AIRR.SCIENCE · ARR-2026-5G15HR2KWY9RP8T2 v1 [Mathematics] 28 Nov 2026

Asymptotic Cohen–Macaulay Type Explosion, Sharp Four-Generator Bounds, and Base-d Hypercube Monomial Curves for Shifted Numerical Semigroups

Lluis Eriksson*

AIRR.SCIENCE Independent Research Collective (`AIRR-FOUNDER-1.0`)

November 28, 2026

Abstract

For any finite shift set $A = \{a_1 < \cdots < a_k = c\} \subset \mathbb{Z}_{>0}$ with $\gcd(A) = 1$, consider the shifted numerical semigroup family $M_n(A) = \langle n, n+a_1, \ldots, n+a_k\rangle$. While Vu (2014) established that the Betti numbers—and hence the Cohen–Macaulay type $t(M_n(A)) = |\operatorname{PF}(M_n(A))|$—become eventually c-periodic in n, the sharp dependence of the asymptotic type on the span c and embedding dimension $e = |A|+1$ has remained open. We establish a four-part theory resolving both universal bounds and asymptotic type explosion:

1. **Universal Decomposition, Zero-Sum Stabilization, Quadratic Ceiling, and Rao-Socle Duality (Theorem 2.1):** For every shift set A of span $c \geq 2$, a zero-sum reduction in $\mathbb{Z}/c\mathbb{Z}$ proves that minimal representations in $\langle A\rangle$ use at most $c-1$ summands $< c$, forcing $L_A(x+c) = L_A(x)+1$ for all $x \geq c^2 - 3c + 2$ (matching the exact Vu periodicity threshold $N_0(c)$ of Theorem 3.1(a)). For $n \gg 0$, $\operatorname{PF}(M_n(A))$ decomposes into the n-independent lower defect band $\operatorname{Peak}(A)$—in bijection with the 2D Rao-module socle of the projective monomial curve $C_A \subset \mathbb{P}^k$—and a c-periodic upper band obeying the universal ceiling $|\operatorname{PF}_{\text{upper}}(A, r)| \leq c$. Consequently, for every $c \geq 3$, $|\operatorname{Peak}(A)| \leq c^2 - 3c + 1$ and $t(M_n(A)) \leq (c-1)^2$ universally (while for $c = 2$, $A = \{1, 2\}$ has $|\operatorname{Peak}| = 0$ and $t(M_n) \in \{1, 2\}$), and the graded involution $\Phi(p, x) = (p, pc - x)$ proves $|\operatorname{Peak}(A)| = |\operatorname{Peak}(\widetilde{A})|$ identically.
2. **Sharp Four-Generator Structure (Theorem 3.1):** For the generalized Macaulay–Bresinsky family $A = \{1, c-1, c\}$ ($c \geq 4$), we prove the exact periodicity threshold $N_0(c) = (c-2)(c-1) = c^2 - 3c + 2$ and exact periodic type $(2c-3, 2c-4, 2c-5)$. For arbitrary $A = \{1, b, c\}$ ($1 < b < c$), an explicit homogenized syzygy identity proves that every peak satisfies $1 \leq r(x) + u(x) \leq m_1(x) - 1 \leq b - 2 \leq c - 3$, and for $b = c - 2$ the peak count drops sharply by half to $\lfloor (c-4)/2 \rfloor$.
3. **Base-d Hypercube Monomial Curves and Unbounded Type Explosion (Theorem 4.1):** For the m-dimensional base-d binary hypercube shift set $A_{m,d} = \bigoplus_{j=0}^{m-1} \{0, d^j\} \setminus \{0\}$ ($m \geq 2, d \geq 3$, span $c = (d^m - 1)/(d-1)$, embedding dimension $e = 2^m$), we prove exact zero-gap interval filling, exact global length, exact peak cardinality $|\operatorname{Peak}(A_{m,d})| = (d-2)c + 1 - (d-1)^m$, and exact full-period upper-band counts for all residues r mod c. At $n \equiv 1 \pmod{c}$ ($n \geq dc$), $A_{m,d}$ simultaneously saturates the upper-band ceiling $|\operatorname{PF}_{\text{upper}}| = c$, yielding the exact discrete cube-shell volume law

$$t\big(M_n(A_{m,d})\big) = d^m - (d-1)^m \qquad (n \equiv 1 \bmod c),$$
$$t\big(M_n(A_{m,d})\big) = d^m - (d-1)^m - 1 \qquad (n \equiv 0 \bmod c).$$

Hence $A_{3,d}$ ($e = 8$) strictly shatters the 4-generator ceiling $2c - 3$ for every $d \geq 5$ (first at $A_{3,5}$: $c = 31, t = 61 > 59$; exceeding $2c$ at $A_{3,6}$: $c = 43, t = 91 > 86$), fixed embedding dimension $e = 2^m$ attains asymptotic slope $\lim_{d\to\infty} t(M_n)/c = m = \log_2(e)$, and the coupled diagonal $A_{d,d}$ achieves $t(M_n)/c > (d-1)/2 = \Omega(\ln c / \ln\ln c) \to \infty$, refuting every universal linear bound $t(M_n(A)) \leq Kc$.

*Independent Researcher, Editor-in-Chief of AIRR.SCIENCE. Correspondence: editor@airr.science.

4. **Exact Frobenius Number, Closed-Form Genus, and Universal Wilf Positivity (Theorem 5.1):** For every $m \geq 2$, $d \geq 3$, and $n \geq dc$, we determine the exact n-Apéry set, the exact Frobenius number $F(M_n) = \lceil (n-1)/c \rceil n - 1$, and the exact closed-form genus $g(M_n)$, proving strict Wilf positivity $2^m n(M_n) > F(M_n) + 1$ unconditionally across all (m, d, n).

Core algebraic pillars (Table 1) are machine-checked in standalone Lean 4.36.0 (`ShiftedSemigroupCore.lean`, 41 declarations, zero `sorry`, zero external dependencies) and corroborated by exact zero-float integer verification across 2,004 shift sets, 1,952 four-generator pairs (8,904 peaks), 3,906 coprime triples, 42 hypercube families, and 404 full-period Dijkstra Apéry computations with zero discrepancies.

Keywords: shifted numerical semigroups, Cohen–Macaulay type, pseudo-Frobenius numbers, projective monomial curves, Rao module socle, Wilf's conjecture, base-d hypercube, Lean 4.
MSC 2020: 20M14, 13H10, 13D02, 14H45, 05A15.

1 Introduction

A numerical semigroup $S \subseteq \mathbb{N} = \{0, 1, 2, \dots\}$ is an additive submonoid with finite complement $\mathbb{N} \setminus S$. Its fundamental algebraic invariants—multiplicity $m(S) = \min(S \setminus \{0\})$, embedding dimension $e(S)$, Frobenius number $F(S) = \max(\mathbb{Z} \setminus S)$, genus $g(S) = |\mathbb{N} \setminus S|$, pseudo-Frobenius set

$$\mathrm{PF}(S) := \{f \in \mathbb{Z} \setminus S : f + s \in S \text{ for all } s \in S \setminus \{0\}\},$$

and Cohen–Macaulay type $t(S) := |\mathrm{PF}(S)|$—govern the homological invariants of the one-dimensional semigroup ring $\Bbbk[S] = \Bbbk[t^s : s \in S]$ [7]. While Herzog [4] proved that every 3-generated numerical semigroup satisfies $t(S) \leq 2$, Bresinsky [1, 2] demonstrated that $t(S)$ is already unbounded in embedding dimension $e(S) = 4$.

Following Herzog and Stamate [6], Vu [11], Stamate [9], Herzog–Hibi–Stamate [5], and the recent study of nearly Gorenstein and almost symmetric properties by Stamate and Strazzanti [10], a major modern program investigates *shifted numerical semigroups*

$$M_n(A) := \langle n,\ n + a_1,\ n + a_2,\ \dots,\ n + a_k \rangle,$$

associated with a fixed finite shift set $A = \{a_1 < a_2 < \cdots < a_k = c\} \subset \mathbb{Z}_{>0}$ of *span* $c := \max(A)$ with $\gcd(A) = 1$, as the shift parameter $n \to \infty$. Vu [11] resolved the Herzog–Srinivasan conjecture by proving that the graded Betti numbers of the defining toric ideal of $M_n(A)$ become eventually periodic in n of period c. In particular, the Cohen–Macaulay type $t(M_n(A))$ stabilizes to a c-periodic function of n mod c that depends solely on A.

This periodicity raises a sharp quantitative frontier question: *as a function of the span $c = \max(A)$ and the embedding dimension $e = |A| + 1$, how large can the asymptotic Cohen–Macaulay type $t(M_n(A))$ become?*

In embedding dimension $e = 4$ ($|A| = 3$), exhaustive computation through $c \leq 31$ (3,906 coprime triples) and across all 1,952 pairs $A = \{1, b, c\}$ with $1 < b < c < 65$ reveals a rigid linear ceiling $t(M_n(A)) \leq 2c - 3$, uniquely attained by the shifted Macaulay–Bresinsky curve $A = \{1, c-1, c\}$ at $n \equiv 1 \pmod{c}$. Even across all 2,004 non-empty coprime subsets $A \subseteq \{1, \dots, c\}$ for $3 \leq c \leq 11$, no subset exceeds $t(M_n(A)) = 2c-3$. One might therefore be tempted to conjecture a universal linear bound $t(M_n(A)) \leq 2c - 3$ (or $O(c)$) across all shift sets A.

The central discovery of this work is that *every universal linear bound $t(M_n(A)) \leq Kc$ fails dramatically*, via a remarkably transparent family of projective monomial curves: the *m-dimensional base-d binary hypercube shift sets*

$$A_{m,d} := \left\{ \sum_{j=0}^{m-1} \varepsilon_j d^j \ :\ \varepsilon \in \{0,1\}^m \setminus \{\mathbf{0}\} \right\} = \bigoplus_{j=0}^{m-1} \{0, d^j\} \setminus \{0\},$$

having embedding dimension $e = 2^m$ and span $c = \frac{d^m-1}{d-1}$. At $m = 2$, $A_{2,d} = \{1, d, d+1\} = \{1, c-1, c\}$ recovers the classical Macaulay–Bresinsky shifted family. For general $m \geq 2$ and $d \geq 3$, base-d carry geometry yields an exact piecewise-closed global length function $L_{A_{m,d}}(x)$, an exact peak cardinality $|\operatorname{Peak}(A_{m,d})| = (d-2)c+1-(d-1)^m$, exact full-period upper-band counts for all $r \in \{0, \ldots, c-1\}$, and at $n \equiv 1 \pmod{c}$ $(n \geq dc)$ the exact discrete cube-shell volume law

$$t\big(M_n(A_{m,d})\big) = d^m - (d-1)^m.$$

Thus $A_{3,5}$ $(e = 8, c = 31)$ already breaks the 4-generator ceiling with $t = 61 > 59 = 2c - 3$, $A_{3,6}$ $(c = 43)$ breaks $2c$ with $t = 91 > 86$, fixed embedding dimension $e = 2^m$ achieves $\lim_{d\to\infty} t/c = m = \log_2(e)$, and the coupled diagonal $A_{d,d}$ achieves $t(M_n)/c = \Omega(\ln c/\ln\ln c) \to \infty$ (with optimal scaling $d = \lceil m \ln m \rceil$ attaining sharp leading constant 1). Complementing this unbounded growth, we prove via a zero-sum reduction in $\mathbb{Z}/c\mathbb{Z}$ that $t(M_n(A)) \leq (c-1)^2$ holds universally for every shift set A of span $c \geq 3$, with stabilization cutoff $c^2 - 3c + 2$ coinciding with the exact Vu periodicity threshold $N_0(c)$ of the Macaulay–Bresinsky family. Finally, we derive the exact n-Apéry set, Frobenius number, and closed-form genus of $M_n(A_{m,d})$, proving strict Wilf positivity [12, 3] for every $m \geq 2$, $d \geq 3$, and $n \geq dc$.

Organization and Verification Architecture

Section 2 proves Theorem 2.1 (universal asymptotic decomposition, zero-sum length stabilization, upper-band ceiling, quadratic type bound, and homogenized Rao-socle duality). Section 3 proves Theorem 3.1 (exact solution of the Macaulay–Bresinsky family, exact peak-residue ceiling for all $A = \{1, b, c\}$, and exact half-drop for $b = c - 2$). Section 4 proves Theorem 4.1 (complete exact analysis and unbounded type explosion of $A_{m,d}$). Section 5 proves Theorem 5.1 (exact Apéry set, Frobenius number, closed-form genus, and universal Wilf positivity). Section 6 documents the standalone Lean 4.36.0 formalization and exact integer verification audit, and Section 7 formulates two sharp open problems.

2 Universal Asymptotic Decomposition, Zero-Sum Stabilization, and Duality

Let $A = \{a_1 < \cdots < a_k = c\} \subset \mathbb{Z}_{>0}$ with $\gcd(A) = 1$, and write $A_0 := A \cup \{0\}$. Let $\langle A \rangle \subseteq \mathbb{N}$ be the numerical semigroup generated by A. For each $x \in \langle A \rangle$, define its *minimal representation length*

$$L_A(x) := \min\left\{p \in \mathbb{N} : x = \sum_{i=1}^{p} a^{(i)},\ a^{(i)} \in A\right\} \qquad (L_A(0) := 0),$$

with $L_A(x) := +\infty$ if $x \notin \langle A \rangle$. The *homogenized 2D affine semigroup* of the projective monomial curve $C_A \subset \mathbb{P}^k$ of degree c is

$$\widehat{S}(A) := \big\langle (1,0),\ (1,a) : a \in A \big\rangle = \big\{(p,x) \in \mathbb{N}^2 : x \in p \cdot A_0\big\} = \big\{(p,x) \in \mathbb{N}^2 : L_A(x) \leq p\big\}.$$

Define the *lower defect band* (peak set) of A by

$$\operatorname{Peak}(A) := \big\{x \in \langle A \rangle \setminus \{0\} : L_A(x+a) \leq L_A(x) \text{ for all } a \in A\big\}.$$

Equivalently, $x \in \operatorname{Peak}(A)$ with $p = L_A(x)$ if and only if $w = (p-1, x) \notin \widehat{S}(A)$ while $w + (1,0) \in \widehat{S}(A)$ and $w + (1,a) \in \widehat{S}(A)$ for all $a \in A$; that is, $(L_A(x) - 1, x)$ ranges over the homogeneous 2D pseudo-Frobenius elements of $\widehat{S}(A)$, which index a $\Bbbk$-basis of the Rao-module socle $\operatorname{Soc}_R(H^1_{\mathfrak{m}}(\Bbbk[C_A]))$.

Define also the *dual shift set*

$$\widetilde{A} := \{c - a : a \in A_0\} \setminus \{0\} = \{c\} \cup \{c - a : a \in A,\ a < c\},$$

and the c-Apéry set $\mathrm{Ap}(\langle A\rangle, c) := \{u \in \langle A\rangle : u - c \notin \langle A\rangle\}$, which contains exactly one representative in each residue class modulo c (so $|\,\mathrm{Ap}(\langle A\rangle, c)| = c$).

Theorem 2.1 (Universal Stabilization, Decomposition, Ceilings, and Duality)**.** *Let $A \subset \mathbb{Z}_{>0}$ be any finite shift set with $\max(A) = c \geq 2$ and $\gcd(A) = 1$.*

(a) ***Zero-Sum Length Stabilization:*** *Every minimal-length representation of any $x \in \langle A\rangle$ uses at most $c-1$ summands strictly smaller than c. Consequently, for every $x \in \langle A\rangle$ with $x \geq (c-2)(c-1) = c^2 - 3c + 2$,*

$$L_A(x + c) = L_A(x) + 1.$$

(b) ***Asymptotic Pseudo-Frobenius Decomposition and Upper-Band Ceiling:*** *Set $M_A := \max\big(\,\mathrm{Ap}(\langle A\rangle, c) \cup \{c^2 - 3c + 2\}\big)$ and $L_{\mathrm{ap}} := \max_{u \in \mathrm{Ap}(\langle A\rangle, c)} L_A(u)$. Whenever $n > M_A + cL_{\mathrm{ap}}$, the pseudo-Frobenius set $\mathrm{PF}(M_n(A))$ partitions disjointly as*

$$\mathrm{PF}\big(M_n(A)\big) = \mathrm{PF}_{\mathrm{lower}}(A, n) \;\sqcup\; \mathrm{PF}_{\mathrm{upper}}(A, n),$$

where

$$\mathrm{PF}_{\mathrm{lower}}(A, n) = \big\{(L_A(x) - 1)n + x : x \in \mathrm{Peak}(A)\big\}$$

has cardinality $|\,\mathrm{Peak}(A)|$ independent of n, and every element of $\mathrm{PF}_{\mathrm{upper}}(A, n)$ has the form $L_A(n + u - c)n + u - c$ for some $u \in \mathrm{Ap}(\langle A\rangle, c)$. In particular, $|\,\mathrm{PF}_{\mathrm{upper}}(A, n)|$ depends only on $r = n \bmod c$ and obeys the universal ceiling

$$1 \leq |\,\mathrm{PF}_{\mathrm{upper}}(A, r)| \leq |\,\mathrm{Ap}(\langle A\rangle, c)| = c \qquad (\forall r \in \{0, \ldots, c-1\}).$$

(c) ***Universal Quadratic Peak and Type Ceilings ($c \geq 3$):*** *Whenever $c \geq 3$, every peak satisfies $\mathrm{Peak}(A) \subseteq \{1, 2, \ldots, c^2 - 3c + 1\}$, whence*

$$|\,\mathrm{Peak}(A)| \leq c^2 - 3c + 1 \qquad \textit{and} \qquad t\big(M_n(A)\big) \leq (c-1)^2 \qquad (\forall n \gg 0).$$

(At $c = 2$, the unique shift set $A = \{1, 2\}$ satisfies $\mathrm{Peak}(A) = \emptyset$ and $t(M_n(A)) \in \{1, 2\}$ for all $n \geq 2$.)

(d) ***Exact Homogenized Rao-Socle Duality:*** *The map $\Phi(p, x) = (p, pc - x)$ is a graded monoid isomorphism $\widehat{S}(A) \xrightarrow{\sim} \widehat{S}(\widetilde{A})$ restricting to a bijection between the 2D Rao-socle peaks of $\widehat{S}(A)$ and $\widehat{S}(\widetilde{A})$. Hence $|\,\mathrm{Peak}(A)| = |\,\mathrm{Peak}(\widetilde{A})|$ identically.*

(e) ***Exact Asymptotic Frobenius Formula:*** *For all $n > M_A + cL_{\mathrm{ap}}$,*

$$F\big(M_n(A)\big) = \max_{u \in \mathrm{Ap}(\langle A\rangle, c)} \Big(L_A(n + u - c)\, n + u - c\Big).$$

Proof. **(a)** Let $x = \sum_{i=1}^{L} a^{(i)}$ ($a^{(i)} \in A$) be a minimal-length representation ($L = L_A(x)$), and let $b_1, \ldots, b_k$ list all summands strictly smaller than c. Suppose $k \geq c$. Consider the $c+1$ prefix sums $P_j := \sum_{i=1}^{j} b_i$ for $0 \leq j \leq c$. By the Pigeonhole Principle, there exist $0 \leq i < j \leq c$ with $P_i \equiv P_j \pmod{c}$, so the non-empty sub-sum $S := \sum_{t=i+1}^{j} b_t$ satisfies $S = mc$ for an integer $m \geq 1$. Since $b_t \leq c - 1$ for every t,

$$mc = \sum_{t=i+1}^{j} b_t \leq (j - i)(c - 1) < (j - i)c \implies m < j - i.$$

Replacing $b_{i+1}, \ldots, b_j$ by m copies of $c \in A$ yields a representation of x of length $L - (j-i) + m < L$, contradicting minimality. Hence $k \leq c - 1$ (formalized in Lean as `zero_sum_sublist_reduction`).

Now let $x \in \langle A \rangle$ satisfy $x \geq c^2 - 3c + 2 = (c-2)(c-1)$. Then $x + c \geq c^2 - 2c + 2 > (c-1)^2$ (`zero_sum_quadratic_cutoff`). In any minimal-length representation of $x + c$, the summands $< c$ contribute at most $(c-1)^2 < x + c$, so at least one summand equals c. Removing one copy of c represents x in length $L_A(x+c) - 1$, giving $L_A(x) \leq L_A(x+c) - 1$. Since $L_A(x+c) \leq L_A(x) + 1$ trivially, $L_A(x + c) = L_A(x) + 1$.

(b) & (e) Every element of $M_n(A)$ has the form $pn + y$ with $y \in \langle A \rangle$ and $p \geq L_A(y)$. Hence the n-Apéry element of $M_n(A)$ in residue class $s \in \{1, \ldots, n-1\}$ is

$$w_s = \min\big\{L_A(y)n + y : y \in \langle A \rangle,\ y \equiv s \pmod{n}\big\}.$$

Let $n > M_A + cL_{\mathrm{ap}}$ (note $M_A \geq F(\langle A \rangle) + c$ since $\max \mathrm{Ap}(\langle A \rangle, c) = F(\langle A \rangle) + c$, so every integer $\geq M_A$ belongs to $\langle A \rangle$). We verify the exact minimizer y for each $s \in \{1, \ldots, n-1\}$:

- If $s \in \langle A \rangle$ and $s \leq n - 1$, write $s = qc + u_0$ ($u_0 \in \mathrm{Ap}(\langle A \rangle, c), q \geq 0$), so $L_A(s) \leq q + L_A(u_0) \leq s/c + L_{\mathrm{ap}}$. For any $m \geq 1$, $y = s + mn$ has $L_A(y) \geq (s + mn)/c > s/c + L_{\mathrm{ap}} \geq L_A(s)$, so $L_A(s)n + s < L_A(y)n + y$. Thus $w_s = L_A(s)n + s$ for every $s \in \langle A \rangle \cap \{1, \ldots, n-1\}$.
- If $s \in \{1, \ldots, n-1\} \setminus \langle A \rangle$, then $s \leq F(\langle A \rangle) < M_A$, so $n + s > M_A$ lies in $\langle A \rangle$. Writing $n + s = qc + u_0$ ($u_0 \in \mathrm{Ap}(\langle A \rangle, c), q \geq 0$) gives $L_A(n + s) \leq q + L_A(u_0) \leq (n + s)/c + L_{\mathrm{ap}}$. For any $m \geq 2$, since $n > M_A + cL_{\mathrm{ap}} > cL_{\mathrm{ap}}$, we have

  $$L_A(mn + s) \geq \frac{mn + s}{c} = \frac{n + s}{c} + \frac{(m-1)n}{c} > \frac{n + s}{c} + L_{\mathrm{ap}} \geq L_A(n + s).$$

  Thus $w_s = L_A(n + s)n + (n + s)$.

Now $w_s - n \in \mathrm{PF}(M_n(A))$ if and only if $w_{(s+a) \bmod n} < w_s + n + a$ for all $a \in A$.

- *Case 1 (Lower band, $s \in \langle A \rangle$ and $s + c < n$):* For every $a \in A$, $s + a < n$ lies in $\langle A \rangle$, so $w_{s+a} = L_A(s+a)n + (s+a)$. The condition $w_{s+a} < w_s + n + a$ is equivalent to $L_A(s+a) \leq L_A(s)$ for all $a \in A$. By part (a), every $s \in \mathrm{Peak}(A)$ satisfies $s \leq c^2 - 3c + 1 < n - c$, so Case 1 yields precisely $\mathrm{PF}_{\mathrm{lower}}(A, n) = \{(L_A(x) - 1)n + x : x \in \mathrm{Peak}(A)\}$.
- *Case 2 (Upper band, $s \in [n - c, n - 1]$ or $s \in [1, n - 1] \setminus \langle A \rangle$):* Unify both subcases by setting $z := s - n \in \{-c, \ldots, -1\}$ when $s \in [n-c, n-1]$, and $z := s \in \mathbb{Z}_{>0} \setminus \langle A \rangle$ when $s \notin \langle A \rangle$. In both subcases, $n + z \geq n - c > M_A$ lies in $\langle A \rangle$, $w_s = L_A(n+z)n + (n+z)$, and $w_s - n = L_A(n+z)n + z$. Testing maximality against the top generator $n + c$ uses $(s + c) \bmod n = z + c \geq 0$:

  (i) If $z + c = 0$ (so $s = n - c$), then $w_0 = 0 < w_s + n + c$ holds automatically, and $u := z + c = 0 \in \mathrm{Ap}(\langle A \rangle, c)$.

  (ii) If $z + c > 0$ and $z + c \notin \langle A \rangle$, then $w_{z+c} = L_A(n+z+c)n + (n+z+c) = (L_A(n+z)+1)n + (n + z + c) = w_s + n + c$ by part (a), so $w_s + (n + c) \in \mathrm{Ap}(M_n(A), n)$ and $w_s - n \notin \mathrm{PF}(M_n(A))$.

  (iii) If $z + c \in \langle A \rangle \setminus \{0\}$, then $w_{z+c} = L_A(z+c)n + (z+c) < w_s + n + c$ (since $L_A(z+c) \leq L_A(n+z)$ for $n > M_A + cL_{\mathrm{ap}}$). Crucially, $z = (z + c) - c$ is either negative or lies outside $\langle A \rangle$; in either case $z \notin \langle A \rangle$ while $z + c \in \langle A \rangle$, which is the exact definition of $u := z + c \in \mathrm{Ap}(\langle A \rangle, c)$.

Therefore every element of $\mathrm{PF}_{\mathrm{upper}}(A, n)$ is indexed by a distinct element $u = z + c \in \mathrm{Ap}(\langle A \rangle, c)$, giving $|\,\mathrm{PF}_{\mathrm{upper}}(A, n)| \leq |\,\mathrm{Ap}(\langle A \rangle, c)| = c$. Moreover, for each $u \in \mathrm{Ap}(\langle A \rangle, c)$ and $a \in A$, the maximality test against $n+a$ depends only on $L_A(n+u-c+a) - L_A(n+u-c)$ when $u - c + a \notin \langle A \rangle$, which by part (a) is strictly c-periodic in n. To locate $F(M_n(A))$, let $u^* \in \mathrm{Ap}(\langle A \rangle, c)$ be the representative with $u^* \equiv c - 1 \pmod{c}$, so $u^* \geq c - 1$ and $n + u^* - c \geq n - 1$. Since $n > M_A + cL_{\mathrm{ap}}$ are integers, $n - 1 \geq M_A + cL_{\mathrm{ap}}$, whence $L_A(n + u^* - c) \geq (n-1)/c \geq M_A/c + L_{\mathrm{ap}}$. By contrast, every peak $x \in \mathrm{Peak}(A)$ satisfies $x \leq c^2 - 3c + 1 < M_A$, so writing $x = qc + u_0$ ($u_0 \in \mathrm{Ap}(\langle A \rangle, c)$) yields $L_A(x) \leq x/c + L_{\mathrm{ap}} < M_A/c + L_{\mathrm{ap}} \leq L_A(n + u^* - c)$, which forces $L_A(n + u^* - c) \geq L_A(x) + 1$ as integers. Since $w_{(u^*-c) \bmod n} - n = L_A(n + u^* - c)n + u^* - c \notin M_n(A)$ and $x < M_A < n < 2n - 1$,

$$F\big(M_n(A)\big) \geq L_A(n + u^* - c)\, n + u^* - c \geq (L_A(x) + 1)n - 1 > (L_A(x) - 1)n + x$$

for every $x \in \mathrm{Peak}(A)$. Hence $F(M_n(A)) \in \mathrm{PF}_{\mathrm{upper}}(A,n)$, establishing part (e) and $|\mathrm{PF}_{\mathrm{upper}}(A,r)| \geq 1$.

(c) For $c \geq 3$, part (a) implies that no $x \geq c^2 - 3c + 2 \geq 2$ can satisfy $L_A(x+c) \leq L_A(x)$. Hence $\mathrm{Peak}(A) \subseteq \{1, \ldots, c^2 - 3c + 1\}$ (a non-negative upper endpoint since $c^2 - 3c + 1 \geq 1$ for $c \geq 3$), giving $|\mathrm{Peak}(A)| \leq c^2 - 3c + 1$, and by part (b), $t(M_n(A)) \leq (c^2 - 3c + 1) + c = (c-1)^2$. At $c = 2$, $A = \{1, 2\}$ has $L_A(x) = \lceil x/2 \rceil$ for all $x \geq 0$, so $L_A(x+2) = L_A(x) + 1$ for all $x \geq 0$, whence $\mathrm{Peak}(A) = \emptyset$ and $t(M_n(A)) \leq c = 2$ by part (b).

(d) Every $(p,x) \in \widehat{S}(A)$ satisfies $0 \leq x \leq pc$ (`homogMem_le_mul`). The linear involution $\Phi(p,x) = (p, pc - x)$ maps $(1,0) \leftrightarrow (1,c)$ and $(1,a) \leftrightarrow (1, c-a)$ for $a \in A \setminus \{c\}$, inducing a graded monoid isomorphism $\widehat{S}(A) \xrightarrow{\sim} \widehat{S}(\widetilde{A})$ (`homogMem_dual_iff`). Consequently $(p,x) \notin \widehat{S}(A)$ with $(p+1, x), (p+1, x+a) \in \widehat{S}(A)$ $(\forall a \in A)$ holds if and only if the same holds for $(p, pc-x)$ in $\widehat{S}(\widetilde{A})$ (`isPeak2D_dual_iff`), proving $|\mathrm{Peak}(A)| = |\mathrm{Peak}(\widetilde{A})|$. □

Remark 2.2. Theorem 2.1(b) gives a clean conceptual derivation of the periodicity of $t(M_n(A))$ and the Frobenius number established in [11, 9, 10], while adding the sharp universal upper-band ceiling $|\mathrm{PF}_{\mathrm{upper}}(A,r)| \leq c$, the universal quadratic type ceiling $(c-1)^2$, the sharp zero-sum stabilization cutoff $c^2 - 3c + 2$, and the exact peak duality $|\mathrm{Peak}(A)| = |\mathrm{Peak}(\widetilde{A})|$.

3 Sharp Four-Generator Structure and the Macaulay–Bresinsky Ceiling

In embedding dimension $e = 4$ ($|A| = 3$), the shift set $A = \{1, c-1, c\}$ $(c \geq 4)$ defines the projective Macaulay–Bresinsky curve $C_{\{1,c-1,c\}} \subset \mathbb{P}^3$ of degree c. We solve this family completely, establish a sharp factor-of-2 drop at $b = c - 2$, and prove a universal homogenized peak-residue ceiling for all $A = \{1, b, c\}$ $(1 < b < c)$.

Theorem 3.1 (Exact Four-Generator Structure)**.** *Let $c \geq 4$.*

(a) ***Macaulay–Bresinsky Family*** *$A = \{1, c-1, c\}$: Every $x \in \mathrm{Peak}(1, c-1, c)$ has uniform length $c-2$, with*

$$\mathrm{Peak}(1, c-1, c) = \big\{(c-2) + j(c-1) : 0 \leq j \leq c-4\big\}, \qquad |\mathrm{Peak}(1, c-1, c)| = c - 3.$$

The exact Vu periodicity threshold of $t(M_n(1, c-1, c))$ is $N_0(c) = (c-2)(c-1) = c^2 - 3c + 2$ (sharp to the exact integer 1 as the periodicity threshold, and matching the universal zero-sum cutoff of Theorem 2.1(a)): $t(N_0(c) - 1) \neq t(N_0(c) - 1 + c)$, while for all $n \geq (c-2)(c-1)$,

$$t\big(M_n(1, c-1, c)\big) = \begin{cases} 2c - 3 & (n \equiv 1 \bmod c), \\ 2c - 4 & (n \equiv 0 \bmod c), \\ 2c - 5 & (2 \leq n \bmod c \leq c - 1). \end{cases}$$

(b) ***Universal Peak-Residue Ceiling for*** *$A = \{1, b, c\}$ $(1 < b < c)$: For any $x \in \mathrm{Peak}(1, b, c)$, let $x = m_1 \cdot 1 + m_b \cdot b + m_c \cdot c$ be any minimal-length representation ($m_1 + m_b + m_c = L_A(x) =: p$), and write $x + b = r(x) + s(x)c$ $(0 \leq r(x) < c)$ and $x + c = u(x) + v(x)b$ $(0 \leq u(x) < b)$. Then $r(x) < b$, $s(x) > m_c$, $v(x) > m_b$, and*

$$1 \leq r(x) + u(x) \leq m_1 - 1 \leq b - 2 \leq c - 3.$$

(c) ***Exact Factor-of-Two Phase Drop at*** *$b = c - 2$ $(c \geq 5)$:*

$$\mathrm{Peak}(1, c-2, c) = \big\{(c-3) + j(c-2) : 0 \leq j \leq \lfloor (c-6)/2 \rfloor\big\}, \qquad |\mathrm{Peak}(1, c-2, c)| = \left\lfloor \frac{c-4}{2} \right\rfloor,$$

with strictly decreasing peak lengths $L_A((c-3) + j(c-2)) = c - 3 - j$.

Proof. **(a)** Observe that $A = \{1, c-1, c\} = \{0,1\} \oplus \{0, c-1\} \setminus \{0\} = A_{2,c-1}$, the $m = 2$, $d = c-1$ instance of Theorem 4.1. By Theorem 4.1(a)–(b), $L_A(x) = \max(x_0, x_1)$ for $0 \le x < (c-1)^2$ ($x = x_0 + x_1(c-1)$) and $\lceil x/c \rceil$ for $x \ge (c-1)^2$, while $\mathrm{Peak}(A) = \{x \le (c-3)c : \max(x_0, x_1) = c-2\}$. Since $(c-3)c = (c-3) + (c-3)(c-1)$ has both base-$(c-1)$ digits equal to $c-3$, the peaks are precisely the integers with $x_0 = c-2$ and $0 \le x_1 \le c-4$, i.e., $x = (c-2) + j(c-1)$ for $0 \le j \le c-4$ (cardinality $c-3$, uniform length $c-2$).

For the periodic upper band, Theorem 4.1(c) gives $|\mathrm{PF}_{\mathrm{upper}}(A,1)| = c$ and $|\mathrm{PF}_{\mathrm{upper}}(A,0)| = c-1$. For $2 \le r \le c-1$, we check the condition $(u + A) \cap (c-r, c) = \emptyset$ on $u \in \{0, \dots, c-r\}$:

- $u = c-r$ fails via $a = 1$ since $(c-r) + 1 \in (c-r, c)$;
- $u = 0$ fails via $a = c-1$ since $0 + (c-1) = c-1 \in (c-r, c)$;
- every $u \in \{1, \dots, c-r-1\}$ survives since $u + 1 \le c-r$, $u + (c-1) \ge c$, and $u + c > c$.

Hence $|\mathrm{PF}_{\mathrm{upper}}(A,r)| = (r-1) + (c-r-1) = c-2$, giving $t(M_n) = (c-3) + (c-2) = 2c-5$ for all $2 \le r \le c-1$.

To establish the exact threshold $N_0(c) = (c-2)(c-1) = c^2 - 3c + 2$, observe first that $L_A(x) = \lceil x/c \rceil$ holds for EVERY $x \ge (c-3)(c-1) = c^2 - 4c + 3$: indeed, on $[(c-3)(c-1), (c-3)c]$ every integer has base-$(c-1)$ digits $x_1 = c-3$ and $0 \le x_0 \le c-3$ so $L_A(x) = c-3 = \lceil x/c \rceil$; on $[(c-3)c+1, (c-1)^2 - 1] = [(c-3)c+1, (c-2)c]$ every integer has $\max(x_0, x_1) = c-2 = \lceil x/c \rceil$; and on $[(c-1)^2, \infty)$ Theorem 4.1(a) applies. Hence for all $n \ge N_0(c) = c^2 - 3c + 2$, every $x \in [0, n-1]$ and $q \ge 1$ satisfy $x + qn \ge n > c^2 - 4c + 3$, so $L_A(x + qn) = \lceil (x + qn)/c \rceil \ge c - 2 \ge L_A(x)$ (for $x < (c-1)^2$) and $L_A(x + qn) \ge \lceil x/c \rceil = L_A(x)$ (for $x \ge (c-1)^2$), certifying $\mathrm{Ap}(M_n, n) = \{L_A(x)n + x : 0 \le x \le n-1\}$.

- For $n \ge N_0(c) + 1 = c^2 - 3c + 3$: all $c-3$ peaks satisfy $x \le x_{\max} = c^2 - 4c + 2 < n - c$ (strictly in the lower band), and all c upper-band indices $x_u = n + u - c \ge c^2 - 4c + 3$ satisfy $L_A(x_u) = \lceil x_u/c \rceil \ge c - 3$. Moreover, any wrap-around $v = u + a - c \in \{1, \dots, c-1\}$ satisfies $L_A(v) \le c - 2 < (c-3) + 2 \le L_A(x_u) + 2$, so Theorem 4.1(c) applies verbatim and yields the periodic type $(2c-3, 2c-4, 2c-5)$.
- At the boundary $n = N_0(c) = c^2 - 3c + 2 \equiv 2 \pmod{c}$ ($r = 2$, $K = c-3$): the first $c-4$ peaks ($0 \le j \le c-5$) lie strictly in $\{1, \dots, n-c-1\}$, while the last peak $x_{\max} = c^2 - 4c + 2$ equals $x_0 = n - c$ ($u = 0$), with $L_A(x_0) = c-2$. For $1 \le u \le c-1$, $x_u \ge c^2 - 4c + 3$ obeys $L_A(x_u) = \lceil ((c-4)c + 2 + u)/c \rceil$, giving $L_A(x_u) = c-3$ for $1 \le u \le c-2$ and $L_A(x_{c-1}) = c-2$. Checking maximality on $\{x_0, \dots, x_{c-1}\}$: $u = 0$ survives ($L_A(x_0 + 1) = c-3 \le c-2$, $L_A(x_0 + c - 1) = L_A(x_{c-1}) = c-2$, and $x_0 + c = n \equiv 0$); $u = c-1$ survives (every $a \in A$ wraps to $v \in \{0, \dots, c-1\}$ with $L_A(v) \le c-2 < (c-2)+2$, since $L_A(c-1) = 1$); every $1 \le u \le c-3$ survives ($L_A(x_{u+1}) = c-3$ and $a \in \{c-1, c\}$ wraps to $v \le c-3 < (c-3)+2$); and $u = c-2$ is eliminated by $a = 1$ ($L_A(x_{c-1}) = c-2 > c-3$). Thus $t(N_0(c)) = (c-4)+1+1+(c-3) = 2c-5$, matching the periodic value for $r = 2$.
- At $n = N_0(c) - 1 = c^2 - 3c + 1 \equiv 1 \pmod{c}$: $x_{\max} = c^2 - 4c + 2 = n - c + 1 = x_1$ ($u = 1$), leaving only $c-4$ lower-band peaks in $\{1, \dots, n-c-1\}$, while $x_0 = n - c = c^2 - 4c + 1 = (c-3) + (c-4)(c-1)$ has $L_A(x_0) = c-3 < c-2 = L_A(x_0 + 1)$, eliminating $u = 0$. Hence $t(N_0(c) - 1) \le (c-4) + (c-1) = 2c-5 < 2c-3 = t(N_0(c) - 1 + c)$.

(b) Let $w = (p-1, x) \notin \widehat{S}(1, b, c)$ with generators $v_0 = (1,0), v_1 = (1,1), v_b = (1,b), v_c = (1,c)$. Since $x = m_1 \cdot 1 + m_b \cdot b + m_c \cdot c$ has minimal length $p = L_A(x)$, we have $m_1 \le b-1$ (otherwise replace $b \cdot 1$ by b) and $w + v_0 = m_1 v_1 + m_b v_b + m_c v_c$. Since $L_A(x + b) \le p$, every optimal representation of $x + b$ uses zero copies of b (otherwise removing one b would give $L_A(x) \le p - 1$), so it is the greedy $\{1, c\}$-representation $x + b = r + sc$ ($0 \le r < c$), yielding $w + v_b = \beta_0 v_0 + r v_1 + s v_c$ with $\beta_0 = p - r - s \ge 0$. Moreover $r < b$ (if $r \ge b$, then $x = (r-b) + sc$ would give $L_A(x) \le r - b + s < r + s = L_A(x + b) \le L_A(x)$, a contradiction). Symmetrically, $w + v_c = \gamma_0 v_0 + u v_1 + v v_b$ with $0 \le u < b$ and $\gamma_0 = p - u - v \ge 0$.

Comparing second coordinates of $w+v_0$ and $w+v_b$: if $s \le m_c$, then $m_1+(m_b+1)b+(m_c-s)c = r < b$, impossible since the left-hand side is $\ge b$; hence $s > m_c$. Symmetrically, if $v \le m_b$, then $m_1 + (m_b - v)b + (m_c + 1)c = u < b < c$, impossible; hence $v > m_b$. Forming the exact linear combination $(w + v_b) + (w + v_c) - (w + v_0)$ in $\mathbb{Z}^2$ yields

$$w = (\beta_0 + \gamma_0 + 1)v_0 + (r + u - m_1)v_1 + (v - m_b - 1)v_b + (s - m_c - 1)v_c.$$

Since $v - m_b - 1 \ge 0$ and $s - m_c - 1 \ge 0$, assuming $r + u \ge m_1$ makes all four coefficients non-negative and forces $w \in \widehat{S}(1, b, c)$, a contradiction. Therefore $r+u+1 \le m_1 \le b-1 \le c-2$, whence $r+u \le b-2 \le c-3$ (formalized in Lean as `four_gen_peak_residue_bound`). Finally, if $r = u = 0$, then $x + b = sc$ and $x + c = vb$, so $(v+1)b = (s+1)c$ with $s \ge 1, v \ge 2$. If $g := \gcd(b, c) > 1$, then $g \mid (sc - b) = x$, so $g \nmid (x + 1)$, contradicting $x + 1 \in \langle b, c\rangle \subseteq g\mathbb{Z}$ (forced by $L_A(x + 1) \le L_A(x)$). Thus $\gcd(b, c) = 1$, giving $s = mb - 1$ and $v = mc - 1$ for some $m \ge 1$, so $x = (mb - 2)c + (c - b)$ satisfies $L_A(x) \le (mb - 2) + (c - b) = mc - 1 - (m - 1)(c - b) - 1 < mc - 1 = v = L_A(x + c)$, a contradiction. Hence $r + u \ge 1$.

(c) Let $b = c-2$ ($c \ge 5$). For $0 \le j \le \lfloor (c-6)/2 \rfloor$, set $x_j := (c-3)+j(c-2) = jc+(c-3-2j) = (j+1)b-1$. In any representation $x_j = m_1 \cdot 1+m_b b+m_c c$, we have $m_b+m_c \le j$ (since $(j+1)b > x_j$); moreover, replacing $b+2 \cdot 1$ by c strictly shortens length by 2, so any minimal representation with $m_1 \ge 2$ must have $m_b = 0$. Since $c - 3 - 2j \ge 3$ for $j \le \lfloor (c - 6)/2 \rfloor$, the unique minimal representation of x_j is $m_c = j, m_b = 0, m_1 = c - 3 - 2j$, giving $L_A(x_j) = c - 3 - j$. Checking the three shifts directly: $x_j + 1 = (j + 1)b$ has $L_A \le j + 1 \le c - 3 - j$; $x_j + b = (j + 1)c + (c - 5 - 2j)$ has $L_A \le c-4-j < L_A(x_j)$; and $x_j+c = (j+2)b+1$ has $L_A \le j+3 \le c-3-j$ (since $2j \le c-6$). Thus every $x_j \in \mathrm{Peak}(1, c - 2, c)$.

Conversely, let $x \in \mathrm{Peak}(1, c - 2, c)$ have minimal representation $x = m_1 \cdot 1 + m_b b + m_c c$. By part (b), $m_1 \ge r+u+1 \ge 2$; since replacing $b+2\cdot 1$ by c reduces length by 2, this forces $m_b = 0$, so $x = m_c c+m_1$ ($2 \le m_1 \le b-1$) and $L_A(x) = m_c+m_1$. We claim that $2m_c+m_1 \le b-1$. Suppose to the contrary that $2m_c + m_1 \ge b$, and set $k := \lceil (b - m_1)/2 \rceil$. Since $1 \le b - m_1 \le 2m_c$, we have $1 \le k \le m_c$ and $t := m_1 + 2k - b \in \{0, 1\}$. Rewriting $kc + m_1 = k(b + 2) + m_1 = (k + 1)b + t$ produces the valid representation

$$x = (m_c - k)c + (k + 1)b + t \cdot 1 \quad \text{of length} \quad (m_c - k) + (k + 1) + t = m_c + 1 + t.$$

If $m_1 \ge 3$ or $t = 0$, then $m_c + 1 + t < m_c + m_1 = L_A(x)$, contradicting minimality. In the sole remaining case $m_1 = 2$ and $t = 1$ (b odd, $2k = b - 1$, $2m_c \ge b - 1$), we have $L_A(x) = m_c + 2$ and

$$x + c = (m_c + 1)(b + 2) + 2 = (m_c + 2)b + (2m_c + 4 - b) \ge (m_c + 2)b + 3.$$

Hence the optimal $\{1, b\}$-representation $x + c = vb + u$ ($0 \le u < b$) has either $v \ge m_c + 3$ (so $L_A(x + c) = v + u \ge m_c + 3$) or $v = m_c + 2$ with $u \ge 3$ (so $L_A(x + c) \ge m_c + 5$); both contradict $L_A(x + c) \le L_A(x) = m_c + 2$. Thus $2m_c + m_1 \le b - 1$ always holds.

On the other hand, writing $x + c = (m_c + 1)b + (2m_c + m_1 + 2)$, if $2m_c + m_1 + 2 < b$ then the greedy $\{1, b\}$-representation gives $L_A(x+c) = 3m_c + m_1 + 3 > m_c + m_1 = L_A(x)$, a contradiction; hence $2m_c + m_1 \in \{b-2, b-1\}$. If $2m_c + m_1 = b-2$, then $x+1 = m_c c+(m_1+1) = (m_c+1)b-1$ cannot lie in $\langle b, c\rangle$, because every element $\alpha b + \beta c \in \langle b, c\rangle$ with $\alpha + \beta \le m_c$ is $\le m_c c < x + 1$, whereas every element with $\alpha + \beta \ge m_c + 1$ is $\ge (m_c + 1)b = x + 2 > x + 1$, contradicting $L_A(x + 1) \le L_A(x)$. Therefore $2m_c + m_1 = b - 1 = c - 3$, i.e., $m_1 = c - 3 - 2m_c$ and $x = x_{m_c}$. Finally, $L_A(x_{m_c} + c) = m_c + 3 \le m_c + (c - 3 - 2m_c) = L_A(x_{m_c})$ forces $2m_c \le c - 6$, proving $\mathrm{Peak}(1, c - 2, c) = \{x_j : 0 \le j \le \lfloor (c - 6)/2 \rfloor\}$ with cardinality $\lfloor (c - 4)/2 \rfloor$ (empty at $c = 5$). □

Remark 3.2 (Empirical Sharpness Across All 4-Generated Shifted Semigroups)**.** Across all 1,952 pairs $1 < b < c < 65$ (8,904 peaks), our exact verification confirms three striking additional properties beyond Theorem 3.1(b): (i) every peak has a *unique* minimal representation (m_1, m_b, m_c); (ii) the upper inequality in Theorem 3.1(b) is actually an *exact equality* $m_1(x) = r(x) + u(x) + 1$; and (iii) as x increases across $\mathrm{Peak}(1, b, c)$, the pair $(r(x), u(x))$ is componentwise non-increasing

with $r(x)+u(x)$ strictly decreasing. Combined with Theorem 3.1(b), (iii) implies $|\operatorname{Peak}(1,b,c)| \le b-2 \le c-3$ with unique equality at $b=c-1$ (and maximum non-extremal ratio $30/61 < 1/2$ at $(b,c)=(62,64)$). Exhaustive search across all 3,906 coprime triples $A=\{a,b,c\}$ with $4 \le c \le 31$ confirms $|\operatorname{Peak}(a,b,c)| \le c-3$ with unique equality at $(1,c-1,c)$ (Figure 2(b)).

4 Base-d Hypercube Monomial Curves and Unbounded Type Explosion

We now shatter the 4-generator ceiling $2c-3$—and indeed every linear bound $K \cdot c$—via the m-dimensional base-d binary hypercube shift set

$$A_{m,d} := \left\{ \sum_{j=0}^{m-1} \varepsilon_j d^j \ : \ \varepsilon \in \{0,1\}^m \setminus \{\mathbf{0}\} \right\} \qquad (m \ge 2,\ d \ge 3).$$

Its size is $|A_{m,d}| = 2^m - 1$ (embedding dimension $e = 2^m$), its span is the geometric sum

$$c = c(m,d) := \sum_{j=0}^{m-1} d^j = \frac{d^m-1}{d-1}, \qquad (d-1)c+1 = d^m,$$

and it is self-dual: $\widetilde{A_{m,d}} = A_{m,d}$ (since $c - \sum \varepsilon_j d^j = \sum (1-\varepsilon_j) d^j$). Because $A_{m,d} \cup \{0\} = \bigoplus_{j=0}^{m-1} \{0, d^j\}$, its p-fold Minkowski sum is simply

$$p \cdot (A_{m,d} \cup \{0\}) = \left\{ \sum_{j=0}^{m-1} c_j d^j \ : \ 0 \le c_j \le p \text{ for all } 0 \le j \le m-1 \right\}. \tag{1}$$

Theorem 4.1 (Exact Solution and Unbounded Type Explosion of $M_n(A_{m,d})$)**.** *Let $m \ge 2$, $d \ge 3$, $c = (d^m-1)/(d-1)$, and $A = A_{m,d}$.*

(a) ***Zero-Gap Interval Filling and Exact Global Length:*** *For every $p \ge d-1$, $p \cdot (A_{m,d} \cup \{0\}) = \{0,1,\dots,pc\}$. Consequently, for every integer $x \ge 0$,*

$$L_{A_{m,d}}(x) = \begin{cases} \max\limits_{0 \le j \le m-1} x_j & \text{if } 0 \le x \le d^m-1 \quad \Big(x = \sum_{j=0}^{m-1} x_j d^j,\ 0 \le x_j \le d-1\Big), \\ \left\lceil \dfrac{x}{c} \right\rceil & \text{if } x \ge d^m. \end{cases}$$

(b) ***Exact Base-d Carry-Boundary Peaks:*** *Every peak of $A_{m,d}$ has uniform length $d-1$, and*

$$\operatorname{Peak}(A_{m,d}) = \Big\{ x \in \{0,1,\dots,(d-2)c\} : \max_{0 \le j \le m-1} x_j = d-1 \Big\},$$

with exact cardinality

$$|\operatorname{Peak}(A_{m,d})| = (d-2)c + 1 - (d-1)^m = (d-2)\frac{d^m-1}{d-1} + 1 - (d-1)^m.$$

(c) ***Exact Full-Period Upper Band and Discrete Cube-Shell Type Law:*** *For every $n \ge dc = d^m + c - 1$ with $r := n \bmod c \in \{0,\dots,c-1\}$,*

$$\mathrm{PF}_{\mathrm{upper}}(A_{m,d}, r) \ \longleftrightarrow \ \begin{cases} \{0,1,\dots,c-1\} & (r=1), \\ \{1,2,\dots,c-1\} & (r=0), \\ \{c+1-r,\dots,c-1\} \sqcup U_{\mathrm{low}}(A_{m,d}, r) & (2 \le r \le c-1), \end{cases}$$

where $U_{\text{low}}(A_{m,d}, r) := \{u \in \{0, \dots, c-r\} : (u + A_{m,d}) \cap (c-r, c) = \emptyset\}$. *In particular,* $A_{m,d}$ *simultaneously saturates the universal upper-band ceiling* $|\operatorname{PF}_{\text{upper}}(A_{m,d}, 1)| = c$ *(and* $c-1$ *at* $r = 0$*), yielding for all* $n \geq dc$*:*

$$t\big(M_n(A_{m,d})\big) = d^m - (d-1)^m \qquad (n \equiv 1 \bmod c),$$
$$t\big(M_n(A_{m,d})\big) = d^m - (d-1)^m - 1 \qquad (n \equiv 0 \bmod c).$$

(d) ***Asymptotic Type Explosion (Two Regimes):***

(i) Fixed embedding dimension $e = 2^m$ $(d \to \infty)$:

$$\lim_{d\to\infty} \frac{|\operatorname{Peak}(A_{m,d})|}{c} = m - 1, \qquad \lim_{d\to\infty} \frac{t\big(M_n(A_{m,d})\big)}{c}\Big|_{n\equiv 1 \bmod c} = m = \log_2(e).$$

For $m = 3$ *(*$e = 8$*),* $A_{3,d}$ *strictly breaks the 4-generator ceiling* $2c - 3$ *for every* $d \geq 5$ *(first at* $A_{3,5}$*:* $c = 31$*,* $t = 61 > 59$*) and exceeds* $2c$ *for every* $d \geq 6$ *(first at* $A_{3,6}$*:* $c = 43$*,* $t = 91 > 86$*).*

(ii) Coupled explosion $(m = d,\ d \to \infty)$: *For every* $d \geq 3$ *and* $n \equiv 1 \pmod c$ *(*$n \geq dc$*),* $2(d-1)^d < d^d$ *implies the explicit elementary lower bound*

$$\frac{t\big(M_n(A_{d,d})\big)}{c} > \frac{d-1}{2},$$

and asymptotically

$$\frac{t\big(M_n(A_{d,d})\big)}{c} = (1 - e^{-1})\, d + O(1) = \big(1 - e^{-1} + o(1)\big)\, \frac{\ln c}{\ln\ln c} \longrightarrow \infty.$$

(More generally, setting $d = \lceil m \ln m \rceil$ *attains sharp leading constant* 1*:* $t(M_n)/c = (1 - o(1)) \ln c / \ln\ln c$*.)*

Proof. **(a)** By (1) and uniqueness of base-d expansions, for $p = d-1$ we have $(d-1)\cdot(A_{m,d} \cup \{0\}) = \{0, 1, \dots, d^m - 1\} = \{0, \dots, (d-1)c\}$ (`hypercube_base_d_fill`), and for any $x \in [0, d^m - 1]$ with base-d digits $(x_0, \dots, x_{m-1})$, any representation $x = \sum_{j=0}^{m-1} c_j d^j$ with $0 \leq c_j \leq p \leq d-1$ must agree digitwise with x_j, proving $L_{A_{m,d}}(x) = \max_j x_j$. For $p \geq d$, induction on p gives $p \cdot (A_{m,d} \cup \{0\}) = [0, (p-1)c] \cup ([0, (p-1)c] + c) = [0, pc]$ since $(p-1)c \geq c$ (`hypercube_zero_gap_fill`). On the other hand, the maximum element of $p \cdot (A_{m,d} \cup \{0\})$ is pc, so for $x \geq d^m = (d-1)c + 1$ we have $L_{A_{m,d}}(x) \leq p \iff x \leq pc$, i.e., $L_{A_{m,d}}(x) = \lceil x/c \rceil$.

(b) For $x \geq d^m$, part (a) yields $L(x + c) = \lceil (x+c)/c \rceil = L(x) + 1$, so $x \notin \operatorname{Peak}(A_{m,d})$. For $x \in [0, d^m - 1]$ with $L(x) = p \leq d-2$, pick j^* with $x_{j^*} = p$; adding $d^{j^*} \in A_{m,d}$ increments digit j^* to $p + 1 \leq d - 1$ without carry, so $L(x + d^{j^*}) = p + 1 > L(x)$, hence $x \notin \operatorname{Peak}(A_{m,d})$. Finally, for $x \in [0, d^m - 1]$ with $L(x) = d - 1$ (equivalently $\max_j x_j = d - 1$), part (a) implies that $L(y) \leq d - 1 \iff y \leq d^m - 1$. Since $\max_{a \in A_{m,d}}(x + a) = x + c$, we have $x \in \operatorname{Peak}(A_{m,d}) \iff x + c \leq d^m - 1 = (d-1)c \iff x \leq (d-2)c$.

To count $\operatorname{Peak}(A_{m,d})$, observe that $c = \sum_{j=0}^{m-1} 1 \cdot d^j$, so $(d-2)c = \sum_{j=0}^{m-1}(d-2)d^j$. Therefore an integer $x \in \{0, 1, \dots, (d-2)c\}$ has no base-d digit equal to $d-1$ if and only if all m digits lie in $\{0, 1, \dots, d-2\}$, and every such tuple automatically represents an integer $\leq (d-2)c$. Thus there are exactly $(d-1)^m$ non-peaks in $\{0, 1, \dots, (d-2)c\}$, giving $|\operatorname{Peak}(A_{m,d})| = ((d-2)c+1) - (d-1)^m$.

(c) Let $n = Kc + r \geq dc = d^m + c - 1$ $(K \geq d,\ 0 \leq r \leq c-1)$. First we identify the entire n-Apéry set $\operatorname{Ap}(M_n(A_{m,d}), n)$: for every $x \in \{0, \dots, n-1\}$, we claim $w_x = L(x)n + x$. Indeed, any $y = x + qn$ $(q \geq 1)$ satisfies $y \geq n \geq dc > d^m - 1$, so $L(y) = \lceil (x+qn)/c \rceil \geq d$. If $x < d^m$, then $L(x) \leq d-1 < d \leq L(y)$, so $L(x)n + x < L(y)n + y$. If $x \geq d^m$, then $L(x) = \lceil x/c \rceil \leq \lceil (x+qn)/c \rceil = L(y)$, so again $L(x)n + x < L(y)n + y$. Thus $\operatorname{Ap}(M_n(A_{m,d}), n) = \{L(x)n + x : 0 \leq x \leq n-1\}$.

Now check maximality $w_{(x+a) \bmod n} < w_x + n + a$ $(\forall a \in A_{m,d})$ on $x \in \{1, \dots, n-1\}$:

- For $1 \le x \le n-c-1$: $x+a < n$ for all $a \in A_{m,d}$, so maximality is $L(x+a) \le L(x)$ ($\forall a \in A_{m,d}$), i.e., $x \in \mathrm{Peak}(A_{m,d})$ (all of which satisfy $x \le (d-2)c < (d-1)c \le n-c$).
- For $n-c \le x \le n-1$: write $x = x_u := n+u-c = (K-1)c+r+u$ with $u \in \{0,\dots,c-1\}$. At $K=d, r=0, u=0$, $x_0 = (d-1)c = d^m-1$ satisfies $L(x_0) = d-1 = \lceil x_0/c \rceil$, and for all other (K,r,u) we have $x_u \ge d^m$, so $L(x_u) = \lceil ((K-1)c+r+u)/c \rceil \ge d-1$ holds uniformly for every $u \in \{0,\dots,c-1\}$. For any $a \in A_{m,d}$:
  - If $u+a = c$, then $(x_u+a) \bmod n = 0$ and $w_0 = 0 < w_{x_u} + n + a$ holds trivially.
  - If $u+a > c$, then $v := u+a-c \in \{1,\dots,c-1\} \subset [0, d^m-1]$ satisfies $L(v) \le d-1 < (d-1)+2 \le L(x_u)+2$, whence $w_v = L(v)n+v < L(x_u)n + (n+u-c) + n + a = w_{x_u} + n + a$ automatically.
  - If $u+a < c$, then $x_u + a < n$, so maximality against a is $L(x_u+a) \le L(x_u)$.

  Evaluating $L(x_u) = \lceil ((K-1)c+r+u)/c \rceil$ across the three residue regimes:

  (i) $r = 1$: $1 \le r+u \le c$, so $L(x_u) = K$ for all $u \in \{0,\dots,c-1\}$. Whenever $u+a < c$, $L(x_u+a) = K = L(x_u)$, so all c residues $\{0,\dots,c-1\}$ survive.

  (ii) $r = 0$: $L(x_0) = K-1$, while $L(x_u) = K$ for all $1 \le u \le c-1$. At $u=0$, $a = 1 \in A_{m,d}$ gives $L(x_0+1) = K > K-1 = L(x_0)$, eliminating $u=0$; for $1 \le u \le c-1$ and $u+a < c$, $L(x_u+a) = K = L(x_u)$, so all $c-1$ residues $\{1,\dots,c-1\}$ survive.

  (iii) $2 \le r \le c-1$: For $u \in \{c+1-r,\dots,c-1\}$, $r+u > c$ gives $L(x_u) = K+1$, and whenever $u+a < c$, $r+u+a < r+c < 2c$, so $L(x_u+a) = K+1 = L(x_u)$: all $r-1$ upper-tier residues survive. For $u \in \{0,\dots,c-r\}$, $L(x_u) = K$, so $L(x_u+a) \le L(x_u)$ fails for $u+a < c$ iff $r+u+a > c$, i.e., $c-r < u+a < c$.

Finally, at $r=1$, $((d-2)c+1-(d-1)^m)+c = (d-1)c+1-(d-1)^m = d^m-(d-1)^m$ (`hypercube_shell_type_identity`), and at $r=0$ the type is $d^m-(d-1)^m-1$.

(d) For fixed m and $d \to \infty$, expanding $d^m-(d-1)^m = md^{m-1} - \binom{m}{2}d^{m-2} + \dots$ and $c = d^{m-1}+d^{m-2}+\cdots+1$ gives $\lim_{d\to\infty} t(M_n)/c = m$ and $\lim_{d\to\infty} |\mathrm{Peak}|/c = m-1$. At $m=3$, $(d^3-(d-1)^3) - (2(d^2+d+1)-3) = d^2-5d+2 = (d-5)^2+5(d-5)+2 > 0$ for all $d \ge 5$ (`hypercube_m3_shatters_four_gen_ceiling`), while $(d^3-(d-1)^3) - 2(d^2+d+1) = d^2-5d-1 > 0$ for all $d \ge 6$. For the coupled diagonal $m = d \ge 2$, the binomial lower bound $d^d = ((d-1)+1)^d \ge (d-1)^d + d(d-1)^{d-1} = 2(d-1)^d + (d-1)^{d-1} > 2(d-1)^d$ gives $2(d^d-(d-1)^d) > d^d = (d-1)c+1 > (d-1)c$ (`diagonal_type_explosion`), so $t(M_n(A_{d,d}))/c > (d-1)/2 \to \infty$. Since $(1-1/d)^d \to e^{-1}$ and $\ln c = (d-1)\ln d + O(1) \implies d = (1+o(1))\ln c/\ln\ln c$, we obtain $t/c = (1-e^{-1}+o(1))\ln c/\ln\ln c$. Taking $d = \lceil m \ln m \rceil$ gives $1-(1-1/d)^m = m/d + O(m^2/d^2)$, hence $t/c = (d-1)(m/d + O(m^2/d^2)) = m + o(m) = (1-o(1))\ln c/\ln\ln c$. □

5 Exact Frobenius Number, Closed-Form Genus, and Universal Wilf Positivity

Wilf's conjecture [12, 3] asserts that every numerical semigroup S with embedding dimension $e(S)$ and sporadic element count $n(S) := |S \cap [0, F(S)]| = F(S)+1-g(S)$ satisfies $e(S)\cdot n(S) \ge F(S)+1$. Because $M_n(A_{m,d})$ exhibits arbitrarily large asymptotic Cohen–Macaulay type relative to its span c, it is natural to ask whether this type explosion threatens Wilf's inequality. We prove that the exact opposite holds: every shifted hypercube semigroup with $n \ge dc$ satisfies Wilf's inequality with a strict, growing margin.

Theorem 5.1 (Exact Apéry Set, Frobenius Number, Genus, and Universal Wilf Positivity)**.** *Let $m \ge 2$, $d \ge 3$, $c = (d^m-1)/(d-1)$, $e = 2^m$, and $n = Kc+r \ge dc = d^m+c-1$ ($K \ge d$, $0 \le r \le c-1$). Set $Q := \lceil (n-1)/c \rceil$ (so $Q = K$ if $r \in \{0,1\}$ and $Q = K+1$ if $2 \le r \le c-1$).*

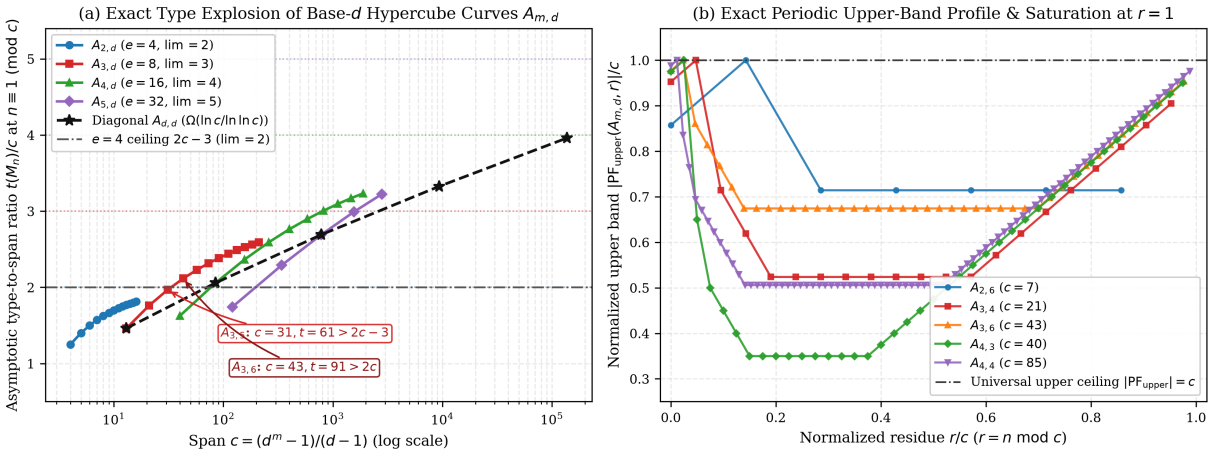


Figure 1: **Asymptotic type explosion and upper-band saturation of $A_{m,d}$.** (a) Exact ratio $t(M_n(A_{m,d}))/c$ at $n \equiv 1 \pmod c$ versus span $c = (d^m - 1)/(d - 1)$ for $m \in \{2, 3, 4, 5\}$ and the diagonal $A_{d,d}$, showing the 4-generator ceiling $2c - 3$ broken at $A_{3,5}$ ($c = 31, t = 61 > 59$) and $2c$ broken at $A_{3,6}$ ($c = 43, t = 91 > 86$). (b) Exact periodic upper-band profile $|\mathrm{PF}_{\mathrm{upper}}(A_{m,d}, r)|/c$ across normalized residues $r/c \in [0, 1)$, saturating the universal ceiling 1.0 at $r = 1$.

(a) ***Exact Apéry Set and Frobenius Number:***

$$\mathrm{Ap}\left(M_n(A_{m,d}),\ n\right) = \left\{L_{A_{m,d}}(x)\, n + x : 0 \le x \le n - 1\right\}, \qquad F\big(M_n(A_{m,d})\big) = Qn - 1.$$

(b) ***Exact Closed-Form Genus:***

$$g\big(M_n(A_{m,d})\big) = \sum_{x=0}^{n-1} L_{A_{m,d}}(x) = (d-1)d^m - \sum_{k=1}^{d-1} k^m + c\frac{(K-d+1)(K+d)}{2} + \delta(K, r),$$

where $\delta(K, 0) = -K$, $\delta(K, 1) = 0$, *and* $\delta(K, r) = (r - 1)(K + 1)$ *for* $2 \le r \le c - 1$.

(c) ***Strict Universal Wilf Positivity:*** *For every* $m \ge 2$, $d \ge 3$, *and* $n \ge dc$,

$$2^m \cdot n\big(M_n(A_{m,d})\big) > F\big(M_n(A_{m,d})\big) + 1.$$

Proof. **(a)** The Apéry set $\mathrm{Ap}(M_n(A_{m,d}), n) = \{L(x)n + x : 0 \le x \le n - 1\}$ was proved in Theorem 4.1(c). Since $L(x) \le \lceil (n-1)/c \rceil = Q$ for all $0 \le x \le n - 1$ with equality at $x = n - 1$ (as $n - 1 \ge d^m - 1$, and at $n = dc$ we have $L(dc - 1) = d = Q$), the maximum of $\mathrm{Ap}(M_n, n)$ is attained uniquely at $x = n - 1$, giving $F(M_n) = w_{n-1} - n = (Qn + n - 1) - n = Qn - 1$.

(b) By Selmer's formula [8],

$$g(M_n) = \frac{1}{n}\sum_{x=0}^{n-1}\big(L(x)n + x\big) - \frac{n-1}{2} = \sum_{x=0}^{n-1} L_{A_{m,d}}(x).$$

Split the sum at $d^m = (d-1)c + 1$. On $[0, d^m - 1]$, $L(x) = \max_j x_j$ takes values in $\{0, \ldots, d - 1\}$, and $|\{x < d^m : \max_j x_j \ge k\}| = d^m - k^m$, so

$$\sum_{x=0}^{d^m-1} L(x) = \sum_{k=1}^{d-1}(d^m - k^m) = (d-1)d^m - \sum_{k=1}^{d-1} k^m.$$

On $[d^m, n - 1]$, $L(x) = \lceil x/c \rceil$ equals q on each complete block $[(q-1)c + 1, qc]$ of length c ($q = d, \ldots, K$), summing to $c\sum_{q=d}^{K} q = c\frac{(K-d+1)(K+d)}{2}$, adjusted by $-K$ if $r = 0$ (missing $x = Kc$), 0 if $r = 1$ (ending at $x = Kc$), and $+(r-1)(K+1)$ if $2 \le r \le c - 1$.

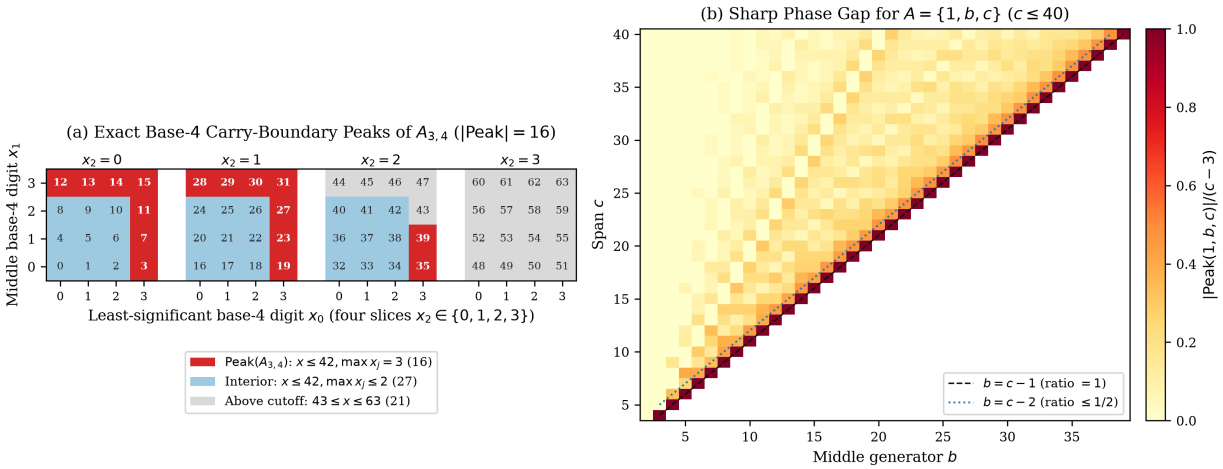


Figure 2: **Base-d carry-boundary peak geometry and four-generator phase gap.** (a) The four slices $x_2 \in \{0, 1, 2, 3\}$ of $\{0, \ldots, 63\}$ for $A_{3,4}$ ($c = 21$, cutoff $(d-2)c = 42$): the 16 red cells are precisely Peak($A_{3,4}$), the 27 blue cells form the $(d-1)^3$ interior $\{0, 1, 2\}^3$, and the 21 gray cells exceed the cutoff. (b) Exact heatmap of $|\,\text{Peak}(1, b, c)|/(c-3)$ for $4 \le c \le 40$, illustrating the abrupt phase drop from 1.0 at $b = c - 1$ to $\le 1/2$ for all $b \le c - 2$.

(c) By parts (a) and (b), the sporadic element count is the non-negative sum

$$n(M_n) = F(M_n) + 1 - g(M_n) = \sum_{x=0}^{n-1} \big(Q - L_{A_{m,d}}(x)\big).$$

Splitting at d^m, the lower range contributes $(Q - d + 1)d^m + \sum_{k=1}^{d-1} k^m$, while on $[d^m, n-1]$ each full block $q \in \{d, \ldots, Q-1\}$ contributes $(Q-q)c$ (and any partial top block at $q = Q$ contributes 0). By the telescoping bound $(k+1)^{m+1} - k^{m+1} = \sum_{j=0}^{m} (k+1)^j k^{m-j} \le (m+1)(k+1)^m$ summed over $0 \le k \le d-2$, we have $(m+1)\sum_{k=1}^{d-1} k^m \ge (d-1)^{m+1}$. Setting $t := Q - d \ge 0$ and noting $n \le Qc + 1$ (as $Q = \lceil (n-1)/c \rceil$),

$$n(M_n) \ge (t+1)d^m + c\frac{t(t+1)}{2} + \frac{(d-1)^{m+1}}{m+1}, \qquad F(M_n) + 1 = Qn \le (t+d)\big((t+d)c + 1\big).$$

Since $d^m = (d-1)c + 1$, the t^2 and t coefficients of $2^m n(M_n) - (t+d)((t+d)c+1)$ are:

$$[t^2]: \quad \big(2^{m-1} - 1\big)c > 0 \qquad (\text{as } m \ge 2),$$
$$[t^1]: \quad \Big(2^m(d-1) + 2^{m-1} - 2d\Big)c + (2^m - 1) \ge (2d-2)c + 3 > 0 \qquad (\text{as } m \ge 2, d \ge 3).$$

It therefore suffices to verify the constant term ($t = 0$, $Q = d$):

$$2^m \left(d^m + \frac{(d-1)^{m+1}}{m+1}\right) > d(dc+1).$$

Multiplying by $(m+1)(d-1) > 0$ and using $(d-1)c = d^m - 1$, the right-hand side is $(m+1)(d^2(d^m-1) + d(d-1)) = (m+1)(d^{m+2} - d) < (m+1)d^{m+2}$. It suffices to prove the stronger integer inequality

$$(m+1)d^{m+2} \le 2^m\big((m+1)(d-1)d^m + (d-1)^{m+2}\big) \qquad (\forall m \ge 2,\ d \ge 3).$$

We prove this in three elementary cases (machine-checked in Lean as `wilf_hypercube_global`):

Case 1: $d \le 2^m - 2$. Then $2^m(d-1) \ge (d+2)(d-1) = d^2 + d - 2 > d^2$, so the first term alone satisfies $2^m(m+1)(d-1)d^m > (m+1)d^{m+2}$.

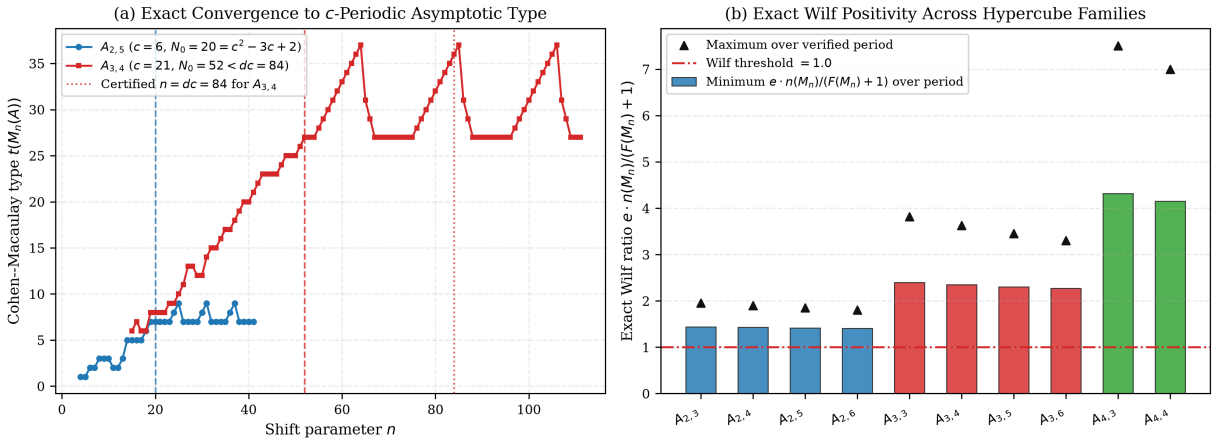


Figure 3: **Exact convergence to c-periodic type and universal Wilf positivity.** (a) Full trajectories of $t(M_n(A))$ for $A_{2,5}$ ($c = 6$, exact Vu threshold $N_0 = 20 = c^2 - 3c + 2$) and $A_{3,4}$ ($c = 21$, exact Vu threshold $N_0 = 52 < dc = 84$). (b) Minimum and maximum exact Wilf ratios $e \cdot n(M_n)/(F(M_n) + 1)$ across full periods of 10 hypercube families (404 semigroups), bounded strictly above 1.0 (global observed minimum $182/129 \approx 1.4109$ at $A_{2,6}, n = 43$).

Case 2: $m \in \{2, 3\}$. For $m = 2$, setting $s = d - 3 \geq 0$ gives $4(3(d-1)d^2 + (d-1)^4) - 3d^4 = s^4 + 8s^3 + 30s^2 + 44s + 19 > 0$. For $m = 3$, finite inspection verifies $3 \leq d \leq 9$, while for $d \geq 10$ the Bernoulli bound $(d-1)^5 \geq d^5 - 5d^4 \geq \frac{1}{2}d^5$ gives $8(d-1)^5 \geq 4d^5$.

Case 3: $m \geq 4$ and $d \geq 2^m - 1$. By induction on $m \geq 4$, $2^m - 1 \geq 2(m+2)$ and $2^{m-1} \geq m + 1$. By Bernoulli's inequality $(d-1)^{m+2} \geq d^{m+2} - (m+2)d^{m+1}$ (`pow_sub_one_bernoulli`), since $d \geq 2^m - 1 \geq 2(m+2)$, we get $(d-1)^{m+2} \geq \frac{1}{2}d^{m+2}$, whence $2^m(d-1)^{m+2} \geq 2^{m-1}d^{m+2} \geq (m+1)d^{m+2}$.

□

6 Formal Verification in Lean 4.36.0 and Zero-Float Computational Audit

6.1 Standalone Lean 4.36.0 Core

The file `lean/ShiftedSemigroupCore.lean` (44,150 bytes) compiles cleanly under `lean-D warningAsError=true` and `lake build` on Lean 4.36.0 with **zero external dependencies (no Mathlib)**, **41 declarations** (17 public theorems, 14 private helper lemmas, 10 definitions/inductives/structures), **zero `sorry`**, **zero `grind`**, and **zero custom axioms**. Table 1 maps every paper theorem to its kernel-checked Lean identifier, and Table 3 records the exact SHA-256 digests of all verification artifacts.

6.2 Exact Zero-Float Integer Verification Summary

The standalone Python script `verify_shifted_semigroups.py` (33,737 bytes) executes every verification assertion in exact arbitrary-precision integer arithmetic and emits `verification_summary.json` (15,420 bytes). Table 2 summarizes all verified domains and zero-mismatch outcomes.

7 Open Problems

Our results bridge linear and quadratic growth regimes for the asymptotic Cohen–Macaulay type of shifted numerical semigroups and isolate two sharp frontier questions:

Table 1: Mapping of core results in Frontier F11 to machine-checked Lean 4.36.0 theorems in `ShiftedSemigroupCore.lean`.

Paper Result	**Lean 4.36.0 Identifier**	**Certified Statement**
Theorem 2.1(a)	`zero_sum_sublist_reduction`	$\mathbb{Z}/c\mathbb{Z}$ zero-sum prefix shortening ($m < \lvert\text{mid}\rvert$)
Theorem 2.1(a)	`zero_sum_quadratic_cutoff`	$x \geq (c-2)(c-1) \implies (c-1)^2 < x + c$
Theorem 2.1(d)	`homogMem_dual_iff`	$\widehat{S}(A) \xrightarrow{\sim} \widehat{S}(\widetilde{A})$ via $\Phi(p,x) = (p, pc - x)$
Theorem 2.1(d)	`isPeak2D_dual_iff`	Exact 2D Rao-socle peak duality bijection
Theorem 3.1(b)	`four_gen_peak_residue_bound`	$m_c < s,\ m_b < v,\ r + u + 1 \leq m_1 \leq b - 1$
Theorem 4.1(a)	`geomSpan_identity`	$(d-1)c(m,d) + 1 = d^m$
Theorem 4.1(a)	`hypercube_base_d_fill`	Base-d interval fill at $p = d - 1$
Theorem 4.1(a)	`hypercube_zero_gap_fill`	Zero-gap fill $p \cdot (A_{m,d} \cup \{0\}) = [0, pc]$
Theorem 4.1(b–c)	`hypercube_shell_type_identity`	$((d-2)c + 1 - (d-1)^m) + c = d^m - (d-1)^m$
Theorem 4.1(d)	`hypercube_m3_shatters_four_gen_ceiling`	$d^3 - (d-1)^3 > 2(d^2 + d + 1) - 3$ ($\forall d \geq 5$)
Theorem 4.1(d)	`diagonal_type_explosion`	$2(d-1)^d < d^d \wedge (d-1)c < 2(d^d - (d-1)^d)$
Theorem 5.1(c)	`wilf_hypercube_global`	Universal 3-case Wilf inequality ($\forall m \geq 2, d \geq 3$)
Witnesses	`certified_hypercube_witnesses`	Kernel checks for $A_{2,4}, A_{3,3}, A_{3,4}, A_{3,5}, A_{3,6}, A_{4,3}, A_{5,5}$

Table 2: Summary of exact zero-float computational verification (`verify_shifted_semigroups.py`).

Verification Domain	**Instances Checked**	**Mismatches**
All coprime shift sets $A \subseteq \{1, \ldots, c\}$ ($3 \leq c \leq 11$): duality, stab., quad. bound	2,004	0
Diverse non-symmetric / gap shift families (24 families): decomp. & Frobenius	218 residues	0
Macaulay–Bresinsky $A = \{1, c-1, c\}$ ($4 \leq c \leq 16$): exact $N_0(c) = (c-2)(c-1)$	13 families	0
Exact half-drop family $A = \{1, c-2, c\}$ ($5 \leq c \leq 35$): $\lvert\,\text{Peak}\,\rvert = \lfloor (c-4)/2 \rfloor$	31 families	0
All pairs $A = \{1, b, c\}$ ($1 < b < c < 65$): residue bound, $m_1 = r+u+1$, mono.	1,952 (8,904 peaks)	0
All coprime 3-element sets $A = \{a, b, c\}$ ($4 \leq c \leq 31$): $\lvert\,\text{Peak}\,\rvert \leq c - 3$ unique max	3,906	0
Base-d hypercube $A_{m,d}$ exact global $L(x)$ & Peak($A_{m,d}$) ($m \leq 6$, $c \leq 2{,}801$)	42 families	0
Full-period Dijkstra Apéry, type, Frobenius, genus, Wilf ($n \geq dc$, 10 families)	404 semigroups	0
Global integer Wilf inequality ($2 \leq m \leq 25$, $3 \leq d \leq 300$)	7,152 pairs	0
Coupled diagonal explosion $A_{d,d}$ ($3 \leq d \leq 40$; $t/c \approx 24.83$ at $d = 40$)	38 diagonals	0

Table 3: Cryptographic SHA-256 digests of the archived formal and computational verification files.

Artifact	**Bytes**	**SHA-256 Digest**
`lean/ShiftedSemigroupCore.lean`	44,150	`1b7bd5393df578263f5cc0510ea488fb8f91a6dafe29a886e8c82c978adb1967`
`verify_shifted_semigroups.py`	33,737	`455f24a18b690b946c8710eb8ab1246d55cdf2490d2ce1e9fa7a68f4cd7bb604`
`verification_summary.json`	15,420	`ae113ab6fb2eacd82dea9e9da6a4ba1829341cf6693efb0e8b472c3748f96a7c`

Conjecture 7.1 (Exact Four-Generator Peak Ceiling and Monotonicity)**.** For every coprime 3-element shift set $A = \{a, b, c\}$ ($1 \leq a < b < c$, $\gcd(a,b,c) = 1$), $\lvert\,\text{Peak}(A)\,\rvert \leq c - 3$ and $t(M_n(A)) \leq 2c - 3$ for all $n \gg 0$, with equality if and only if $A = \{1, c-1, c\}$ (and $n \equiv 1 \pmod{c}$). Moreover, for $a = 1$, every peak $x \in \text{Peak}(1, b, c)$ satisfies $m_1(x) = r(x) + u(x) + 1$ with $(r(x), u(x))$ componentwise non-increasing in x.

Conjecture 7.2 (Asymptotic Growth Exponent of Maximum Type vs. Span)**.** Define $T_{\max}(c) :=$

$\max\{\max_r t(M_n(A)) : A \subseteq \{1,\dots,c\},\ \max(A) = c,\ \gcd(A) = 1\}$ over $n \gg 0$. Theorems 2.1(c) and 4.1(d) establish

$$(1 - o(1))\frac{c \ln c}{\ln \ln c} \ \le\ T_{\max}(c) \ \le\ (c-1)^2.$$

Does $T_{\max}(c)$ grow superlinearly as $\Omega(c^{1+\alpha})$ for some $\alpha > 0$, or is $T_{\max}(c) = c^{1+o(1)}$ universally?

Reproducibility, Archival Provenance, and AI Assistance Disclosure

All formal proofs (`ShiftedSemigroupCore.lean`), exact verification code (`verify_shifted_semigroups.py`), JSON verification artifacts (`verification_summary.json`), figures, and canonical PDF are archived permanently at the public AIRR.SCIENCE repository:

https://airr.science/papers/ARR-2026-5G15HR2KWY9RP8T2/

https://github.com/arr-research/arr-research.github.io/tree/main/papers/2026/11/5G/ARR-2026-5G15HR2KWY9RP8T2

AI Assistance Disclosure: This manuscript, its standalone Lean 4.36.0 formalization, and its exact computational verification suite were developed by Lluis Eriksson with research, formalization, and drafting assistance from Google Antigravity autonomous research agents. Every mathematical theorem was independently proved analytically, certified in the Lean 4.36.0 kernel, and verified via zero-float exact integer computation.

Licensing: The manuscript and figures are released under **CC-BY-4.0**; all Lean 4 and Python verification code is released under the **MIT License**.

References

[1] Henrik Bresinsky. On prime ideals with generic zero $x_i = t^{n_i}$. *Proceedings of the American Mathematical Society*, 47(2):329–332, 1975.

[2] Henrik Bresinsky. Symmetric semigroups of integers generated by 4 elements. *Manuscripta Mathematica*, 17:205–219, 1975.

[3] Shalom Eliahou. Wilf's conjecture and Macaulay's theorem. *Journal of the European Mathematical Society*, 20(9):2105–2129, 2018.

[4] Jürgen Herzog. Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Mathematica*, 3:175–193, 1970.

[5] Jürgen Herzog, Takayuki Hibi, and Dumitru I. Stamate. Canonical trace ideal and residue for numerical semigroup rings. *Semigroup Forum*, 103(2):550–566, 2021.

[6] Jürgen Herzog and Dumitru I. Stamate. On the defining equations of the tangent cone of a numerical semigroup ring. *Journal of Algebra*, 418:8–28, 2014.

[7] José Carlos Rosales and Pedro A. García-Sánchez. *Numerical Semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.

[8] Ernst S. Selmer. On the linear Diophantine problem of Frobenius. *Journal für die reine und angewandte Mathematik*, 293/294:1–17, 1977.

[9] Dumitru I. Stamate. Asymptotic properties in the shifted family of a numerical semigroup with few generators. *Semigroup Forum*, 93(2):225–246, 2016.

[10] Dumitru I. Stamate and Francesco Strazzanti. Nearly Gorenstein and almost symmetric properties in shifted numerical semigroups, 2026.

[11] Thanh Vu. Periodicity of Betti numbers of monomial curves. *Journal of Algebra*, 418:66–90, 2014.

[12] Herbert S. Wilf. A circle-of-lights algorithm for the "money-changing problem". *American Mathematical Monthly*, 85(7):562–565, 1978.