hexagon:2611.00031v2

The binary Collatz dynamics of the trinomials $x^n + x + 1$: an independent proof of two conjectures of Gallardo and Rahavandrainy

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

Version 2, 3 November 2026

Abstract

Gallardo and Rahavandrainy studied an analogue of the Collatz map on $\mathbb{F}_2[x]$, in which $x(x+1)$ plays the role of 2 and x^2+x+1 that of 3: an odd polynomial A is sent to the odd part of $1+(x^2+x+1)A$. They proved that every orbit reaches 1, and conjectured that the orbit of the trinomial x^n+x+1 has length 2^s+1, where s is the largest integer with $2^{s+1} < n$, and that for $1 \le t \le s-1$ it contains 2^t terms of the same degree. We prove both statements for every $n \ge 3$. They were proved earlier, with a complete Lean 4 formalization, by W. Choi; the proof given here was obtained independently. The proof rests on the identity $(x^2+x+1)+x(x+1)=1$: it reduces the dynamics to a map from one plateau to the next, characterises the last plateau of any orbit, and shows that along the orbit of x^n+x+1 the plateaus start at the 2^j-th powers of the odd parts of the polynomials $x^m(x^2+x+1)+1$, the index m following an explicit binary recursion. We also note that a later restatement of the conjecture, with a non-strict inequality, fails exactly when n is a power of 2. A script checks all the statements numerically.

1 Introduction

Throughout we work in $\mathbb{F}_2[x]$ and put

$$D = x(x+1) = x^2 + x, \qquad M = x^2 + x + 1, \qquad \text{so that} \qquad M + D = 1. \tag{1}$$

A polynomial A is *odd* if $\gcd(A, D) = 1$, that is, $A(0) = A(1) = 1$. For $B \neq 0$ we write $\mathrm{odd}(B)$ for B with all its factors x and $x+1$ removed. For odd A the Collatz step of Gallardo and Rahavandrainy [3] is

$$\mathrm{T}(A) = \mathrm{odd}(1 + MA).$$

In their notation $A_1 = \mathrm{odd}(A)$, $A_{2k} = 1 + MA_{2k-1}$ and $A_{2k+1} = \mathrm{odd}(A_{2k})$, so the *odd sequence* of an odd A is $A, \mathrm{T}(A), \mathrm{T}^2(A), \ldots$; they proved [3, Theorem 1.2] that it reaches 1, with length at most $2^{\deg A - 1}$. Its *length* ℓ_A is the number of its terms up to and including the first 1; this is the integer $\ell_A = m + 1$ of [3, Theorem 1.2], whose odd sequence is $[A_1, A_3, \ldots, A_{2m-1}, 1]$.

For the trinomials $T_n = x^n + x + 1$ they made two conjectures [3, Section 3.10]. Let s be the largest integer such that $n - 2^{s+1} \ge 1$.

- **Conjecture 3.12.** For every positive integer $t \le s-1$, the odd sequence of T_n contains 2^t polynomials which have the same degree d_t; in particular $d_1 = \deg A_5 = \deg A_7$ and $d_2 = \deg A_9 = \cdots = \deg A_{15}$.
- **Conjecture 3.13.** $\ell_{T_n} = 2^s + 1$.

The family is considered for $n \geq 2$; for $n = 2$ one gets $s = -1$, while $T_2 = M$ has length 2, so the conjectures are meaningful for $n \geq 3$. For $n \geq 3$ one has $s = k - 2$, where $k = \lceil \log_2 n \rceil$, since $2^{s+1} < n \leq 2^{s+2}$. We prove both conjectures for every $n \geq 3$.

Theorem 1. *Let $n \geq 3$ and $k = \lceil \log_2 n \rceil$. The odd sequence of $T_n = x^n + x + 1$ has length $2^{k-2} + 1$. If $n \geq 5$, it consists of T_n, then of $k - 2$ blocks $B_1, \ldots, B_{k-2}$, where B_j consists of exactly 2^{j-1} consecutive terms of the same degree δ_j, with $n > \delta_1 > \delta_2 > \cdots > \delta_{k-2}$, and finally of 1.*

Corollary 2. *Conjectures 3.12 and 3.13 of [3] hold for every $n \geq 3$.*

Proof. Theorem 1 with $s = k-2$ gives Conjecture 3.13. For $1 \leq t \leq s-1$ the block B_{t+1} consists of 2^t terms of degree δ_{t+1}, and no other term has this degree since the degrees $n, \delta_1, \delta_2, \ldots$ are distinct; this is Conjecture 3.12, with $d_t = \delta_{t+1}$. Moreover T_n and $B_1, \ldots, B_t$ have 2^t terms in all, so B_{t+1} occupies the positions $2^t + 1, \ldots, 2^{t+1}$ of the odd sequence, that is, it consists of $A_{2^{t+1}+1}, A_{2^{t+1}+3}, \ldots, A_{2^{t+2}-1}$; for $t = 1, 2$ these are A_5, A_7 and $A_9, \ldots, A_{15}$. □

The blocks are made explicit in Proposition 9: B_j starts with $V(m_j)^{2^{j-1}}$, where $V(m) = \mathrm{odd}(x^m M + 1)$, $m_1 = n - 3$, and m_{j+1} is obtained from m_j by a binary rule (Lemma 10). The last block starts from a power of one of the four polynomials $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^4 + x + 1$, $x^5 + x^3 + x^2 + x + 1$.

Section 2 contains three statements valid for every odd polynomial: the plateau lemma, the plateau-to-plateau map with a necessary and sufficient criterion for the orbit to end after a given plateau, and an infinite family of polynomials whose orbit is a single plateau. Section 3 treats the trinomials. In Section 4 we note that the restatement of Conjecture 3.13 as Conjecture 3.3 of [4], with a non-strict inequality, fails exactly at the powers of 2.

The polynomial analogue of the $3x + 1$ problem goes back to Hicks, Mullen, Yucas and Zavislak [5], who used the map sending f to f/x if $x \mid f$ and to $(x+1)f + 1$ otherwise; see also Nichols [6]. The variant studied here, with $x(x + 1)$ in the role of 2, is that of [3, 4].

Related work. After the first version of this note was written, we learned that W. Choi had made public on 14 October 2026 a proof of the same two statements, with a complete formalization in Lean 4 [1]. That work predates the present note. It also proves, for every nonzero A, the bound $\lfloor (\deg A)^2/4 \rfloor + 1$ on the length of the odd sequence, and that, for $n \geq 2$, the longest initial run of terms of degree n in the odd sequence of a polynomial of degree n has length $\lfloor n/2 \rfloor$; neither result is treated here. The proof given here was obtained independently; it follows a similar route, through the polynomials $x^m M + 1$ and their valuations at $x + 1$.

2 Three facts valid for every odd polynomial

For odd u we write $z = u + 1$, which is divisible by D, and

$$\mu(u) = \max\{t \geq 0 : \ D^t \mid u + 1\} \ \geq 1.$$

Since $D = x(x + 1)$ with x, $x + 1$ coprime, $\mu(u) = \min\big(v_x(u + 1), v_{x+1}(u + 1)\big)$, and $\mu(u^{2^e}) = 2^e \mu(u)$ because $u^{2^e} + 1 = (u + 1)^{2^e}$.

Lemma 3 (Plateau lemma)**.** *Let u be odd of degree at least 1, $z = u + 1$ and $\mu = \mu(u)$.*

(i) $\deg \mathrm{T}(u) \leq \deg u$*, with equality if and only if $\mu \geq 2$; in that case $\mathrm{T}(u) + 1 = Mz/D$ and $\mu(\mathrm{T}(u)) = \mu - 1$.*

(ii) Consequently $u, \mathrm{T}(u), \ldots, \mathrm{T}^{\mu-1}(u)$ all have degree $\deg u$, and $\deg \mathrm{T}^{\mu}(u) < \deg u$.

Proof. (i) Since $M+1=D$, we have $1+Mu=M(z+1)+1=Mz+D$. As $M(0)=M(1)=1$, the valuation of Mz at x is $v_x(z)\geq 1$, while $v_x(D)=1$. Hence $v_x(Mz+D)=1$ if $v_x(z)\geq 2$, and $v_x(Mz+D)\geq 2$ if $v_x(z)=1$; the same holds at $x+1$. Since $\deg(Mz+D)=\deg u+2$, the degree of $\mathrm{T}(u)=\mathrm{odd}(Mz+D)$ is $\deg u+2-v_x(Mz+D)-v_{x+1}(Mz+D)\leq \deg u$, with equality exactly when both valuations equal 1, that is, when $D^2\mid z$, that is, when $\mu\geq 2$. In that case $\mathrm{T}(u)=(Mz+D)/D=Mz/D+1$, so $\mathrm{T}(u)+1=Mz/D$, and $\mu(\mathrm{T}(u))=\mu-1$ because M is coprime to D.

(ii) follows by applying (i) μ times: the values of μ along $u,\mathrm{T}(u),\dots$ are $\mu,\mu-1,\dots,1$, and the step from the term with $\mu=1$ lowers the degree. □

We call $u,\mathrm{T}(u),\dots,\mathrm{T}^{\mu-1}(u)$ the *plateau* issued from u.

Lemma 4 (Plateau-to-plateau map)**.** *Let u be odd of degree at least 1, $\mu=\mu(u)$, and*

$$W=\frac{M^\mu(u+1)}{D^\mu}\in\mathbb{F}_2[x].$$

Then $\deg W=\deg u$, $\mathrm{T}^\mu(u)=\mathrm{odd}(W+1)$, *and*

$$\mathrm{T}^\mu(u)=1 \iff W+1=x^i(x+1)^j \text{ for some } i,j\geq 0.$$

Proof. By Lemma 3(i), $\mathrm{T}^t(u)+1=M^tz/D^t$ for $0\leq t\leq \mu-1$. For $w=\mathrm{T}^{\mu-1}(u)$ we get, as in the proof of Lemma 3,

$$1+Mw=M(w+1)+D=\frac{M^\mu z}{D^{\mu-1}}+D=D\,(W+1),$$

so $\mathrm{T}^\mu(u)=\mathrm{odd}(D(W+1))=\mathrm{odd}(W+1)$. The degree of W is $\deg u+2\mu-2\mu$; in particular $W+1\neq 0$. Finally $\mathrm{odd}(W+1)=1$ if and only if $W+1$ is a product of powers of x and $x+1$. □

In the terminology of [2], the orbit ends right after the plateau issued from u if and only if W is a Mersenne polynomial, the exponents i,j being allowed to vanish.

Proposition 5 (Single-plateau orbits)**.** *Let $i,j\geq 0$ with $(i,j)\neq(0,0)$ and $i\equiv j \pmod 3$. Then M divides $x^i(x+1)^j+1$, and the polynomial*

$$P_{i,j}=1+\frac{D\left(x^i(x+1)^j+1\right)}{M}$$

is odd of degree $i+j$. For every $e\geq 0$ the odd sequence of $P_{i,j}^{2^e}$ consists of 2^e terms of degree $2^e(i+j)$, followed by 1.

Proof. Let $\omega\in\mathbb{F}_4$ be a root of M; then $\omega+1=\omega^2$, so $\omega^i(\omega+1)^j+1=\omega^{i+2j}+1$, which vanishes since $i+2j\equiv i-j\equiv 0 \pmod 3$. The same holds for the conjugate root ω^2, so $M\mid E:=x^i(x+1)^j+1$. Clearly $P_{i,j}(0)=P_{i,j}(1)=1$ and $\deg P_{i,j}=2+(i+j)-2$. Since $(i,j)\neq(0,0)$, $\deg E=i+j$ and at least one of $E(0)$, $E(1)$ equals 1; as $P_{i,j}+1=DE/M$, we get $\mu(P_{i,j})=1+\min\big(v_x(E),v_{x+1}(E)\big)=1$. For $u=P_{i,j}^{2^e}$ we get $\mu(u)=2^e$ and $W=M^{2^e}(P_{i,j}+1)^{2^e}/D^{2^e}=E^{2^e}$, so $W+1=(E+1)^{2^e}=x^{i2^e}(x+1)^{j2^e}$. Lemmas 3 and 4 conclude. □

For instance $P_{1,1}=M$, $P_{3,0}=x^3+x+1$, $P_{0,3}=x^3+x^2+1$, $P_{2,2}=x^4+x+1$ and $P_{1,4}=x^5+x^3+x^2+x+1$.

3 The trinomials

For $m \geq 0$ put

$$F_m = x^m M + 1, \qquad V(m) = \mathrm{odd}(F_m).$$

Thus $F_0 = D$ and $V(0) = 1$.

Lemma 6 (First step)**.** *For $n \geq 3$, $\mu(T_n) = 1$ and $\mathrm{T}(T_n) = V(n-3)$.*

Proof. Here $z = T_n + 1 = x^n + x = x(x^{n-1}+1)$, so $v_x(z) = 1$ and $\mu(T_n) = 1$. Then $W = Mz/D = M(x^{n-1}+1)/(x+1)$ and, using $M + x + 1 = x^2$,

$$W + 1 = \frac{Mx^{n-1} + M + x + 1}{x+1} = \frac{Mx^{n-1} + x^2}{x+1} = \frac{x^2 F_{n-3}}{x+1}.$$

By Lemma 4, $\mathrm{T}(T_n) = \mathrm{odd}(W+1) = V(n-3)$. □

Lemma 7 (Valuations)**.** *For $m \geq 1$, $v_x(F_m) = 0$ and*

$$v_{x+1}(F_m) = 1,\ 3,\ 1,\ 2 \qquad \textit{according as} \qquad m \equiv 0,\ 1,\ 2,\ 3 \pmod 4.$$

Hence $\deg V(m) = m + 2 - v_{x+1}(F_m)$; in particular $\deg V(m) \leq m+1$, and $\deg V(m) \leq m$ if m is odd. Moreover $V(1) = 1$ and $\deg V(m) \geq 3$ for $m \geq 2$.

Proof. $F_m(0) = 1$ for $m \geq 1$. Put $y = x + 1$; then $M = y^2 + y + 1$ and

$$F_m = (1+y)^m(1+y+y^2) + 1 = (m+1)\,y + \Big(\tbinom{m}{2} + m + 1\Big)y^2 + \Big(\tbinom{m}{3} + \tbinom{m}{2} + m\Big)y^3 + O(y^4),$$

the coefficients being read modulo 2. If m is even, the coefficient of y is 1. If m is odd, it vanishes and the coefficient of y^2 is $\binom{m}{2}$, which by Lucas' theorem is odd if and only if the bit of weight 2 of m is 1, that is, $m \equiv 3 \pmod 4$. If $m \equiv 1 \pmod 4$, then $\binom{m}{2}$ and $\binom{m}{3}$ are even, again by Lucas, and the coefficient of y^3 is $m \equiv 1$. The degree formula follows from $\deg F_m = m+2$. Finally $F_1 = x^3+x^2+x+1 = (x+1)^3$, and for $m \geq 2$ the bound $v_{x+1}(F_m) \leq 3$ gives $\deg V(m) \geq m - 1 \geq 3$ when $m \geq 4$, while $\deg V(2) = \deg V(3) = 3$. □

Lemma 8 (Renormalisation)**.** *For $m \geq 2$ define*

$$m' = \begin{cases} m/2 - 1 & m \textit{ even}, \\ (m-3)/2 & m \equiv 1 \pmod 4, \\ (m-1)/2 & m \equiv 3 \pmod 4. \end{cases}$$

Then $m' \geq 0$, $\mathrm{T}(V(m)) = V(m')^2$, and $\mu(V(m)) = 1$.

Proof. Note $m' \geq 0$ ($m \equiv 1 \pmod 4$ and $m \geq 2$ force $m \geq 5$). Write $b = v_{x+1}(F_m)$, so $V(m) = F_m/(x+1)^b$ by Lemma 7, and

$$MV(m) + 1 = \frac{MF_m + (x+1)^b}{(x+1)^b} = \frac{M^2 x^m + M + (x+1)^b}{(x+1)^b}.$$

In characteristic 2 one has $M + (x+1) = x^2$, $M + (x+1)^2 = x$ and $M + (x+1)^3 = x^3$. Hence, with $b = 1, 3, 2$ in the three cases of the definition of m',

$$MV(m) + 1 = \frac{x^2\big(M^2 x^{m-2} + 1\big)}{x+1}, \qquad \frac{x^3\big(M^2 x^{m-3} + 1\big)}{(x+1)^3}, \qquad \frac{x\big(M^2 x^{m-1} + 1\big)}{(x+1)^2},$$

and in each case $M^2 x^{2m'} + 1 = (Mx^{m'} + 1)^2 = F_{m'}^2$. Taking odd parts, $\mathrm{T}(V(m)) = \mathrm{odd}(F_{m'})^2 = V(m')^2$.

For the last assertion, by Lemma 3(i) it suffices to show $\deg \mathrm{T}(V(m)) < \deg V(m)$, that is, $2\deg V(m') < \deg V(m)$. If m is even, $2\deg V(m') \le 2(m'+1) = m < m+1 = \deg V(m)$ (for $m'=0$, $V(0)=1$). If m is odd, then m' is odd, since $m-3 \equiv 2 \pmod 4$ when $m \equiv 1$ and $m-1 \equiv 2 \pmod 4$ when $m \equiv 3 \pmod 4$; hence $\deg V(m') \le m'$ by Lemma 7, and $2\deg V(m') \le m-3 < m-1 = \deg V(m)$ if $m \equiv 1 \pmod 4$, $2\deg V(m') \le m-1 < m = \deg V(m)$ if $m \equiv 3 \pmod 4$. □

Proposition 9 (Frobenius induction)**.** *Let $m \ge 2$, $e \ge 0$ and $u = V(m)^{2^e}$. Then $\mu(u) = 2^e$ and $\mathrm{T}^{2^e}(u) = V(m')^{2^{e+1}}$.*

Proof. By Lemma 8, $\mu(u) = 2^e \mu(V(m)) = 2^e$. Put $H = M(V(m)+1)/D$; then $W = M^{2^e}(u+1)/D^{2^e} = H^{2^e}$ and $W+1 = (H+1)^{2^e}$. By (1),

$$H+1 = \frac{M(V(m)+1)+D}{D} = \frac{MV(m)+1}{D},$$

so $\mathrm{odd}(H+1) = \mathrm{T}(V(m)) = V(m')^2$ by Lemma 8. By Lemma 4, $\mathrm{T}^{2^e}(u) = \mathrm{odd}(W+1) = \mathrm{odd}(H+1)^{2^e} = V(m')^{2^{e+1}}$. □

Lemma 10 (A binary recursion)**.** *For $m \ge 2$ put $N = m+2$ and $N' = m'+2$. Then N' is obtained from N by deleting its two lowest binary digits $b_1 b_0$ and appending the digit $b_1 \vee b_0$:*

$$N' = 2\lfloor N/4 \rfloor + (b_0 \vee b_1).$$

In particular, if N has $L \ge 3$ binary digits then N' has $L-1$, and after $t \le L-2$ iterations the value has digits $b_{L-1} \dots b_{t+1}\,(b_t \vee \cdots \vee b_0)$.

Proof. If m is even, N is even, $b_0 = 0$, and $N' = m/2+1 = N/2 = 2\lfloor N/4 \rfloor + b_1$. If $m \equiv 1 \pmod 4$, then $N = 4q+3$ and $N' = (m+1)/2 = 2q+1$. If $m \equiv 3 \pmod 4$, then $N = 4q+1$ and $N' = (m+3)/2 = 2q+1$. The other assertions follow by induction. □

Proof of Theorem 1. If $n \in \{3,4\}$, then $T_3 = P_{3,0}$ and $T_4 = P_{2,2}$, so $\ell_{T_n} = 2 = 2^{k-2}+1$ by Proposition 5.

Let $n \ge 5$, so $m_1 = n-3 \ge 2$, and define $m_{j+1} = m_j'$ as long as $m_j \ge 2$. Put $N_j = m_j + 2$. Since $2^{k-1} < n \le 2^k$, the integer $N_1 = n-1$ has exactly k binary digits, and by Lemma 10 N_j has $k-j+1$ digits. Hence $m_j \ge 2$ (i.e. $N_j \ge 4$) exactly for $1 \le j \le k-2$, and $m_{k-1} \in \{0,1\}$, so $V(m_{k-1}) = 1$.

By Lemma 6 the odd sequence starts with T_n, a plateau of length 1, followed by $V(m_1)$. By Proposition 9 and induction on j, for $1 \le j \le k-2$ the term following T_n and the blocks $B_1, \dots, B_{j-1}$ is $V(m_j)^{2^{j-1}}$, and the plateau issued from it, B_j, has exactly 2^{j-1} terms; the term after B_{k-2} is $V(m_{k-1})^{2^{k-2}} = 1$. By Lemma 3(ii) the degree drops strictly after T_n and after each block. The length is $1 + (1 + 2 + \cdots + 2^{k-3}) + 1 = 2^{k-2}+1$. □

Remark 11 (The last block). The last block starts from $V(m_{k-2})^{2^{k-3}}$, where $N_{k-2} = m_{k-2}+2$ has the three digits $1\,b_{k-2}\,(b_{k-3} \vee \cdots \vee b_0)$ of $n-1 = \sum b_i 2^i$. Thus $V(m_{k-2})$ is $V(2) = x^3+x+1$, $V(3) = x^3+x^2+1$, $V(4) = x^5+x^3+x^2+x+1$ or $V(5) = x^4+x+1$ according as $N_{k-2} = 4,5,6,7$; these are $P_{3,0}$, $P_{0,3}$, $P_{1,4}$ and $P_{2,2}$ of Proposition 5. For example, $n = 33$ gives $m = 30, 14, 6, 2$ and x^3+x+1.

4 A remark on the restatement in the 2025 paper

In the arXiv version of [4], Conjecture 3.13 of [3] is restated as Conjecture 3.3, for both the even and the odd sequences of $A = x^n + x + 1$, $n \ge 4$, with s the greatest positive integer such that $n - 2^{s+1} \ge 0$. With this non-strict inequality the predicted length $2^s + 1$ differs from the

true length $2^{k-2}+1$ exactly when n is a power of 2: for $n = 2^k$ it predicts $2^{k-1}+1$. Thus it fails for $n = 4$ and $n = 8$ (predicting 3 and 5 instead of 2 and 3), and for instance, for $n = 32$ the length is 9, as in the table of [4], whereas the restated formula gives 17. The original statement of [3], with the strict inequality $n - 2^{s+1} \geq 1$, is the one proved here.

5 Verification

The ancillary file `verify_collatz_binary.py` (Python 3, no dependency) recomputes, by exact arithmetic on bit-encoded polynomials, the identities used above and the statements of Lemmas 3–10, Propositions 5 and 9 and Theorem 1 on the ranges it prints (for instance the length formula for $3 \leq n \leq 1199$, and the blocks and the last block for $5 \leq n \leq 699$), and the comparison of Section 4 for $4 \leq n \leq 2099$. It runs in less than two minutes. These computations check the statements; the proofs above do not depend on them.

Acknowledgements. Technical assistance: Claude (Anthropic).

References

[1] W. Choi, *Exact lengths and a quadratic bound for a Collatz variant over binary polynomials*, preprint, Zenodo, 2026, doi:10.5281/zenodo.23356586; Lean 4 formalization: `https://github.com/coo001/binpoly-collatz-lean`.

[2] L. H. Gallardo and O. Rahavandrainy, *On Mersenne polynomials over* $\mathbb{F}_2$, Finite Fields Appl. **59** (2019), 284–296.

[3] L. H. Gallardo and O. Rahavandrainy, *On Collatz conjecture for binary polynomials*, arXiv:2308.01181, 2023.

[4] L. H. Gallardo and O. Rahavandrainy, *A variant of Collatz's conjecture over binary polynomials*, arXiv:2510.07530, 2025; Rev. Un. Mat. Argentina **69** (2026), no. 1, 295–302, doi:10.33044/revuma.5555.

[5] K. Hicks, G. L. Mullen, J. L. Yucas and R. Zavislak, *A polynomial analogue of the* $3N + 1$ *problem*, Amer. Math. Monthly **115** (2008), no. 7, 615–622.

[6] D. Nichols, *Analogues of the* $3x + 1$ *problem in polynomial rings of characteristic* 2, Experiment. Math., doi:10.1080/10586458.2016.1227734; arXiv:1610.02545.