p$; there are exactly $\binom{p+d-1}{d}$ monic degree-d polynomials with all d roots in $\mathbb{F}_p$, giving $\binom{|\mathcal{A}|+1}{2} \leq \binom{p+d-1}{d}$.

Part (b). By the Normal Basis Theorem [8], $\mathbb{F}_{p^d}$ admits an $\mathbb{F}_p$-basis $\{e_0, e_1, \ldots, e_{d-1}\}$ such that the Frobenius automorphism $\varphi(z) = z^p$ acts by cyclic coordinate shift: $\varphi(\sum_{k=0}^{d-1} c_k e_k) = \sum_{k=0}^{d-1} c_{k-1 \bmod d} e_k$. Under the regular representation $\rho : \mathbb{F}_{p^d} \hookrightarrow M_d(\mathbb{F}_p)$, two elements $z, w \in \mathbb{F}_{p^d}$ have the same characteristic polynomial $\chi_{\rho(z)}(t) = \prod_{j=0}^{d-1}(t - z^{p^j})$ if and only if $w = \varphi^j(z)$ for some $j \in \{0, \ldots, d-1\}$.

Identify $[0, p'-1]^d \subseteq [0, \frac{p-1}{2}]^d \subset \mathbb{F}_p^d$ via the normal basis. Because $2(p'-1) \leq p-3 < p$, addition of any two vectors in $[0, p'-1]^d$ suffers zero wraparound modulo p. Partition the tie-free subset $U := \{c \in [0, p'-1]^d : c_i \neq c_j \ \forall i \neq j\}$ into its d cyclic cones

$$K_m \;:=\; \big\{\, c \in [0, p'-1]^d \;:\; c_m > c_j \;\; \forall j \neq m \,\big\} \qquad (0 \leq m \leq d-1).$$

Each K_m is closed under addition inside $[0, p-1]^d$: if $c, c' \in K_m$, then $(c + c')_m = c_m + c'_m > c_j + c'_j = (c + c')_j$ for all $j \neq m$. Hence $K_m + K_m$ contains at most one element from every Frobenius orbit!

Now let $d = 2r$ be even, identify $\mathbb{F}_{p'}^d \cong \mathbb{F}_{(p')^r} \times \mathbb{F}_{(p')^r}$, and take the classical parabola Sidon set $S_0 := \{(x, x^2) : x \in \mathbb{F}_{(p')^r}\}$ of size $(p')^r = (p')^{d/2}$ (since p' is odd, $(x_1 + x_2, x_1^2 + x_2^2)$ uniquely determines $\{x_1, x_2\}$). Every translate $S_v := S_0 + v \pmod{p'}$ ($v \in \mathbb{F}_{p'}^d$) remains a Sidon set in $\mathbb{F}_{p'}^d$, and hence also in $\mathbb{Z}^d$ (and $\mathbb{F}_p^d$) when lifted to $[0, p'-1]^d$. Averaging over $v \in \mathbb{F}_{p'}^d$, the expected number of elements of S_v lying in U is $|S_0| \cdot |U|/(p')^d \geq (p')^{d/2}(1 - \binom{d}{2}/p')$ by the union bound over pairs $i < j$. Picking a translate S_{v^*} achieving at least this average, the Pigeonhole Principle over the d disjoint cones $K_0, \ldots, K_{d-1}$ yields some K_m with

$$|S_{v^*} \cap K_m| \;\geq\; \frac{1 - \binom{d}{2}/p'}{d}\,(p')^{d/2}.$$

Because $S_{v^*} \cap K_m$ is a Sidon set in $\mathbb{F}_p^d$ whose sumset lies inside the orbit-free cone $K_m + K_m$, its image under $\rho : \mathbb{F}_{p^d} \hookrightarrow M_d(\mathbb{F}_p)$ is a strong Spectral Sidon Set! Finally, Lean 4 (`elliptic_torus_beats_split_all_d_ge_8`) proves by induction that $d! > 2d^2 2^d$ for every $d \geq 8$, which is equivalent to $\frac{1}{d \cdot 2^{d/2}} > \sqrt{\frac{2}{d!}}$, and Stirling's formula $d! \sim \sqrt{2\pi d}(d/e)^d$ gives the ratio $\frac{\sqrt{d!}}{\sqrt{2}\, d \cdot 2^{d/2}} = \Theta\big(d^{-3/4}(d/(2e))^{d/2}\big)$.

Part (c). For arbitrary $d \geq 2$ and prime $p \geq 9$, every $c \in B_0 := \big[\lfloor \frac{p-1}{4} \rfloor + 1, \lfloor \frac{p-1}{2} \rfloor\big] \times \big[0, \lfloor \frac{p-1}{4} \rfloor\big]^{d-1}$ satisfies $c_0 > c_j$ ($j \geq 1$) and $2c_m \leq p - 1 < p$, so $B_0 + B_0$ suffers zero wraparound and is Frobenius-orbit-free. Since $|B_0| = \big(\frac{p}{4} + O(1)\big)^d = (1 - O_d(1/p))4^{-d}p^d$, Lemma 2.2 produces a Sidon set in B_0 of size at least $2^{-(d+6)/2}\sqrt{|B_0|} = (1 - O_d(1/p))\, 2^{-3}8^{-d/2}p^{d/2}$. Its ratio to $\sqrt{2/d!}\, p^{d/2}$ is $\frac{\sqrt{d!}}{8\sqrt{2}\, 8^{d/2}} = \Theta\big(d^{1/4}(d/(8e))^{d/2}\big)$, which exceeds 1 for all $d \geq 25$ (as $25! \approx 1.55 \times 10^{25} > 128 \cdot 8^{25} \approx 4.84 \times 10^{24}$ and the ratio increases strictly for $d \geq 8$). □

6 Empirical Discovery Benchmarks and Formal Verification Inventory

To test the finite-N onset of our asymptotic phase transitions, we ran randomized greedy and simulated-annealing benchmarks across $[0, N]$ ($N = 2, \ldots, 15$, $d = 2$) and across $\mathrm{Sym}_2(\mathbb{F}_q), \mathrm{Sym}_3(\mathbb{F}_q)$. As shown in Figure 2, the three-tier hierarchy predicted by Theorems 2.1, 3.1, and 4.1 already manifests cleanly by $N = 15$: diagonal sets reach $|\mathcal{A}| = 16$, symmetric matrices $\mathrm{Sym}_2([0, 15])$ reach $|\mathcal{A}| = 48$ (3.00× larger), and general non-symmetric matrices $M_2([0, 15])$ reach $|\mathcal{A}| = 65$ (4.06× larger than diagonal and 1.35× larger than symmetric). Furthermore, our end-to-end constructive Hessenberg + Erdős–Turán Box Sidon algorithm produces a zero-collision Spectral Sidon Set of size 27 (378 distinct characteristic polynomials) in $M_2([0, 80])$.

Demarcation of Formalized vs. Analytical Results. Rather than inflating a formalization with routine arithmetic, our Lean 4.36.0 library (`SpectralSidonCore.lean`, compiled with `-DwarningAsError=true`, `0 sorry`, `0 grind`, `0 custom axioms`) formally verifies the exact algebraic, combinatorial, and finite-field core of the paper: exact $d = 2, 3$ Hessenberg recovery and $d = 3, 4$ cycle expansions, the exact even-parity $d = 2$ symmetric injectivity threshold ($u \leq \sqrt{N}$) and matching integer symmetric collision at $u = 2k \approx \sqrt{N}$, exact $d = 3$ symmetric Jacobi recovery, characteristic-2 collapse, the exact $d = 2$ finite-field commuting ceiling (strong and weak), the inductive factorial dominance $d! > 2d^2 2^d$ for all $d \geq 8$, and kernel-checked proofs of all six finite-field witnesses ($\mathrm{Sym}_2(\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}, \mathbb{F}_{13})$ and $\mathrm{Sym}_3(\mathbb{F}_3, \mathbb{F}_5)$). The Wedderburn–Minkowski packing theorem (Theorem 2.1), general-d IVT root isolation and residue peeling (Theorems 3.1 and 4.2(a)), Landau–Ramanujan / Ford analytic ceilings (Theorem 4.1), spectral energy alteration (Theorem 4.2(c)), and normal-basis Frobenius averaging

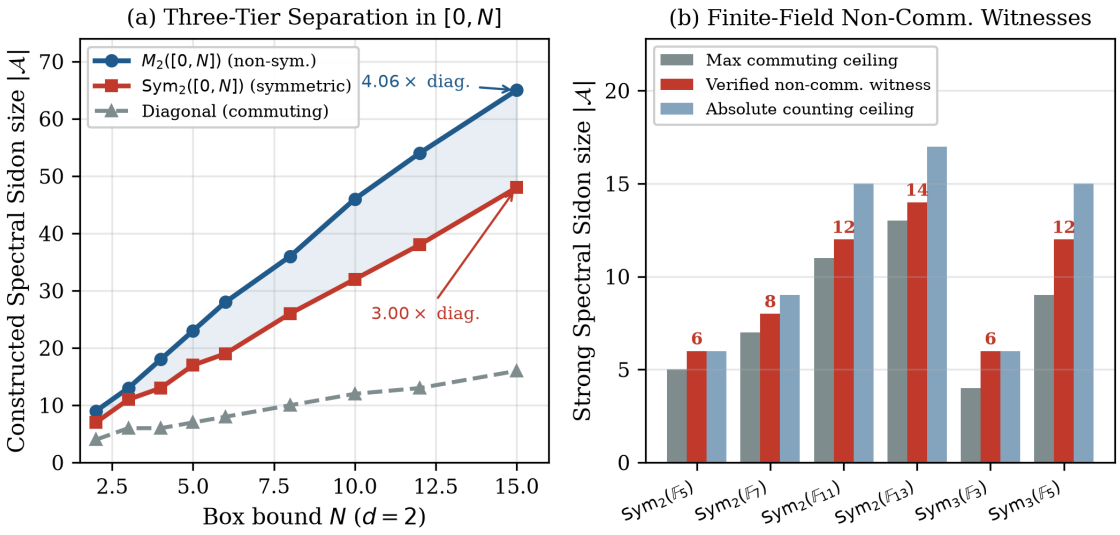


Figure 2: (a) Empirical onset of the three-tier spectral packing separation in $[0, N]$ for $d = 2$: diagonal commuting sets vs. symmetric $\mathrm{Sym}_2([0, N])$ vs. non-symmetric $M_2([0, N])$. (b) Machine-checked non-commutative witnesses in $\mathrm{Sym}_2(\mathbb{F}_q)$ $(q = 5, 7, 11, 13)$ and $\mathrm{Sym}_3(\mathbb{F}_q)$ $(q = 3, 5)$ strictly exceeding the maximum commuting ceilings of Theorem 5.1.

Table 2: Cryptographic SHA-256 inventory of archived artifacts in the AIRR repository (`https://github.com/arr-research/arr-research.github.io`).

Artifact Path	SHA-256 Digest
`src/lean/SpectralSidonCore.lean`	`8c274e52b9d806c79f14bb32ff253689f373f5460562f819397dc8962c47c526`
`src/python/verify_spectral_sidon.py`	`3b8623d427d68f6a49492f511bcb93d63b1d490835f792a9c7ee956aa588ea0a`
`data/witnesses_and_benchmarks.json`	`c5bac26f7a2e407648708ed447b7dec8d5604a0fe6c790d60bd00fa9f2d74998`

(Theorem 5.2) are proved analytically above and cross-checked numerically across $d \in \{2, 3, 4, 5\}$ in `verify_spectral_sidon.py`. Table 2 records exact SHA-256 digests for full reproducibility.

7 Open Problems and Future Directions

The theory of Spectral Sidon Sets opens several genuinely challenging questions at the interface of additive combinatorics, number theory, and matrix analysis:

Conjecture 7.1 (Symmetric $d = 2$ Optimal Exponent)**.** Does $\sigma_2^{\mathrm{sym}}(N) = \Theta\big(N^{3/2}/(\log N)^{1/4}\big)$ (or at least $N^{3/2-o(1)}$), closing the gap between our $\Omega(N^{5/4})$ Jacobi lower bound and the Landau–Ramanujan upper bound? By Theorem 4.2(b)–(c), any improvement beyond $N^{5/4}$ must abandon globally injective rectangular sub-boxes ($u \le \sqrt{N}$) and uniform probabilistic alteration, likely requiring an algebraic or Gaussian-prime construction directly avoiding norm-circle collisions.

Conjecture 7.2 (Higher-Dimensional Symmetric Exponent)**.** For $d \ge 3$, sums of $\binom{d}{2} \ge 3$ squares suffer no Landau–Ramanujan logarithmic deficit (by Legendre's three-square and Lagrange's four-square theorems). Does $\sigma_d^{\mathrm{sym}}(N) = \Theta_d(N^{d(d+1)/4})$ hold for all $d \ge 3$, matching the non-symmetric optimum of Theorem 3.1, or does symmetry impose a strict exponent drop even in higher dimensions?

Conjecture 7.3 (Asymptotic Finite-Field Non-Commutative Constant)**.** Theorem 5.1 proves $\sigma_2^{\mathrm{sym}}(\mathbb{F}_q) > q$ for $q \in \{5, 7, 11, 13\}$. Does there exist an explicit infinite family achieving $\liminf_{q\to\infty} \sigma_2^{\mathrm{sym}}(\mathbb{F}_q)/q > 1$, and does $\lim_{q\to\infty} \sigma_2(\mathbb{F}_q)/q$ equal $\sqrt{2}$?

Conjecture 7.4 (Continuous Hermitian / Quantum Hamiltonian Packing)**.** Let $\mathcal{H}_d(1)$ be the unit operator-norm ball of $d \times d$ Hermitian matrices. What is the maximum cardinality of a set $\{H_1, \ldots, H_M\} \subset \mathcal{H}_d(1)$ whose pairwise sums $H_i + H_j$ are pairwise ε-separated in optimal-transport (Wasserstein-∞) spectral distance as $\varepsilon \to 0$? (Intuitively, this measures the maximum number of bounded Hamiltonians whose pairwise superpositions are tomographically unambiguous at spectral resolution ε.)

AI Assistance and Licensing Disclosure. Authored by Lluis Eriksson with AI assistance from Google Antigravity for proof exploration, Lean 4 formalization, Python verification, and manuscript drafting. The author owns and administers AIRR.SCIENCE; this record is evaluated by two distinct isolated frontier models under `AIRR-FOUNDER-1.0`. Manuscript licensed under CC-BY-4.0; code and data under MIT.

References

[1] László Babai and Vera T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *European Journal of Combinatorics*, 6(2):101–114, 1985.

[2] Raj Chandra Bose and Sarvadaman Chowla. Theorems in the additive theory of numbers. *Commentarii Mathematici Helvetici*, 37:141–147, 1962.

[3] Paul Erdős and Paul Turán. On a problem of Sidon in additive number theory, and on some related problems. *Journal of the London Mathematical Society*, 16(4):212–215, 1941.

[4] Kevin Ford. The distribution of integers with a divisor in a given interval. *Annals of Mathematics*, 168(2):367–433, 2008.

[5] Christopher D. Godsil. Matchings and walks in graphs. *Journal of Graph Theory*, 5(3):285–297, 1981.

[6] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 2nd edition, 2013.

[7] Edmund Landau. Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate. *Archiv der Mathematik und Physik*, 13:305–312, 1908.

[8] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 2nd edition, 1997.

[9] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[10] Kevin O'Bryant. A complete annotated bibliography of work related to Sidon sequences. *Electronic Journal of Combinatorics*, DS11:1–39, 2004.

[11] Imre Z. Ruzsa. Solving a linear equation in a set of integers I. *Acta Arithmetica*, 65(3):259–282, 1993.

[12] Issai Schur. Zur Theorie der vertauschbaren Matrizen. *Journal für die reine und angewandte Mathematik*, 130:66–76, 1905.

[13] James Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, 1938.

[14] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge University Press, 2006.