The exact Sidon constant of {0, 1, 2, 3} and its formalization

Haoxiang Yu
yhx12243@gmail.com

Deepseek
noreply@deepseek.com

Claude Code
noreply@anthropic.com

June 03, 2026

Abstract

We determine the exact value of the Sidon constant of the four-element set $\{0, 1, 2, 3\}$ to be $\frac{5}{3}$. The lower bound was established by Neuwirth via an explicit family of trigonometric polynomials; we prove the matching upper bound. Our proof introduces a new method: given a point on the unit circle we construct a cubic self-inversive polynomial whose three roots lie on the unit circle, extract positive real weights from these roots, and use a weighted square-sum identity to obtain the sharp estimate. The entire proof is formalized in Lean 4 using mathlib.

Keywords Sidon constant · Analysis · Functional Analysis · Formalization · Lean 4

1 Introduction

A set of integers $\Lambda \subset \mathbb{Z}$ is called a **Sidon set** if there exists a constant C such that for every trigonometric polynomial with spectrum in Λ,

$$\sum_{\lambda\in\Lambda}|c_\lambda| \le C \left\|\sum_{\lambda\in\Lambda} c_\lambda e^{i\lambda t}\right\|_\infty, \tag{1}$$

where $\|f\|_\infty = \max_{t\in\mathbb{T}}|f(t)|$ and $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ is the unit circle. The optimal constant $S(\Lambda)$ is the **Sidon constant** of Λ. Equivalently, $S(\Lambda)$ is the supremum of $\sum_{\lambda\in\Lambda}|c_\lambda|$ over all trigonometric polynomials with spectrum in Λ bounded by 1 in supremum norm. Equivalently again, $S(\Lambda)$ is the complex unconditionality constant of the sequence of characters $\{e^{i\lambda t}\}_{\lambda\in\Lambda}$ in the space $C(\mathbb{T})$ of continuous functions on the unit circle.

For the initial segment $\Lambda = \{0, 1, ..., N\}$, Newman (see [1]) obtained the upper bound $S(\Lambda) \le \sqrt{N}$ via an averaging argument over the N-th roots of unity, improving the trivial bound $\sqrt{N+1}$ from Parseval's theorem. Shapiro proved that equality $S(\Lambda) = \sqrt{N}$ can hold exactly when $N \in \{1, 2, 4\}$. In particular, $S(\{0, 1, 2, 3\}) < \sqrt{3} \approx 1.732$, but the exact value was not determined.

For three-element sets, Neuwirth [2] completely solved the problem, proving that

$$S(\{\lambda_0, \lambda_1, \lambda_2\}) = \sec\left(\frac{\pi}{2n}\right), \quad n = \frac{\max|\lambda_i - \lambda_j|}{\gcd(\lambda_1 - \lambda_0, \lambda_2 - \lambda_0)}. \tag{2}$$

This yields $S(\{0, 1, 2\}) = \sqrt{2}$ and $S(\{0, 1, 3\}) = \frac{2}{\sqrt{3}}$, but $\{0, 1, 2, 3\}$ is a set of four elements and does not fit this framework. In that same paper, Neuwirth conjectured $S(\{0, 1, 2, 3\}) = \frac{5}{3}$.

The lower bound $\frac{5}{3} \le S(\{0, 1, 2, 3\})$ was established by Neuwirth [3] twenty-five years later, together with a proof that the **real** unconditional constant of $\{0, 1, 2, 3\}$ is exactly $\frac{5}{3}$ and the general upper bound $S(\Lambda) \le \sqrt{|\Lambda| - 1}$ for all finite Λ. The sharp upper bound for the complex Sidon constant, however, remained open.

In this paper we prove the upper bound $S(\{0, 1, 2, 3\}) \le \frac{5}{3}$, thereby establishing:

Main Theorem. $S(\{0,1,2,3\}) = \frac{5}{3}$.

Our proof introduces a method that may be of independent interest. Given a unimodular parameter ξ (which encodes the relative phase between the extremal coefficients a_0 and a_3), we construct the cubic polynomial

$$P(X) = X^3 - \psi X^2 + \psi X - \xi, \quad \psi = \frac{\xi + 1}{4}. \tag{3}$$

We prove that P is **self-inversive** and that its three roots z_1, z_2, z_3 all lie on the unit circle. From these roots we extract positive real weights

$$\mu_j = \frac{18}{6 - 2\Re(z_j) + \Re\left(z_j^2\right)} > 0 \tag{4}$$

satisfying four remarkable moment identities:

$$\sum_{j=1}^{3} \mu_j = 10, \quad \sum_{j=1}^{3} \mu_j z_j = 2, \quad \sum_{j=1}^{3} \mu_j z_j^2 = -2, \quad \sum_{j=1}^{3} \mu_j z_j^3 = -1 + 9\xi^*. \tag{5}$$

A weighted square-sum identity then yields, for any polynomial $f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3$ bounded by 1,

$$6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2 \le 10. \tag{6}$$

Together with a reduction step that aligns coefficients and a binary Cauchy–Schwarz estimate, this gives the sharp bound $\sum\|a_j\| \le \frac{5}{3}$.

The entire proof of the upper bound has been formalized in Lean 4 using mathlib. We discuss the formalization in Section 5.

The paper is organized as follows. Section 2 reviews related work. Section 3 collects preliminaries on self-inversive polynomials. Section 4 contains the complete proof, broken into subsections tracing the logical arc described above. Section 5 discusses the formalization. Section 6 lists open questions.

2 Related Works

2.1 The three-element case

Neuwirth [2] solved the extremal problem for sets of three frequencies. By reducing to a real-variable optimization in two parameters and analyzing the critical points of $\Phi(t,\vartheta) = \left|1 + re^{i\vartheta}e^{ikt} + se^{ilt}\right|^2$, he proved that the minimum of $\max_t \Phi(t,\vartheta)$ over phases ϑ oCurs at $\vartheta = \frac{\pi}{l}$ (where k, l are the normalized frequency differences). This yields the exact formula

$$S(\{\lambda_0, \lambda_1, \lambda_2\}) = \sec\left(\frac{\pi}{2n}\right), \tag{7}$$

with $n = \max \frac{|\lambda_i - \lambda_j|}{\gcd(\lambda_1 - \lambda_0, \lambda_2 - \lambda_0)}$. In particular, $S(\{0,1,2\}) = \sqrt{2}$ (recovering Newman's result) and $S(\{0,1,3\}) = \frac{2}{\sqrt{3}}$. The extremal polynomials have coefficients proportional to the frequency gaps and carry sign patterns determined by the 2-adic valuations of the differences. An important consequence is that for three-element sets, the real and complex unconditionality constants coincide in $C(\mathbb{T})$. The paper concludes by conjecturing $S(\{0,1,2,3\}) = \frac{5}{3}$.

2.2 Lower bound and earlier upper bounds

Neuwirth [3] established the lower bound $S(\{0,1,2,3\}) \geq \frac{5}{3}$ by exhibiting a one-parameter family of trigonometric polynomials

$$f_\tau(z) = \frac{i2\sqrt{2}\cos\tau - 1 - 3\sin\tau}{15} + \frac{3+\sin\tau}{10}z + \frac{3-\sin\tau}{10}z^2 + \frac{i2\sqrt{2}\cos\tau - 1 + 3\sin\tau}{15}z^3 \quad (8)$$

whose coefficients satisfy $\sum|c_j| = 1$ for every τ and whose supremum norm is identically $\frac{3}{5}$ on the unit circle. The calculation involves solving the critical point equations of $\Phi(t,\tau) = \left|f(e^{it},\tau)\right|^2$; for each τ there are exactly three points on the circle attaining the maximum $\frac{9}{25}$, and a careful algebraic elimination yields the parameterization.

The same paper also gave an independent proof of the general bound $S(\Lambda) \leq \sqrt{|\Lambda| - 1}$ by interpreting the Sidon constant as the norm of linear functionals on $C_{\Lambda(\mathbb{T})}$ and lifting them to sums of Dirac measures on roots of unity. For $\Lambda = \{0,1,2,3\}$ this gives $S(\Lambda) \leq \sqrt{3}$, which is not sharp. Finally, the real unconditional constant of $\{0,1,2,3\}$ was shown to be exactly $\frac{5}{3}$ by explicitly evaluating all sign patterns modulo symmetries.

What remained open was the sharp upper bound for the complex Sidon constant. Our main contribution is closing this gap.

3 Preliminaries

We work over the complex numbers. The unit circle is $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ and the closed unit disk is $\mathbb{D} = \{z \in \mathbb{C} : |z| \leq 1\}$. For $z \in \mathbb{T}$ we write $z^* = z^{-1}$. $\mathbb{C}[X]$ denotes polynomials in one variable with complex coefficients.

3.1 Sidon constant and linear functionals

For a finite set $\Lambda \subset \mathbb{Z}$, let $C_\Lambda(\mathbb{T})$ be the subspace of $C(\mathbb{T})$ spanned by the characters $\{e_\lambda : z \mapsto z^\lambda\}_{\lambda\in\Lambda}$. A linear functional ℓ on $C_\Lambda(\mathbb{T})$ is determined by its values $u_\lambda = \ell(e_\lambda)$. By the Hahn–Banach and Riesz representation theorems, the norm of ℓ satisfies

$$\|\ell\| = \inf\Big\{\sum|b_k| : \ell(f) = \sum b_k f(z_k), \forall f \in C_{\Lambda(\mathbb{T})}\Big\}, \quad (9)$$

where the z_k are points on $\mathbb{T}$. The Sidon constant admits the dual characterization

$$S(\Lambda) = \sup\{\|\ell\| : |\ell(e_\lambda)| = 1, \forall\lambda \in \Lambda\}. \quad (10)$$

3.2 Self-inversive polynomials

Definition (Self-inversive polynomial). A polynomial $P \in \mathbb{C}[X]$ of degree n is **self-inversive** if

$$P(0)^*\, X^n\, P\Big(\frac{1}{X^*}\Big)^* = \mathrm{lc}(P)^*\, P(X), \quad (11)$$

where $\mathrm{lc}(P)$ is the leading coefficient. Equivalently, for all $0 \leq i \leq n$,

$$\mathrm{lc}(P)^* \cdot \mathrm{coeff}_i(P) = \mathrm{coeff}_{n-i}(P)^* \cdot P(0). \quad (12)$$

Self-inversive polynomials generalize self-reciprocal (palindromic) polynomials and characterize those whose roots are symmetric with respect to the unit circle: if r is a root with multiplicity m, then $\frac{1}{r^*}$ is also a root with the same multiplicity. An immediate consequence:

Lemma (Leading coefficient and constant term). If P is self-inversive and $P(0) \neq 0$, then $\|\mathrm{lc}(P)\| = \|P(0)\|$.

Lemma (Disk to sphere). If P is self-inversive and all its roots lie in the closed unit disk $\mathbb{D}$, then all its roots lie on the unit circle $\mathbb{T}$.

Proof: Let r be a root. By self-inversivity, $\frac{1}{r^*}$ is also a root. If $|r| < 1$ then $\left|\frac{1}{r^*}\right| > 1$, contradicting the assumption that all roots lie in $\mathbb{D}$. The case $|r| > 1$ is excluded by hypothesis. Thus $|r| = 1$.

3.3 Gauss–Lucas theorem

We rely on the following classical result:

Theorem (Gauss–Lucas). The roots of the derivative P' of a polynomial P lie in the convex hull of the roots of P.

In particular, if all roots of P lie in $\mathbb{D}$, then all roots of P' lie in $\mathbb{D}$ as well, since $\mathbb{D}$ is convex.

3.4 Cohn's root theorem about self-inversive polynomials

The following lemma controls the modulus of a self-inversive polynomial's reversal outside the disk. It is a special case of the Cohn's root theorem[4] about self-inversive polynomials.

Lemma (Blaschke product estimate). Let $P \in \mathbb{C}[X]$ have all its roots in $\mathbb{D}$. Then for any $r \in \mathbb{C}$ with $|r| \geq 1$,

$$|P_{\mathrm{rev}}(r)| \leq |P(r)|, \tag{13}$$

where $P_{\mathrm{rev}}(X) = X^{\deg P}\, P\big(\frac{1}{X^*}\big)^*$.

Proof: Factor P over its roots r_k: $P(X) = c\prod(X - r_k)$. Then $P_{\mathrm{rev}}(X) = c^* \prod(1 - r_k^* X)$. Evaluating at r and comparing moduli, each factor satisfies $|r - r_k|^2 - |1 - r_k^* r|^2 = (|r|^2 - 1)\big(1 - |r_k|^2\big) \geq 0$ since $|r_k| \leq 1$ and $|r| \geq 1$. Hence $|1 - r_k^* r| \leq |r - r_k|$ and the product inequality follows.

Theorem (Cohn). Let $P \in \mathbb{C}[X]$ be a self-inversive polynomial. Then all roots of P lie on the unit circle $\mathbb{T}$ if and only if all roots of the derivative P' lie in the closed unit disk $\mathbb{D}$.

Proof. ($\Rightarrow$) If all roots of P lie on $\mathbb{T} \subset \mathbb{D}$, then by Gauss–Lucas the roots of P' lie in the convex hull of the roots of P, which is contained in $\mathbb{D}$.

($\Leftarrow$) Suppose all roots of P' lie in $\mathbb{D}$. Let $\alpha = \mathrm{lc}(P)$, $\beta = P(0)$, and $n = \deg P$. Self-inversivity yields the polynomial identity

$$\alpha^* \cdot (XP'(X)) + \beta \cdot P'_{\mathrm{rev}}(X) = n\alpha^* P(X). \tag{14}$$

Evaluating at any root r of P, we obtain $|rP'(r)| = |P'_{\mathrm{rev}}(r)|$. If $|r| > 1$, the Blaschke estimate applied to P' gives $|P'_{\mathrm{rev}}(r)| \leq |P'(r)|$, hence $|r||P'(r)| \leq |P'(r)|$, forcing $|r| \leq 1$, a contradiction. Thus all roots lie in $\mathbb{D}$, and by the disk-to-sphere lemma they must lie on $\mathbb{T}$. □

4 Solution

In this section we prove the main theorem. Let

$$f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3, \quad a_j \in \mathbb{C}. \tag{15}$$

Assume $\|f\|_\infty \leq 1$, i.e., $|f(z)| \leq 1$ for all $z \in \mathbb{T}$. Our goal is to show $\sum_{j=0}^{3} \|a_j\| \leq \frac{5}{3}$.

4.1 Reduction to aligned coefficients

We first simplify the configuration of the coefficients through two normalization steps.

Lemma (Alignment of a_1, a_2). Without loss of generality, we may assume $\|a_1\| + \|a_2\| = \|a_1 + a_2\|$.

Proof: If $a_1 = 0$ or $a_2 = 0$ the equality is trivial. Otherwise, set $\mu = \text{normalize}\left(\frac{a_1}{a_2}\right)$ (the unimodular complex number with the same argument as $\frac{a_1}{a_2}$). Because $|\mu| = 1$, the rotated polynomial $f(\mu z)$ still satisfies $\|f(\mu\,\cdot)\|_\infty \le 1$, and its coefficients become $(\mu a_1, \mu^2 a_2)$ which are positively aligned: $\|\mu a_1\| + \left\|\mu^2 a_2\right\| = \left\|\mu a_1 + \mu^2 a_2\right\|$. The sum of coefficient moduli is unchanged. Hence we may work with the rotated polynomial.

With a_1, a_2 aligned, we have

$$\|a_0\| + \|a_1\| + \|a_2\| + \|a_3\| = \|a_0\| + \|a_1 + a_2\| + \|a_3\|. \tag{16}$$

Lemma (Alignment of a_0, a_3). There exists $\xi \in \mathbb{T}$ such that $\|a_0\| + \|a_3\| = \|\xi a_0 + a_3\|$.

Proof: This is a general fact: for any two complex numbers a, b with $b \neq 0$, the function $g(z) = \|za + b\| - \|a\|$, defined for unimodular z, attains its maximum value $\|b\|$ at some $\xi \in \mathbb{T}$. (Take $\xi = \text{normalize}\left(\frac{b}{a}\right)$ when $a \neq 0$; otherwise any ξ works.)

Applying both lemmas, we may assume

$$\|a_1\| + \|a_2\| = \|a_1 + a_2\|, \quad \|a_0\| + \|a_3\| = \|\xi a_0 + a_3\| \tag{17}$$

for some fixed ξ with $|\xi| = 1$.

We now apply a binary Cauchy–Schwarz estimate. Write

$$S = \|a_0\| + \|a_1 + a_2\| + \|a_3\| \tag{18}$$

and set $r_1 = \|a_1 + a_2\|$, $r_2 = \|\xi a_0 + a_3\|$. Since $\|a_0\| + \|a_3\| = r_2$, the total sum is $S = r_1 + r_2$. The elementary inequality $(r_1 + r_2)^2 \le (f_1 + f_2)\left(\frac{r_1^2}{f_1} + \frac{r_2^2}{f_2}\right)$ (a Cauchy–Schwarz inequality on a discrete two-point space, with $f_1 = 6$, $f_2 = 9$) gives:

$$S^2 \le (6+9)\left(\frac{\|a_1 + a_2\|^2}{6} + \frac{\|\xi a_0 + a_3\|^2}{9}\right) = 15 \cdot \frac{6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2}{18}. \tag{19}$$

Thus,

$$\left(\sum_{j=0}^{3} \|a_j\|\right)^2 \le (6^{-1} + 9^{-1})\left(6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2\right). \tag{20}$$

The problem is reduced to proving $6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2 \le 10$, which will yield $S^2 \le \frac{5}{18} \cdot 10 = \frac{25}{9}$, hence $S \le \frac{5}{3}$.

4.2 The key polynomial system

Fix $\xi \in \mathbb{T}$ from the previous section. Define

$$\psi = \frac{\xi + 1}{4}, \quad P(X) = X^3 - \psi X^2 + \psi X - \xi. \tag{21}$$

Lemma (Basic properties of P). P is a monic self-inversive polynomial of degree 3.

Proof: Monicity and degree are clear from the definition. For self-inversivity, write $P(X) = X^3 + c_2 X^2 + c_1 X + c_0$ with $c_2 = -\psi$, $c_1 = \psi$, $c_0 = -\xi$. With $c_3 = 1$, the coefficient condition reads $c_0^* c_i = c_{3-i}^* c_3$ for $i = 0, 1, 2, 3$. The key relation is $\psi^* \xi = \psi$, which follows from

$$\psi^* \xi = \frac{\xi^* + 1}{4}\xi = \frac{1 + \xi}{4} = \psi, \tag{22}$$

using $|\xi| = 1$.

Lemma (Roots of Q lie in the open unit disk). Let $Q(X) = P'(X) = 3X^2 - 2\psi X + \psi$. Every root r of Q satisfies $|r| < 1$.

Proof: From $Q(r) = 0$ we have $(2r-1)\psi = 3r^2$. Taking moduli, $3|r|^2 = |2r-1| \cdot |\psi|$. Since $|\xi| = 1$, the triangle inequality gives

$$|\psi| = \frac{|\xi + 1|}{4} \leq \frac{2}{4} = \frac{1}{2}. \tag{23}$$

Thus $3|r|^2 \leq \frac{1}{2} \cdot |2r-1| \leq \frac{1}{2}(2|r|+1) = |r| + \frac{1}{2}$. The inequality $3x^2 \leq x + \frac{1}{2}$ implies $x < 1$, since $3x^2 - x - \frac{1}{2} = 0$ has largest root $\frac{1+\sqrt{7}}{6} \approx 0.607 < 1$.

Theorem (Roots of P lie on the unit circle). All three roots z_1, z_2, z_3 of P satisfy $\left|z_j\right| = 1$, and they are pairwise distinct.

Proof: The previous lemma shows that $Q = P'$ has all its roots in the open unit disk $\mathrm{int}(\mathbb{D})$. In particular, all roots of Q lie in the closed unit disk $\mathbb{D}$. Since P is self-inversive, Cohn's theorem (Section 3) immediately yields that all roots of P lie on the unit circle $\mathbb{T}$: $\left|z_j\right| = 1$ for $j = 1, 2, 3$.

Since all roots of P lie on the unit circle while all roots of P' lie in the open unit disk, P and P' must be coprime, which implies the separability of P. Moreover, z_1, z_2, z_3 are pairwise distinct.

From Vieta's formulas applied to $P(X) = (X - z_1)(X - z_2)(X - z_3)$, we immediately obtain the symmetric sum relations:

Proposition (Root relations): The roots z_1, z_2, z_3 of P satisfy

$$z_1 + z_2 + z_3 = \psi, \quad z_1 z_2 + z_1 z_3 + z_2 z_3 = \psi, \quad z_1 z_2 z_3 = \xi. \tag{24}$$

In particular, $\left|z_j\right| = 1$ for $j = 1, 2, 3$.

4.3 The Λ coefficients and moment identities

We now define a rational function Λ of three variables that, when evaluated at the roots of P, produces positive real weights.

Definition (Λ coefficients). For distinct complex numbers z_1, z_2, z_3, define

$$\Lambda(z_1, z_2, z_3) = \frac{2(5z_2 z_3 - z_2 - z_3 - 1)}{(z_1 - z_2)(z_1 - z_3)}. \tag{25}$$

Set $\mu_1 = \Lambda(z_1, z_2, z_3)$, $\mu_2 = \Lambda(z_2, z_3, z_1)$, $\mu_3 = \Lambda(z_3, z_1, z_2)$, obtained by cyclic permutation.

Theorem (Moment identities). The weights μ_1, μ_2, μ_3 satisfy:

$$\begin{aligned} \mu_1 + \mu_2 + \mu_3 &= 10, \\ \mu_1 z_1 + \mu_2 z_2 + \mu_3 z_3 &= 2, \\ \mu_1 z_1^2 + \mu_2 z_2^2 + \mu_3 z_3^2 &= -2, \\ \mu_1 z_1^3 + \mu_2 z_2^3 + \mu_3 z_3^3 &= -1 + 9\xi. \end{aligned} \tag{26}$$

Proof: These identities are verified by rational function algebra. The denominators $(z_1 - z_2)(z_1 - z_3)$ are nonzero because the z_j are pairwise distinct. Clearing denominators, each identity reduces to a polynomial relation among z_1, z_2, z_3 that follows from the root relations $z_1 + z_2 + z_3 = \psi$, $z_1 z_2 + z_1 z_3 + z_2 z_3 = \psi$, $z_1 z_2 z_3 = \xi$, together with $\psi = \frac{\xi+1}{4}$. The computations are elementary though lengthy; the Lean formalization carries them out using the `field` tactic for rational simplifications.

As an illustration, for the cubic moment (5), we use $z_j^3 = \psi z_j^2 - \psi z_j + \xi$ (since $P(z_j) = 0$) together with moments (2)–(4) and $\psi = \frac{\xi+1}{4}$:

$$\begin{aligned}\sum \mu_j z_j^3 &= \psi \sum \mu_j z_j^2 - \psi \sum \mu_j z_j + \xi \sum \mu_j \\ &= \psi(-2) - \psi(2) + \xi(10) \\ &= -4\psi + 10\xi \\ &= -4\frac{\xi+1}{4} + 10\xi \\ &= -1 + 9\xi.\end{aligned} \tag{27}$$

The second crucial fact is that these weights are positive reals.

Lemma (Positivity of the weights). When $|z_1| = |z_2| = |z_3| = 1$, the weight $\mu_1 = \Lambda(z_1, z_2, z_3)$ depends only on z_1 and simplifies to a positive real number:

$$\Lambda(z_1, z_2, z_3) = \frac{36z_1^2}{1 - 2z_1 + 12z_1^2 - 2z_1^3 + z_1^4} = \frac{18}{6 - 2\Re(z_1) + \Re(z_1^2)} > 0. \tag{28}$$

In particular, μ_1, μ_2, μ_3 are all positive real numbers.

Proof: Using the root relations and $P(z_1) = 0$, express ψ and the symmetric sums of z_2, z_3 in terms of z_1. Concretely, $z_2 + z_3 = \psi - z_1$ and $z_2 z_3 = \psi - z_1(z_2 + z_3) = \psi - z_1(\psi - z_1) = z_1^2 - \psi z_1 + \psi$. Using $P(z_1) = 0$ to eliminate ψ, the rational expression simplifies to the stated form.

For $|z| = 1$, we use $z^{-1} = z^*$ to rewrite the denominator:

$$\begin{aligned}1 - 2z + 12z^2 - 2z^3 + z^4 &= z^2(z^{-2} - 2z^{-1} + 12 - 2z + z^2) \\ &= z^2\left(z^{*^2} - 2z^* + 12 - 2z + z^2\right) \\ &= z^2(12 - 4\Re(z) + 2\Re(z^2)).\end{aligned} \tag{29}$$

Thus $\Lambda' = 36\frac{z^2}{z^2(12-4\Re(z)+2\Re(z^2))} = \frac{18}{6-2\Re(z)+\Re(z^2)}$.

The denominator is strictly positive because for $|z| \le 1$, $6 - 2\Re(z) + \Re(z^2) \ge 6 - 2 - 1 = 3 > 0$.

4.4 The weighted square-sum identity

Consider $f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3$. For any $z \in \mathbb{T}$, the modulus squared expands as a Hermitian form:

$$|f(z)|^2 = \left(\sum_{j=0}^{3} a_j z^j\right)\left(\sum_{k=0}^{3} a_k^* z^{*^k}\right) = \sum_{j,k=0}^{3} a_j a_k^*, z^{j-k}. \tag{30}$$

Using $z^* = z^{-1}$ on $\mathbb{T}$, we can write this as a Laurent polynomial whose real part is a trigonometric polynomial in the argument of z. Concretely,

$$|f(z)|^2 = \Re\left(\sum_{j=0}^{3} |a_j|^2 + 2(a_0^* a_1 + a_1^* a_2 + a_2^* a_3)z + 2(a_0^* a_2 + a_1^* a_3)z^2 + 2a_0^* a_3 z^3\right). \tag{31}$$

Now evaluate this expression at z_1, z_2, z_3, multiply by the positive weights μ_1, μ_2, μ_3, and sum.

Theorem (Weighted square-sum identity).

$$\sum_{j=1}^{3} \mu_j \left|f(z_j)\right|^2 = |a_0 + 2a_1 - 2a_2 - a_3|^2 + 6|a_1 + a_2|^2 + 9|\xi^* a_0 + a_3|^2. \tag{32}$$

Proof: Writing $\delta_0 = \sum |a_j|^2$, $\delta_1 = a_0^* a_1 + a_1^* a_2 + a_2^* a_3$, $\delta_2 = a_0^* a_2 + a_1^* a_3$, $\delta_3 = a_0^* a_3$, we have

$$\left|f(z_j)\right|^2 = \Re\left(\delta_0 + 2\delta_1 z_j + 2\delta_2 z_j^2 + 2\delta_3 z_j^3\right). \tag{33}$$

Since μ_j are real, the weighted sum is

$$\sum_{j=1}^{3} \mu_j \big|f(z_j)\big|^2 = \Re\big(\delta_0 \sum \mu_j + 2\delta_1 \sum \mu_j z_j + 2\delta_2 \sum \mu_j z_j^2 + 2\delta_3 \sum \mu_j z_j^3\big). \tag{34}$$

Substituting the four moment identities (2)–(5) replaces each sum by its known value, and expanding the real part yields exactly the sum-of-squares expression stated. The computation, while lengthy, is a purely algebraic verification.

4.5 The core inequality

Since $\|f\|_\infty \le 1$, we have $\big|f(z_j)\big| \le 1$ for each root $z_j \in \mathbb{T}$. Because the weights μ_j are positive and sum to 10,

$$\sum_{j=1}^{3} \mu_j, \big|f(z_j)\big|^2 \le \sum_{j=1}^{3} \mu_j = 10. \tag{35}$$

Combined with the weighted square-sum identity, we obtain:

Theorem (Core inequality). For any polynomial $f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3$ bounded by 1 on $\mathbb{T}$, and for the unimodular parameter ξ constructed in Section 4.1,

$$6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2 \le 10. \tag{36}$$

Proof. The three nonnegative terms on the right-hand side of the weighted identity are $|a_0 + 2a_1 - 2a_2 - a_3|^2 \ge 0$, $6|a_1 + a_2|^2 \ge 0$, and $9|\xi^* a_0 + a_3|^2 \ge 0$. Discarding the first term and applying the bound $\sum \mu_j \big|f(z_j)\big|^2 \le 10$ gives $6|a_1 + a_2|^2 + 9|\xi^* a_0 + a_3|^2 \le 10$. Taking norms (which equal absolute values for complex numbers) completes the proof.

4.6 Completion of the upper bound

We now assemble the pieces.

Theorem (Upper bound). $S(\{0,1,2,3\}) \le \frac{5}{3}$.

Proof Let $f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3$ satisfy $\|f\|_\infty \le 1$. By the reduction in Section 4.1, we may assume $\|a_1\| + \|a_2\| = \|a_1 + a_2\|$ and $\|a_0\| + \|a_3\| = \|\xi a_0 + a_3\|$ for some $\xi \in \mathbb{T}$.

The binary Cauchy–Schwarz reduction (1) gives

$$\left(\sum_{j=0}^{3} \|a_j\|\right)^2 \le (6^{-1} + 9^{-1})\big(6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2\big). \tag{37}$$

The core inequality (Section 4.5) gives $6\|a_1 + a_2\|^2 + 9\|\xi a_0 + a_3\|^2 \le 10$.

Therefore

$$\left(\sum_{j=0}^{3} \|a_j\|\right)^2 \le \left(\frac{1}{6} + \frac{1}{9}\right) \cdot 10 = \frac{5}{18} \cdot 10 = \frac{25}{9}. \tag{38}$$

Taking square roots yields $\sum \|a_j\| \le \frac{5}{3}$, as claimed.

4.7 The lower bound

For completeness we recall the lower bound established by Neuwirth [3].

Theorem (Lower bound). $S(\{0,1,2,3\}) \ge \frac{5}{3}$.

Proof. Consider the one-parameter family of polynomials

$$f_{\tau(z)} = \frac{i2\sqrt{2}\cos\tau - 1 - 3\sin\tau}{15} + \frac{3+\sin\tau}{10}z + \frac{3-\sin\tau}{10}z^2 + \frac{i2\sqrt{2}\cos\tau - 1 + 3\sin\tau}{15}z^3, \quad (39)$$

parametrized by $\tau \in \mathbb{R}$. A direct verification shows that $\sum_{j=0}^{3}|c_j| = 1$ independently of τ. Setting $\Phi(t,\tau) = \left|f_\tau(e^{it})\right|^2$, an algebraic computation yields

$$\begin{aligned}\Phi(t,\tau) = \frac{2\sqrt{2}\sin(2\tau)}{75}(\sin t - \sin 2t + 2\sin 3t) + \frac{247 - 13\cos(2\tau)}{900} \\ +(1+\cos(2\tau))\left(\frac{\cos t}{20} - \frac{\cos 2t}{25}\right) + \frac{1+17\cos(2\tau)}{225}\cos 3t.\end{aligned} \quad (40)$$

Solving the critical point equations $\frac{\partial\Phi}{\partial t} = 0$ and $\frac{\partial\Phi}{\partial\tau} = 0$ shows that for each τ, the global maximum of $\Phi(t,\tau)$ is $\frac{9}{25}$, attained at exactly three points on the circle. Hence $\|f_\tau\|_\infty = \frac{3}{5}$, and the ratio of coefficient sum to supremum norm is $\frac{1}{\frac{3}{5}} = \frac{5}{3}$. The Sidon constant, being the supremum of such ratios, is therefore at least $\frac{5}{3}$.

Together with the upper bound, this completes the proof of the Main Theorem: $S(\{0,1,2,3\}) = \frac{5}{3}$.

5 Formalization

The entire proof of the upper bound (Sections 4.1–4.6) has been formalized in Lean 4 using the mathlib library. The source code is available at https://github.com/yhx-12243/Sidon3, consists of six source files.

5.1 Module structure

The formalization mirrors the logical structure of the paper:

- `Polynomial/SelfInversive.lean` defines self-inversive polynomials and proves the disk/sphere lemma. This uses the root symmetry property (r is a root iff $\frac{1}{r^*}$ is) and relies on mathlib's C*-algebra norm library for $\|\mathrm{lc}(P)\| = \|P(0)\|$.
- `Polynomial/Cohn.lean` proves the Blaschke product estimate and uses it to establish: for a self-inversive P, the roots of P lie on the unit sphere iff the roots of P' lie in the closed unit disk. The proof constructs an algebraic identity relating P, P', and the reversal of P', then applies the Blaschke estimate.
- `KeySystem.lean` is the heart of the proof. It defines $\psi = \frac{\xi+1}{4}$, the cubic $P(X) = X^3 - \psi X^2 + \psi X - \xi$, and its derivative Q. It proves P is self-inversive and separable, that the roots of Q lie in the open unit disk, and hence (via the Cohn lemma) the three roots z_1, z_2, z_3 of P lie on the unit circle. Vieta's formulas give the symmetric sum relations. The Λ coefficients are defined and the four moment identities are proved using field arithmetic; the positivity of the weights is established by the rational simplification to $\mu_j = \frac{18}{6-2\Re(z_j)+\Re(z_j^2)}$.
- `SquareCoeffBound.lean` proves the weighted square-sum identity. Expanding $|f(z)|^2$ on the unit circle as a Hermitian form, it evaluates the μ-weighted sum at the three roots, substitutes the moment identities, and simplifies to the sum-of-squares decomposition. From this and the hypothesis $\|f\|_\infty \le 1$, it deduces the core inequality.
- `Main.lean` assembles the final proof. It handles the two coefficient alignment reductions (using `NormedSpace.normalize` for unimodular rotation), states the binary Cauchy–Schwarz inequality, and chains everything together to obtain $S(\{0,1,2,3\}) \le \frac{5}{3}$.

5.2 Design decisions

Rational function computation. The moment identities involve rational expressions simplified under the side conditions $z_1 \neq z_2$, $z_1 \neq z_3$, $z_2 \neq z_3$ and the root relations. The `field` tactic in mathlib, which clears denominators and reduces to polynomial equations, handles these cleanly.

C*-algebra norms. The self-inversive lemmas use properties specific to $\mathbb{C}$ as a C*-algebra, in particular $\|z^*z\| = \|z\|^2$. Mathlib's `CStarRing` typeclass provides this uniformly, and the proof of $\|\mathrm{lc}(P)\| = \|P(0)\|$ uses $\mathrm{lc}(P)^* \cdot \mathrm{lc}(P) = P(0)^* \cdot P(0)$.

Algebraic over analytic. The proof that Q has roots in the open disk uses only elementary inequalities (triangle inequality and $|\psi| \leq \frac{1}{2}$) rather than general complex analysis. The Blaschke estimate is the only place where root factorization is needed.

Compilation. The project is configured via Lake and depends on `mathlib`. It compiles successfully and the proof of the main theorem `Sidon3` can be inspected directly.

6 Further Questions

The exact value of the Sidon constant is now known for a handful of sets: all sets of size ≤ 3 [2], $\{0, 1, 2, 3\}$ (this paper), and $\{0, 1, 2, 3, 4\}$ [1] (value 2). Several directions remain open.

1. **Four-element sets.** Can the Sidon constant of an arbitrary four-element set be computed? The method introduced here relies on the fact that the cubic $X^3 - \psi X^2 + \psi X - \xi$ has all roots on the unit circle. For larger sets, one needs higher-degree self-inversive polynomials with all roots unimodular and carefully tuned Vieta coefficients.

2. **Real vs. complex unconditionality.** For $\{0, 1, 2, 3\}$ in $C(\mathbb{T})$, the real and complex unconditionality constants coincide (both equal $\frac{5}{3}$). This is also true for all three-element sets [2]. Does there exist any subset of $\mathbb{Z}$ for which they differ in $C(\mathbb{T})$? The question is open even for $L^p(\mathbb{T})$ with $p \neq 2$, and in particular for $\{0, 1, 2, 3\}$ in L^p when p is not a small even integer [3].

3. **Sets with Sidon constant close to 1.** The three-element result shows that one can achieve Sidon constants arbitrarily close to 1 by taking well-chosen triples with large $n = \max \frac{|\lambda_i - \lambda_j|}{\gcd}$. For four-element sets, the minimum possible Sidon constant is unknown.

4. **Connection to Hadamard matrices.** The bound $S(\Lambda) \leq \sqrt{|\Lambda| - 1}$ is sharp only when a circulant complex Hadamard matrix exists of appropriate size. This connects the Sidon constant problem to the existence theory of biunimodular sequences [5]. Our result shows that for $n = 3$, the extremal configuration is *not* of Hadamard type.

5. **Mechanization of the lower bound.** The present formalization covers only the upper bound. A complete formal verification of the Main Theorem would require also formalizing the lower bound, i.e., the verification that Neuwirth's extremal polynomials indeed have supremum norm $\frac{3}{5}$.

References

[1] H. S. Shapiro, "Extremal problems for polynomials and power series," Master's thesis, 1951.

[2] S. Neuwirth, “The Sidon constant of sets with three elements.” [Online]. Available: https://arxiv.org/abs/math/0102145

[3] S. Neuwirth, “On the (Fourier analytic) Sidon constant of 0,1,2,3.” [Online]. Available: https://arxiv.org/abs/2603.28229

[4] A. Cohn, “Über die Anzahl der Wurzeln einer algebraischen Gleichung in einem Kreise,” *Mathematische Zeitschrift*, vol. 14, no. 1, pp. 110–148, 1922.

[5] G. Björck and B. Saffari, “New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries,” *C. R. Acad. Sci. Paris Sér. I Math.*, vol. 320, pp. 319–324, 1995.