

Period Separation and the Single-Period Conjecture

An application of binary necklace partitions

Abstract

The single-period conjecture for the binary Ducci map asks whether an odd width at which every nonzero periodic word has the same temporal period must be prime. We apply the partition into binary-necklace components to this question. If $2^s \equiv -1 \pmod{n}$, the classical identity $D^{2^s-1} = R^{-1}$ on the periodic subspace implies that a word of temporal period τ has spatial period $\gcd(n, \tau)$. Distinct spatial-period classes therefore have disjoint temporal spectra. Every divisor $d > 1$ of n occurs, yielding at least $d(n) - 1$ nonzero periods, where $d(n)$ is the number of positive divisors of n . We give the exact cardinality of each spatial class and of its full basin in the power set. Combining this separation with the finite-field degree condition proves that a composite single-period width, if one exists, must have odd multiplicative order of 2. A polynomial-gcd criterion then certifies period diversity and counts both parts of the resulting partition without selecting words. At Mersenne widths it gives a complete ordinary-period census, including exact counts for $n = 2047$. The remaining question is a uniform obstruction for composite widths satisfying the odd-order and constant-degree conditions.

Keywords. Binary necklaces; Ducci map; temporal periods; spatial periods; finite fields; overpseudoprimes; Möbius inversion.

1 The question and the contribution

Let $n > 1$ be odd. On $V_n = \mathbb{F}_2^n$, let R rotate coordinates one position to the right and put $D = I + R$. Thus D replaces each bit by its sum modulo two with its preceding neighbor. On binary entries this is the absolute difference operation of the Ducci map. A word v is *periodic* if $D^\tau v = v$ for some $\tau > 0$; its *ordinary temporal period* is the least such τ . Define

$$\mathcal{S}(n) = \{\text{per}_D(v) : v \neq 0, v \text{ is periodic}\}. \quad (1.1)$$

The zero fixed point is excluded. It is the only fixed word, since $Dv = v$ would give $Rv = 0$.

Conjecture 1.1 (Single-period conjecture). *If $n > 1$ is odd and $|\mathcal{S}(n)| = 1$, then n is prime.*

Breuer, Lötter, and van der Merwe pose this as Question 6.1 in [3], counting the zero fixed point's period 1 as well: do exactly two periods force prime width? The conjecture is also recorded in OEIS A138004 [6]. The converse is false; prime width need not give a single nonzero period. Nor does a single period mean a single cycle: many cycles can have the same length.

The companion papers *Consequences of Binary Necklaces* [1] and *The Partitioning of Power Sets Into Graphs* [2] pass from words to their rotation classes and then to components of the induced functional graph. Here that partition becomes a tool for a specific period question. The essential point is to retain spatial period and rotational drift. The unlabeled graph shape alone does not determine a word's temporal period.

We develop three consequences. First, when a power of 2 is -1 modulo n , a temporal period determines its spatial period. The component partition then separates at least $d(n) - 1$ temporal

periods, where $d(n)$ counts the positive divisors of n . Second, a finite-field degree argument extends the exclusion to *every composite width with even* $\text{ord}_n(2)$. Third, fixed subspaces give exact polynomial certificates of period diversity, including for widths outside the first theorem.

The polynomial description of Ducci periods is established [3, Theorems 3.7 and 3.9], and the operator identity behind our first theorem is classical [4, proof of Theorem 2]. We derive their spatial-period refinement, its mass formulas, and the resulting reduction of Conjecture 1.1. All required arguments are included. These are presented as deductions from the established framework; no claim of priority for the corollaries is made.

2 The periodic part and the necklace partition

2.1 The periodic subspace

Identify a word v with $\sum_{i=0}^{n-1} v_i x^i$ modulo $x^n + 1$. Then R and D are multiplication by x and $1 + x$. Set

$$Q_n(x) = \frac{x^n + 1}{x + 1}. \quad (2.1)$$

The polynomial $x^n + 1$ is squarefree because n is odd. The Chinese remainder theorem gives

$$V_n \simeq \mathbb{F}_2 \oplus W_n, \quad W_n = \mathbb{F}_2[x]/Q_n(x). \quad (2.2)$$

Evolution kills the first coordinate and is invertible on W_n . Consequently the periodic words correspond precisely to $\{0\} \oplus W_n$; we identify this subspace with W_n . In word coordinates it is the even-weight subspace: the first CRT coordinate is evaluation at $x = 1$. It has 2^{n-1} elements.

Let $\rho : V_n \rightarrow W_n$ be the periodic-coordinate projection. Each $w \in W_n$ has two lifts under ρ , one periodic and one transient. The eventual temporal period of either lift equals the period of w . Thus a union of periodic orbits containing a core words corresponds to $2a$ starting words in the full power set. In particular, the zero core has a basin of size two.

2.2 Three different periods

For a nonzero periodic word w , write

$$d(w) = \min\{d > 0 : R^d w = w\}, \quad (2.3)$$

$$t(w) = \min\{t > 0 : D^t w \in \langle R \rangle w\}, \quad (2.4)$$

$$\tau(w) = \min\{\tau > 0 : D^\tau w = w\}. \quad (2.5)$$

These are its spatial period, necklace period, and ordinary temporal period. If $D^t w = R^s w$, with $0 \leq s < d$, then

$$\tau = \frac{td}{\gcd(d, s)}. \quad (2.6)$$

Indeed an exact return takes a multiple kt of the necklace period, and it is an exact return precisely when $d \mid ks$.

The joint orbit $\langle R, D \rangle w$ has dt periodic words. Its rotation quotient is one necklace cycle of length t . Together with its transient predecessors, it gives one component of the necklace functional graph and represents $2dt$ words of V_n . The core contains $dt/\tau = \gcd(d, s)$ ordinary cycles. These facts also follow from the coset classification in [2]; here they follow directly by counting the t rotation orbits of size d .

At odd width each cycle vertex in the necklace graph has one transient leaf. To see uniqueness, every core word has a unique periodic predecessor and one transient predecessor. Those two predecessors are complements. Complementation commutes with rotation, so the transient predecessors of one core necklace form one necklace of the same spatial period.

2.3 Local multiplicative orders

Factor $Q_n = \prod_{i=1}^r f_i$ into distinct monic irreducibles and put $e_i = \deg f_i$. Then

$$W_n \simeq \prod_{i=1}^r \mathbb{F}_{2^{e_i}}. \quad (2.7)$$

In factor i , let α_i be the image of x and set $\lambda_i = \text{ord}(1 + \alpha_i)$. Multiplication by $1 + \alpha_i$ gives every nonzero element of that coordinate period λ_i . Hence

$$\mathcal{S}(n) = \{\text{lcm}_{i \in S} \lambda_i : \emptyset \neq S \subseteq \{1, \dots, r\}\}. \quad (2.8)$$

Every support occurs in (2.7). In particular,

$$|\mathcal{S}(n)| = 1 \iff \lambda_1 = \dots = \lambda_r. \quad (2.9)$$

This is the standard local-order criterion [3, 6]. It will be used for the reduction in Section 4; the next theorem does not require factoring Q_n .

3 Separation by spatial period

Suppose throughout this section that

$$2^s \equiv -1 \pmod{n} \quad \text{for some } s \geq 1, \quad B = 2^s - 1. \quad (3.1)$$

Since $n \mid 2^s + 1$, we have

$$\gcd(n, B) = 1. \quad (3.2)$$

Theorem 3.1 (Spatial-period separation). *Under (3.1), every nonzero periodic word satisfies*

$$\boxed{d = \gcd(n, \tau), \quad t = \gcd(B, \tau) = \frac{\tau}{d}, \quad \tau = dt.} \quad (3.3)$$

In particular, $t \mid B$, $\gcd(t, n) = 1$, and words with different spatial periods cannot have the same ordinary temporal period. Each necklace component has exactly one ordinary cycle in its core and has mass $2\tau = 2dt$ in the power set.

Proof. Repeated squaring in characteristic two gives

$$D^{2^s} = I + R^{2^s} = I + R^{-1} = R^{-1}D.$$

On the periodic subspace D is invertible, so cancellation yields the classical identity

$$D^B = R^{-1} \quad \text{on } W_n. \quad (3.4)$$

In particular $D^{nB} = I$, so $\tau \mid nB$. By (3.2), there are unique $d_0 \mid n$ and $t_0 \mid B$ with $\tau = d_0 t_0$. On an ordinary D -cycle of length τ , the permutation D^B has order $\tau / \gcd(\tau, B) = d_0$. Equation (3.4) identifies this order with the spatial period d , so $d = d_0 = \gcd(\tau, n)$.

Moreover $R = D^{-B}$ on the core. Thus rotation stays inside an ordinary D -cycle, and the joint $\langle R, D \rangle$ orbit is that same cycle. Its quotient by rotation has $\tau/d = t_0$ vertices and is one necklace cycle. This proves the formula for t , as well as the one-cycle assertion. The two lifts of each core word give mass 2τ . $\square$

3.1 Exact sizes of the spatial classes

Let $d(n)$ denote the number of positive divisors of n , and let μ denote the integer Möbius function. For odd $d \geq 1$, define

$$A(d) = \sum_{e|d} \mu(d/e) 2^{e-1}. \quad (3.5)$$

In particular $A(1) = 1$.

Lemma 3.2. *For every odd n and every $d \mid n$, exactly $A(d)$ periodic words have spatial period d . If $d > 1$, then $A(d) > 0$.*

Proof. A word fixed by R^d repeats a block of length d . Because n/d is odd, the repeated word has even weight exactly when its block does. There are 2^{d-1} such words. Therefore $2^{d-1} = \sum_{e|d} A(e)$, and Möbius inversion gives (3.5). For positivity, a block of odd length $d > 1$ with weight two cannot be a proper repetition: the odd repetition number would divide two. Its repetition to length n is periodic and has spatial period exactly d . $\square$

For $d \mid n$, $d > 1$, set

$$\mathcal{S}_d(n) = \{\tau(w) : w \in W_n, d(w) = d\}.$$

Under (3.1), Theorem 3.1 gives the disjoint union

$$\mathcal{S}(n) = \bigsqcup_{\substack{d|n \\ d>1}} \mathcal{S}_d(n), \quad \mathcal{S}_d(n) \subseteq \{dt : t \mid B, \gcd(t, n) = 1\}. \quad (3.6)$$

The inclusion is a necessary condition, not an assertion that every listed dt occurs. Each spatial class contains $A(d)$ core words and its full basin contains $2A(d)$ words. These masses satisfy

$$2 + \sum_{\substack{d|n \\ d>1}} 2A(d) = 2^n. \quad (3.7)$$

This equality accompanies a disjoint partition: the spatial period of each core word is unique, and every starting word has a unique core coordinate.

Corollary 3.3. *If (3.1) holds, then*

$$|\mathcal{S}(n)| \geq d(n) - 1. \quad (3.8)$$

Consequently Conjecture 1.1 holds for every odd width at which a power of 2 is -1 modulo n .

Proof. Every set in (3.6) is nonempty by Lemma 3.2. If n is composite, $d(n) - 1 \geq 2$. $\square$

Corollary 3.4 (An infinite family). *At width $n = 3^k$, $k \geq 1$, there are at least k distinct nonzero ordinary periods. For $1 \leq j \leq k$, the spatial class $d = 3^j$ contains*

$$2^{3^j-1} - 2^{3^{j-1}-1} \quad (3.9)$$

periodic words and has basin mass $2^{3^j} - 2^{3^{j-1}}$.

Proof. The congruence $2^{3^{k-1}} \equiv -1 \pmod{3^k}$ follows by induction: cubing a number congruent to -1 modulo 3^k gives -1 modulo 3^{k+1} . Apply Corollary 3.3. Only two terms in (3.5) survive for $d = 3^j$, giving (3.9). $\square$

The corollary provides a lower bound, not a claim of exactly k periods for every k . It separates k classes and counts all their words without determining the individual temporal periods within each class.

4 The even-order cases of the conjecture

For an odd integer $u > 1$, write $\text{ord}_u(2)$ for the least positive r such that $2^r \equiv 1 \pmod{u}$.

Lemma 4.1 (Constant-degree condition). *If $\mathcal{S}(n) = \{T\}$, then*

$$\text{ord}_d(2) = \text{ord}_T(2) = \text{ord}_n(2) \quad \text{for every } d \mid n, d > 1. \quad (4.1)$$

Proof. Take an element α of exact multiplicative order d in an algebraic closure of $\mathbb{F}_2$. It is a root of Q_n , so (2.9) implies that $1 + \alpha$ has exact order T . An element of odd order $u > 1$ has degree $\text{ord}_u(2)$ over $\mathbb{F}_2$, since this is the least exponent r for which raising to 2^r fixes it. But $\mathbb{F}_2(\alpha) = \mathbb{F}_2(1 + \alpha)$, so the two degrees agree. Taking $d = n$ gives the final equality. All these orders are defined: $\alpha \neq 0, 1$, so $1 + \alpha \neq 0, 1$ and $T > 1$ is odd. $\square$

For composite n , condition (4.1) is the divisor-order characterization of an *overpseudoprime to base 2* [5, Theorem 2]. Equal field degrees are necessary for equal local periods, but they do not make the periods equal.

Theorem 4.2 (Odd-order reduction). *If an odd composite n satisfies $|\mathcal{S}(n)| = 1$, then n is an overpseudoprime to base 2 and $\text{ord}_n(2)$ is odd. Equivalently, Conjecture 1.1 holds for every odd n for which $\text{ord}_n(2)$ is even.*

Proof. The overpseudoprime condition follows from Lemma 4.1. Suppose the common order $r = \text{ord}_n(2)$ were even. For each exact prime-power divisor $p^e \parallel n$, that lemma gives $\text{ord}_{p^e}(2) = r$. The residue $2^{r/2}$ has order two modulo p^e . For an odd prime power, the only nonidentity solution of $z^2 = 1$ is $z = -1$: the two factors of $(z - 1)(z + 1)$ have no common odd prime divisor, so one is divisible by p^e . Thus $2^{r/2} \equiv -1 \pmod{p^e}$ for every $p^e \parallel n$. The Chinese remainder theorem gives $2^{r/2} \equiv -1 \pmod{n}$. Corollary 3.3 now supplies at least two nonzero periods, a contradiction. $\square$

Remark 4.3. Even $\text{ord}_n(2)$ alone does not imply that -1 is a power of 2 modulo n . For example, $\text{ord}_{15}(2) = 4$ but the powers of 2 modulo 15 omit -1 . The proof uses the single-period hypothesis to force equal orders on *all* prime-power divisors before applying the Chinese remainder theorem. Width 15 already fails the degree condition because $\text{ord}_3(2) = 2$ and $\text{ord}_5(2) = 4$.

5 Polynomial certificates and exact masses

The remaining widths need not satisfy (3.1). A fixed-space test gives a second way to separate periods. For any odd $n > 1$ and $u \geq 1$, define

$$g_n(u) = \deg \gcd(Q_n(x), (1 + x)^u + 1), \quad F_n(u) = 2^{g_n(u)}. \quad (5.1)$$

All polynomial gcds are monic gcds over $\mathbb{F}_2$.

Proposition 5.1 (A certificate of period diversity). *$F_n(u)$ is the number of periodic words whose ordinary period divides u , including zero. There is more than one nonzero ordinary period if and only if some u satisfies*

$$0 < g_n(u) < n - 1. \quad (5.2)$$

For such a certificate, exactly

$$2^{g_n(u)} - 1 \quad \text{and} \quad 2^{n-1} - 2^{g_n(u)} \quad (5.3)$$

nonzero periodic words have, respectively, period dividing u and period not dividing u . The corresponding full basins contain twice these numbers of words.

Proof. The fixed subspace of D^u is the kernel of multiplication by $(1+x)^u + 1$ on $\mathbb{F}_2[x]/Q_n$. For polynomials Q, f , this kernel has dimension $\deg \gcd(Q, f)$: writing $Q = gP$ and $f = gf_0$, with $g = \gcd(Q, f)$, the congruence $fv = 0 \pmod{Q}$ is equivalent to $P \mid v$, because P and f_0 are coprime. This proves the count.

A proper nonzero fixed subspace contains a nonzero point fixed by D^u and misses another, so those points cannot have equal periods. Conversely, if $a < b$ are two occurring periods, choose $u = a$. A period- a point is fixed and a period- b point is not, giving (5.2). Subtracting zero and the fixed-space size gives (5.3). The basin counts follow from (2.2). $\square$

The fixed subspace is invariant under R and D , and under their inverses on W_n . It is therefore a union of complete joint orbits. The certificate separates whole necklace components by the periods in their cores; it does not merely select unrelated words. This is a direct application of the partition structure. It needs no choice of a word in either part and no irreducible factorization of Q_n . The exponentiation in (5.1) can be reduced modulo Q_n throughout.

Theorem 5.2 (An explicit family of certificates). *Assume (3.1). For every positive integer k , put $h = \gcd(n, k)$ and take $Q_1 = 1$. Then*

$$\gcd(Q_n(x), (1+x)^{kB} + 1) = Q_h(x). \quad (5.4)$$

In particular, any divisor $1 < d < n$ gives a certificate $u = dB$ with $g_n(u) = d - 1$.

Proof. Equation (3.4) means $(1+x)^B = x^{-1} \pmod{Q_n}$. Since x is a unit modulo Q_n , the gcd in (5.4) equals $\gcd(Q_n, x^k + 1)$. The roots of Q_n are the nonidentity n th roots of unity. Among them, the roots of $x^k + 1$ are precisely the nonidentity h th roots. As Q_n is squarefree, the monic gcd is Q_h . $\square$

Thus the same arithmetic congruence yields both a separation theorem and a fully specified algebraic certificate. For a proper divisor d , the two groups of nonzero periodic words have sizes

$$2^{d-1} - 1 \quad \text{and} \quad 2^{n-1} - 2^{d-1}.$$

Only the first population has temporal period dividing dB .

5.1 Recovering exact periods

Let $E_n(u)$ be the number of periodic words of exact ordinary period u , with $E_n(1) = 1$. Möbius inversion gives

$$E_n(u) = \sum_{v|u} \mu(u/v) 2^{g_n(v)}. \quad (5.5)$$

There are $E_n(u)/u$ ordinary cycles of length u and, for $u > 1$, $2E_n(u)$ initial words with eventual period u . Under (3.1), each of these ordinary cycles yields one necklace component, with

$$d = \gcd(n, u), \quad t = u/d, \quad \text{component mass} = 2u. \quad (5.6)$$

Without that hypothesis, the ordinary cycles can be joined by rotation, and their number is not in general the number of necklace components.

For a known maximal period $P = \text{lcm}_i \lambda_i$, a finite refinement of the certificate criterion is

$$|\mathcal{S}(n)| = 1 \iff g_n(P/\ell) = 0 \text{ for every prime } \ell \mid P. \quad (5.7)$$

Indeed, every proper divisor of P divides P/ℓ for some prime $\ell \mid P$, while a point with full support attains period P . This criterion assumes that P is already known; it does not remove the arithmetic difficulty of determining it.

6 Two exact applications

6.1 A spatial separation at width nine

At $n = 9$, take $s = 3$, so $B = 7$. The factorization is

$$Q_9 = (x^2 + x + 1)(x^6 + x^3 + 1).$$

The second factor is irreducible because its roots have order 9 and $\text{ord}_9(2) = 6$. The orders of $1 + x$ modulo the two factors are 3 and 63, respectively. For the second, the order divides $2^6 - 1 = 63$; the two prime-divisor tests are

$$(1 + x)^{21} \equiv 1 + x^3, \quad (1 + x)^9 \equiv x^5 + x^2 + x \pmod{x^6 + x^3 + 1}.$$

Both residues differ from one, establishing exact order 63. Equation (2.8) therefore gives $\mathcal{S}(9) = \{3, 63\}$.

Spatial d	Ordinary τ	Necklace t	Core words	Components	Basin mass
1	1	1	1	1	2
3	3	1	3	1	6
9	63	7	252	4	504

Table 1: The complete partition at width nine, grouped by ordinary period. The first row is the zero core. Each component has one leaf per cycle vertex. The basin masses sum to 512.

The zero component and the period-3 component have the same unlabeled necklace graph: a loop with one leaf. Their masses differ, and only one has a nonzero periodic core. Graph shape alone would lose precisely the information needed for the conjecture.

Theorem 5.2 also gives the shorter certificate

$$\gcd(Q_9, (1 + x)^{21} + 1) = Q_3.$$

Its degree is two, so it separates three nonzero core words from the other 252, without first determining both exact periods.

6.2 An odd-order case with a complete census

The odd-order reduction leaves some genuine arithmetic work. For example, $n = 2047 = 23 \cdot 89$ satisfies the constant-degree condition with $\text{ord}_{2047}(2) = 11$: both prime factors have order 11. It is therefore not excluded by Theorem 4.2. The full-field structure of Mersenne widths gives a separate exact result.

Proposition 6.1 (Ordinary periods at Mersenne widths). *Let $n = 2^r - 1 > 1$. For every positive u ,*

$$g_n(u) = \gcd(n, u) - 1. \quad (6.1)$$

Consequently

$$\mathcal{S}(n) = \{d > 1 : d \mid n\}, \quad E_n(d) = \sum_{e \mid d} \mu(d/e) 2^{e-1} \quad (d \mid n). \quad (6.2)$$

In particular, Conjecture 1.1 holds at every Mersenne width.

Proof. The roots of Q_n are $\mathbb{F}_{2^r} \setminus \{0, 1\}$. Translation $\alpha \mapsto 1 + \alpha$ permutes this set. If $h = \gcd(n, u)$, exactly h elements of the cyclic group $\mathbb{F}_{2^r}^\times$ satisfy $\beta^u = 1$, and one is $\beta = 1$. There are therefore $h - 1$ common roots in (5.1). Squarefreeness proves (6.1).

The orders of the nonidentity elements of a cyclic group of order n are exactly its divisors greater than one. These are the local orders in (2.8); taking least common multiples adds no other values. This proves the spectrum. For $d \mid n$, substitute $g_n(e) = e - 1$ in (5.5). $\square$

For $d > 1$ dividing a Mersenne width, the number of ordinary cycles is

$$\frac{E_n(d)}{d} = \frac{1}{2d} \sum_{e \mid d} \mu(d/e) 2^e. \quad (6.3)$$

It is half the number of binary necklaces of length d with full spatial period. The equality follows from the usual Möbius count of primitive words; it is a numerical correspondence, not an identification of the two kinds of cycle.

At $n = 2047$, the complete nonzero census is

Ordinary period	Number of periodic words
23	$2^{22} - 1$
89	$2^{88} - 1$
2047	$2^{2046} - 2^{88} - 2^{22} + 1.$

(6.4)

Together with the zero word these counts sum to 2^{2046} ; doubling them accounts for all 2^{2047} starting words. Dividing each nonzero entry by its period counts ordinary cycles. These counts need not equal the numbers of necklace components; Theorem 3.1 does not apply here: $\text{ord}_{2047}(2)$ is odd, so no power of 2 is -1 modulo 2047.

The proportion of nonzero periodic words with period less than 2047 is exactly

$$\frac{2^{88} + 2^{22} - 2}{2^{2046} - 1}. \quad (6.5)$$

Thus very small classes can decide the conjecture even when nearly all core words have the maximal period. The exact partition detects both exceptional classes without relying on their frequency. For example, $u = 23$ gives $g_{2047}(23) = 22$, already a complete certificate of period diversity.

7 The remaining obstruction

The results leave a precise problem. A composite counterexample must satisfy the constant divisor-order condition (4.1), with common order r odd. This is a necessary condition, not a sufficient condition and not an assertion that any counterexample exists. Two further necessary bounds clarify what an algebraic obstruction would have to rule out.

Proposition 7.1. *If $\mathcal{S}(n) = \{T\}$ and $r = \text{ord}_n(2)$, then*

$$n \mid T \mid 2^r - 1, \quad n - 1 \leq \varphi(T), \quad (7.1)$$

where φ is Euler's totient function.

Proof. Every nonidentity n th root α belongs to $\mathbb{F}_{2^r}$, and $1 + \alpha$ has exact order T , giving $T \mid 2^r - 1$. Choose α of exact order n . Both $1 + \alpha$ and $1 + \alpha^{-1}$ have order T . Since $1 + \alpha^{-1} = \alpha^{-1}(1 + \alpha)$, raising to T gives $\alpha^T = 1$, hence $n \mid T$. Finally the $n - 1$ distinct elements $1 + \alpha$, with $\alpha^n = 1$ and $\alpha \neq 1$, all have order T . A cyclic group contains exactly $\varphi(T)$ elements of that order. $\square$

In particular $n - 1 > \varphi(2^r - 1)$ is another exclusion, since $T \mid 2^r - 1$ implies $\varphi(T) \leq \varphi(2^r - 1)$. More generally, the unresolved task can be expressed without listing any word:

For every odd composite n satisfying the constant divisor-order condition with odd common order, find a positive integer u for which $0 < \deg \gcd(Q_n, (1 + x)^u + 1) < n - 1$.

By Proposition 5.1, solving this remaining task would settle Conjecture 1.1. The hard part is a uniform argument that forces such a proper fixed subspace; a formula that tests a chosen u is not that argument.

There is also inheritance across widths. If $d > 1$ and $d \mid n$, repetition is an injective map $V_d \rightarrow V_n$ commuting with D , and it preserves exact ordinary periods, using the classical repetition construction [4, Theorem 5 and its proof]. Therefore

$$\mathcal{S}(d) \subseteq \mathcal{S}(n). \tag{7.2}$$

An exclusion at one divisor excludes every multiple. To investigate the remaining composites, one can first discard widths with an already excluded proper divisor, then seek a certificate in the residual cases. This inheritance does not assert that agreement at the prime divisors forces agreement at their product: additional polynomial factors appear at the larger width.

The application developed here is consequently a theorem and a reduction, rather than a general solution of the conjecture. The spatial structure of the necklace partition proves period diversity for an infinite arithmetic class and, through the degree condition, excludes all composite widths of even order. The fixed-space formulation supplies exact certificates and population counts beyond that class. It isolates the remaining difficulty as an interaction between addition and multiplicative order in finite fields, while preserving a disjoint accounting of every word of the power set.

References

- [1] *Consequences of Binary Necklaces*, companion manuscript.
- [2] *The Partitioning of Power Sets Into Graphs*, companion manuscript.
- [3] F. Breuer, E. Lötter, and B. van der Merwe, *Ducci-sequences and cyclotomic polynomials*, Finite Fields and Their Applications **13** (2007), no. 2, 293–304. doi:10.1016/j.ffa.2005.11.003.
- [4] A. Ehrlich, *Periods in Ducci’s n -number game of differences*, The Fibonacci Quarterly **28** (1990), no. 4, 302–305. Full text.
- [5] V. Shevelev, G. García-Pulgarín, J. M. Velásquez-Soto, and J. H. Castillo, *Overpseudoprimes, and Mersenne and Fermat numbers as primover numbers*, Journal of Integer Sequences **15** (2012), Article 12.7.7. Journal article.
- [6] The OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, entry A138004, contributed by T. D. Noe. oeis.org/A138004. The entry records the single-period primality conjecture; accessed 8 October 2026.