ITERATED DICKSON POLYNOMIALS OVER FINITE FIELDS: WHEN THE EVENTUAL PERIOD IS k AND WHEN IT IS $k/2$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $D_n(x,\alpha)$ be the Dickson polynomial of the first kind over $\mathbb{F}_q$ and let $D_{n,\alpha}$ be the self-map of $\mathbb{F}_q$ it induces. Under the hypothesis $\alpha^n = \alpha$, which makes $D_{n,\alpha}^m = D_{n^m,\alpha}$, Chen and Peng (arXiv:2508.08621v3) compare the exact period k of the integer sequence $n^m \bmod \pi_q(\alpha)$ with the exact period κ of the iterates $D_{n,\alpha}^m$, prove $\kappa = k$ when k is odd, observe that $\kappa \in \{k, k/2\}$ when k is even, and ask for a criterion separating the two cases. We give one. Let π_2 be the largest divisor of $\pi_q(\alpha)$ coprime to n, so that k is the order of n modulo π_2, and let $K_\alpha \subseteq (\mathbb{Z}/\pi_2\mathbb{Z})^\times$ be $\{1, q\}$ if $\alpha \neq 1$ and $\{\pm 1, \pm q\}$ if $\alpha = 1$. Then $\kappa = k/|\langle n\rangle \cap K_\alpha|$; in particular $\kappa = k/2$ exactly when k is even and the involution $n^{k/2}$ lies in K_α. The proof runs on the classical double cover $u \mapsto u + \alpha/u$ and on a splitting lemma for cosets of finite subgroups; the group-theoretic core is formalised in Lean 4 for arbitrary commutative groups, and the criterion is verified exhaustively for every admissible pair at the seventeen prime powers $3 \le q \le 32$ inside Lean and at all seventy prime powers $q \le 256$ by an independent program. Two by-products: Corollary 4.3(1) of Chen–Peng is printed with its condition inverted, and the two branches of their question are counted at eleven fields. At $\alpha = 1$ the criterion recovers what Qureshi and Panario's description of Chebyshev dynamics already gives; the new content is $\alpha \neq 1$ in the non-permutation range $\gcd(n, q^2 - 1) > 1$.

1. Introduction

Let $q = p^e$ be a prime power and $\alpha \in \mathbb{F}_q^\times$. The *Dickson polynomials of the first kind* are defined by $D_0(x,\alpha) = 2$, $D_1(x,\alpha) = x$ and

$$D_m(x,\alpha) = x\, D_{m-1}(x,\alpha) - \alpha\, D_{m-2}(x,\alpha) \qquad (m \ge 2), \tag{1}$$

and are characterised by the functional equation

$$D_n\big(u + \alpha/u,\ \alpha\big) = u^n + \alpha^n/u^n. \tag{2}$$

Read modulo $x^q - x$, $D_n(\cdot,\alpha)$ is a function $\mathbb{F}_q \to \mathbb{F}_q$, which we write $D_{n,\alpha}$. Chen and Peng [1] study these functions from two angles. First, as the *index* varies: their Theorem 1.1 determines the exact period $\pi_q(\alpha)$ of the sequence $[D_n(x,\alpha) \bmod (x^q - x)]_{n\ge 1}$. Second, under the standing hypothesis $\alpha^n = \alpha$ of their Section 4, which is what makes the composition law $D_m \circ D_n = D_{mn}$ available and hence $D_{n,\alpha}^m = D_{n^m,\alpha}$, they study the *iteration* of a single map $D_{n,\alpha}$. Two pairs of integers are compared: (l, k), the exact tail length and exact period of the integer sequence $[n^m \bmod \pi_q(\alpha)]_m$, and (λ, κ), the exact tail length and exact period of the sequence of functions $[D_{n,\alpha}^m]_m$ — equivalently, as they note in their Section 1, the maximal preperiod and the least common multiple of the cycle lengths of the functional graph of $D_{n,\alpha}$ on $\mathbb{F}_q$. (Chen and Peng write these as script letters; we write λ, κ throughout, and transliterate accordingly when quoting them.) Their Lemma 4.4

proves $\lambda = l$ and their Proposition 4.5 proves that k odd forces $\kappa = k$. Then, verbatim from the compiled version 3 (p. 12):

> When k is even, we sometimes observe $\kappa = k$ and sometimes $\kappa = \frac{k}{2}$. At present, we do not have a complete criterion distinguishing these two cases. We therefore leave the following question open.
>
> **Question.** When k is even, under what conditions do we have $\kappa = k$ versus $\kappa = \frac{k}{2}$?

This paper answers the Question. Write $\pi = \pi_q(\alpha)$, let π_2 be the largest divisor of π coprime to n (so that k is the multiplicative order of n modulo π_2), and put, inside $(\mathbb{Z}/\pi_2\mathbb{Z})^\times$,

$$K_\alpha = \begin{cases} \{1,\, q\} & \text{if } \alpha \neq 1, \\ \{1,\, -1,\, q,\, -q\} & \text{if } \alpha = 1. \end{cases} \tag{3}$$

Since $\pi_2 \mid q^2 - 1$, every element of K_α squares to 1, so K_α is a subgroup of exponent dividing 2.

Theorem 1.1 (the criterion; Theorem 5.4)**.** *Let q be a prime power, $\alpha \in \mathbb{F}_q^\times$ and $n \geq 1$ with $\alpha^n = \alpha$. Then*

$$\kappa = \frac{k}{|\langle n \rangle \cap K_\alpha|}, \qquad \text{the intersection taken inside } (\mathbb{Z}/\pi_2\mathbb{Z})^\times.$$

Consequently $\kappa \in \{k, k/2\}$; $\kappa = k/2$ if and only if k is even and the unique involution $n^{k/2}$ of the cyclic group $\langle n \rangle$ lies in K_α; and $\kappa = k$ whenever k is odd.

The statement has three layers of support, and we keep them apart throughout.

1. *Proved, for all q.* Section 5 proves Theorem 1.1 by lifting $D_{n,\alpha}$ to the power map $u \mapsto u^n$ on the double cover $\mathbb{F}_q^\times \cup \{u \in \mathbb{F}_{q^2}^\times : u^{q+1} = \alpha\}$ of $\mathbb{F}_q$, identifying the periodic points, and applying a *splitting lemma*: on a coset of a finite subgroup, if s is coprime to the subgroup's order then the two ways a point can be fixed ($u^s = u$ or $u^s = \alpha/u$) cannot be mixed. That lemma is what turns the observed dichotomy into a theorem. Everything after the reduction to the cover is pure group theory, and that part — Theorems 4.1–4.4 — is stated for arbitrary commutative groups and is machine-checked. The reduction itself (Lemmas 5.1–5.3) is proved on paper only.
2. *Certified exhaustively, $q \leq 32$.* Theorem 6.1 verifies the criterion for every α and every admissible n at the seventeen prime powers $3 \leq q \leq 32$, by direct computation inside the proof assistant (by the kernel itself at $q = 3, 4, 5$).
3. *Computed, $q \leq 256$.* An independent C program verifies the same statements for all 4,385,984 admissible pairs (α, n) at all seventy prime powers $2 \leq q \leq 256$, with zero violations (Remark 6.2). These runs are reported, not certified.

Two by-products of the same computations concern the source itself. Corollary 4.3(1) of [1] states the answer in the permutation case $\gcd(n, q^2 - 1) = 1$ with its condition printed the wrong way round; two kernel-checked witnesses over $\mathbb{F}_5$ pin the inversion in both directions (Section 7). And since [1] prints no data for its Question, we tabulate how its two branches split at eleven fields (Theorem 6.3).

What is new and what is not. At $\alpha = 1$ one has $D_n(x, 1) = 2T_n(x/2)$ for odd q, so the functional graph of $D_{n,1}$ is that of a Chebyshev polynomial, and Qureshi and Panario [2] — a paper [1] cites, as its reference [19] — describe that graph

completely for arbitrary n. The $\alpha = 1$ case of Theorem 1.1 is the least common multiple of their per-point periods, and Theorem 8.1 checks that agreement inside the proof assistant rather than asserting it. In the permutation case, Lidl and Mullen [3] treat $\alpha = \pm 1$ and Corollary 4.3(1) of [1] treats every α. None of these reaches $\alpha \neq 1$ with $\gcd(n, q^2 - 1) > 1$, which is precisely the regime the Question is posed in, and κ does depend on α there: over $\mathbb{F}_{13}$ with $n = 3$ the two *squares* $\alpha = 1$ and $\alpha = -1$ share $\pi_{13}(\alpha) = 84$ and give $\kappa = 3$ and $\kappa = 6$ (Theorem 8.1). The technique — the double cover, the splitting of $q^2 - 1$ into its n-part and n-coprime part — is classical and we claim no novelty for it; what we claim is the formula $\kappa = k/|\langle n \rangle \cap K_\alpha|$, valid in all four regimes, and its proof.

Every theorem below that is machine-checked is stated and proved in Lean 4 against Mathlib; the exact statements are reproduced in Appendix A and the verification method is described in Section 9.

On the authorship of [1]. The arXiv metadata of 2508.08621 lists the authors as Wayne Peng and Yen-Ju Chen; the title page of the compiled version 3 lists "Yen-Ju, Chen" (National Taiwan Normal University) first and "Wayne, Peng" (National Central University) second. We cite the paper by its title page.

2. Notation and the objects

2.1. **The cover.** Fix q and $\alpha \in \mathbb{F}_q^\times$, and let $r = \mathrm{ord}(\alpha)$ be the multiplicative order of α. Inside $\mathbb{F}_{q^2}^\times$ put

$$U = \mathbb{F}_q^\times, \qquad V = V_\alpha = \{u \in \mathbb{F}_{q^2}^\times : u^{q+1} = \alpha\}, \qquad W = U \cup V,$$

and define $\varphi_\alpha(u) = u + \alpha/u$ and $\iota(u) = \alpha/u$. Chen and Peng write $\varphi_\alpha^{-1}(\mathbb{F}_q)$ for W and prove (their Lemma 2.5) that it equals $U \cup V$; their diagram (2) expresses $D_{n,\alpha}$ as the quotient of $u \mapsto u^n$ by φ_α when $\alpha^n = \alpha$. We re-prove what we use in Lemma 5.1.

2.2. **The index period.**

> **Theorem 1.1** [1, p. 2]. Let q be a prime power and let $\alpha \in \mathbb{F}_q^\times$. The period of the sequence $[D_n(x, \alpha) \pmod{x^q - x}]_{n \geq 1}$ is $\frac{q^2-1}{2}$ if q is odd and α is a square in $\mathbb{F}_q$, and is $q^2 - 1$ otherwise.

We write $\pi = \pi_q(\alpha)$ for this period, as [1] does. It is re-derived from the definition in Theorem 3.1 at nine fields, and used once in the proof of Theorem 5.4 (Lemma 5.3).

2.3. **The standing hypothesis and the two dynamical structures.** Chen and Peng, Section 4, verbatim: "For a periodic sequence $[a_n]_{n \geq 1}$, we say that the sequence has exact tail length λ and exact period κ if both integers are the smallest integers such that $a_{\lambda+\kappa} = a_\lambda$. We call the pair (λ, κ) the dynamical structure of the sequence." And: "We assume n and α satisfy $\alpha^n = \alpha$ in this section." The hypothesis $\alpha^n = \alpha$, i.e. $r \mid n - 1$, is in force in everything that follows. It is load-bearing: without it the composition law fails, $D_{n,\alpha}^m \neq D_{n^m,\alpha}$, and the dichotomy $\kappa \in \{k, k/2\}$ is false already over $\mathbb{F}_5$ (Proposition 6.5(i)).

For $n \geq 1$ with $\alpha^n = \alpha$, (l, k) denotes the dynamical structure of $[n^m \bmod \pi]_{m \geq 0}$ (their Section 4.2), and (λ, κ) that of $[D_{n,\alpha}^m]_{m \geq 0}$, the composition iterates read modulo $x^q - x$. Their Section 1 says of the latter: "λ is the maximal preperiodic length among all points of $\mathbb{F}_q$, and κ is the least common multiple of the cycle

lengths in the functional graph of $D_{n,\alpha}$." Both readings of κ are the same number, and both equal

$$\kappa = \min\{t \geq 1 : D_{n,\alpha}^t \text{ is the identity on } \Omega\}, \qquad \Omega = \bigcap_{m \geq 0} D_{n,\alpha}^m(\mathbb{F}_q), \tag{4}$$

the set of periodic points: $D_{n,\alpha}$ restricted to Ω is a bijection whose orbits are the cycles of the functional graph, and $D^{\lambda+t} = D^\lambda$ as functions exactly when D^t is the identity on $D^\lambda(\mathbb{F}_q) = \Omega$.

2.4. **The n-part and the kernel classes.** For a positive integer M write $M = M^{(n)}M_{(n)}$, where $M^{(n)}$ is the largest divisor of M supported on the primes dividing n and $M_{(n)} = M/M^{(n)}$ is coprime to n; the decomposition is multiplicative in M. Put

$$\pi_1 = \pi^{(n)}, \qquad \pi_2 = \pi_{(n)}, \qquad k = \operatorname{ord}_{\pi_2}(n), \qquad l = \min\{m \geq 0 : \pi_1 \mid n^m\}.$$

This (l, k) is the dynamical structure of $[n^m \bmod \pi]_m$: modulo π_2 the sequence is purely periodic of period $\operatorname{ord}_{\pi_2}(n)$, modulo π_1 it is 0 from index l on and never before, and $n^{m+k} \equiv n^m \pmod{\pi_1}$ with $m < l$ would force $\pi_1 \mid n^m$ because $\gcd(n^k - 1, \pi_1) = 1$. The set K_α is (3), a subgroup of $(\mathbb{Z}/\pi_2\mathbb{Z})^\times$ of exponent dividing 2 (for $\alpha = 1$ closure uses $(-1)(-q) = q$).

2.5. **Where the classes come from.** Two classical identities explain K_α. *Frobenius:* by (2), $D_q(u + \alpha/u, \alpha) = u^q + \alpha^q u^{-q} = (u + \alpha/u)^q$, and a q-th power is the identity on $\mathbb{F}_q$, so $D_q(x, \alpha) \equiv x \pmod{x^q - x}$; by the composition law, $D_{qm}(\cdot, \alpha) = D_q(D_m(\cdot, \alpha), \alpha^m) = D_m(\cdot, \alpha)$ whenever $\alpha^m = \alpha$. *Negation at $\alpha = 1$:* $D_{-m}(u + 1/u, 1) = u^{-m} + u^m = D_m(u + 1/u, 1)$. These give the classes q, and at $\alpha = 1$ also -1 and $-q$. That there are no others is, in the permutation range, Lemma 4.2 of [1]; in general it is Theorem 5.4.

3. The statements of the source, certified

Nothing in this section is new mathematics; it is the source's own results and printed numbers, re-derived from the recurrence (1) and the definitions alone. We record it because the later theorems rest on the same definitions and the same code, and because two readings of the source were found to be wrong along the way (Section 7, and the Table 3b caption below).

In the proof assistant a finite field is presented as $\mathbb{F}_p[X]/(f)$ for a monic f of degree e, elements are base-p digit vectors, and every sweep statement carries as its first conjunct a check that the presented ring has no zero divisors — which certifies at once that p is prime and f irreducible. The presentations used are $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$, $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$, $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$, $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$, $\mathbb{F}_{25} = \mathbb{F}_5[X]/(X^2 + 2)$, $\mathbb{F}_{27} = \mathbb{F}_3[X]/(X^3 + 2X + 1)$, $\mathbb{F}_{32} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$, and $\mathbb{F}_p$ for the primes. In the statements below, "admissible (α, n)" means $\alpha \in \mathbb{F}_q^\times$, $1 \leq n \leq \pi_q(\alpha)$ and $\alpha^n = \alpha$; the range $n \leq \pi$ is no loss, since $D_{n+\pi}(\cdot, \alpha) = D_n(\cdot, \alpha)$ and $\alpha^n = \alpha$, $\gcd(n, q^2 - 1)$, π_2, k and κ all depend on n only through $n \bmod \pi$ (note $r \mid \pi$, and for odd q every prime dividing $q^2 - 1$ divides $(q^2 - 1)/2$).

Theorem 3.1 (Theorem 1.1 of [1], recomputed)**.** *For $q \in \{3, 4, 5, 7, 8, 9, 11, 13, 16\}$ and every $\alpha \in \mathbb{F}_q^\times$, the exact period of $[D_n(\cdot, \alpha)]_{n \geq 1}$ as functions on $\mathbb{F}_q$ — computed*

as the least $t \geq 1$ with $(D_{1+t}, D_{2+t}) = (D_1, D_2)$, which suffices because the two-term recurrence (1) *is invertible for $\alpha \neq 0$ — equals $\pi_q(\alpha)$ as given by Theorem 1.1.*

Theorem 3.2 (the Frobenius identity)**.** *For $q \in \{3, 4, 5, 7, 8, 9\}$ and every $\alpha \in \mathbb{F}_q^\times$, $D_q(x, \alpha) \equiv x \pmod{x^q - x}$.*

Theorem 3.2 is the classical identity of §2.5, certified as a finite check; it is not claimed here as a general theorem.

Theorem 3.3 (Section 4 of [1], verified)**.** *For each of the seventeen prime powers $q \in \{3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32\}$ and every admissible (α, n): $\lambda = l$ (Lemma 4.4 of* [1]*); if k is odd then $\kappa = k$ (Proposition 4.5); and if k is even then $\kappa \in \{k, k/2\}$ (the dichotomy the Question presupposes). At $q = 3, 4, 5$ the verification is by the kernel of the proof assistant alone; at the other fourteen fields it is by compiled evaluation.*

Altogether 13,866 admissible pairs are covered — a count made outside the proof assistant, which certifies each sweep but does not report its size.

Theorem 3.4 (the printed tables of [1])**.** *The source prints numbers in exactly five places, all in its Section 5 and all over $\mathbb{F}_{11}$: Table 1a (the coefficients of $x^2, x^4, \ldots, x^{120}$ in $D_{120}(x, -1)$, sixty cells in ten columns), Table 1b (the same cells of $3D_{120}(x, 2)$), Table 2 (Table 1a re-laid in eleven columns with the first cell blank), Table 3a (the coefficients of $x^{60}, x^{58}, \ldots, x^2$ in $D_{60}(x, 1)$, thirty cells) and Table 3b (the coefficients of $x^{59}, \ldots, x^1$ in $2D_{61}(x, 9)$). Recomputed from* (1) *alone, every cell of all five blocks agrees with the print, and Table 3a is the reversal of Table 3b (the 180° rotation the source's Section 5 is about).*

Remark 3.5. The prose of [1] introducing Table 3 says that Table 3b lists the coefficients of $D_{61}(x, 9)$, while the sub-caption reads $2D_{61}(x, 9)$. Only the doubled reading matches the printed cells; the sub-caption is the correct one. This is a caption slip, not a mathematical error.

4. The group-theoretic core

Everything in this section is stated for an arbitrary commutative group (or monoid) and is machine-checked with no computation involved; the finite-field dictionary that connects it to $D_{n,\alpha}$ is Section 5. Throughout, G is a commutative group written multiplicatively and u^z for $z \in \mathbb{Z}$ is the integer power.

Theorem 4.1 (splitting lemma)**.** *Let $H \leq G$ be a finite subgroup, $w, \beta_1, \beta_2 \in G$, and let $s \in \mathbb{Z}$ be coprime to $|H|$. Suppose that every element of the coset wH satisfies*

$$(wh)^{s-1} = \beta_1 \qquad \text{or} \qquad (wh)^{s+1} = \beta_2.$$

Then one of the two alternatives holds for every element of wH.

Proof. Suppose not, and pick $a, b \in H$ with $(wa)^{s-1} \neq \beta_1$ and $(wb)^{s+1} \neq \beta_2$; then $(wa)^{s+1} = \beta_2$ and $(wb)^{s-1} = \beta_1$. *(i)* Let $K_1 = \{h \in H : h^{s-1} = 1\}$ and $K_2 = \{h \in H : h^{s+1} = 1\}$. If $\kappa \in K_1$ then $(wa\kappa)^{s-1} = (wa)^{s-1} \neq \beta_1$, so $(wa\kappa)^{s+1} = \beta_2 = (wa)^{s+1}$ and $\kappa^{s+1} = 1$; symmetrically (with b) $K_2 \subseteq K_1$. So $K_1 = K_2 =: K$, and every $\kappa \in K$ satisfies $\kappa^2 = \kappa^{(s+1)-(s-1)} = 1$. *(ii)* For $h \in H$: if $(wh)^{s-1} = \beta_1 = (wb)^{s-1}$ then $h/b \in K_1 = K$ and $h^2 = b^2$; otherwise $(wh)^{s+1} = \beta_2 = (wa)^{s+1}$, $h/a \in K$ and $h^2 = a^2$. So every square in H is a^2

or b^2. *(iii)* Put $x = a/b \in H$. Applying (ii) to x, x^2, x^3, the three elements x^2, x^4, x^6 lie in the two-element set $\{a^2, b^2\}$, so two of them coincide, and each coincidence gives $x^2 = 1$ or $x^4 = 1$; hence $x^4 = 1$. *(iv)* $x^{s-1} = (wa)^{s-1}/\beta_1 \neq 1$ and $x^{s+1} = \beta_2/(wb)^{s+1} \neq 1$, so $x \neq 1$ and $\mathrm{ord}(x) \in \{2, 4\}$. Then $|H|$ is even, so s is odd by coprimality, so $4 \mid s-1$ or $4 \mid s+1$, and $x^4 = 1$ makes the corresponding power of x equal to 1 — a contradiction. □

Theorem 4.2 (the Ω-criterion)**.** *Let $P, R \leq G$ be finite subgroups, $w \in G$, $Q, s \in \mathbb{Z}$ and $E \in \mathbb{N}$. Assume $u^{Q-1} = 1$ for all $u \in P$, $h^{Q+1} = 1$ for all $h \in R$, that s is coprime to $|P|$ and to $|R|$, and that E generates the annihilator of $P \cup wR$, i.e. for every $z \in \mathbb{Z}$,*

$$E \mid z \iff \big(u^z = 1 \ \forall u \in P\big) \wedge \big(h^z = 1 \ \forall h \in R\big) \wedge w^z = 1.$$

Then the following are equivalent:

1. *every $u \in P$ satisfies $u^{s-1} = 1$ or $u^{s+1} = w^{Q+1}$, and every $h \in R$ satisfies $(wh)^{s-1} = 1$ or $(wh)^{s+1} = w^{Q+1}$;*
2. *$E \mid s-1$, or $E \mid s-Q$, or ($w^{Q+1} = 1$ and ($E \mid s+1$ or $E \mid s+Q$)).*

Proof. (1)⇒(2). Apply Theorem 4.1 to $H = P$ with w replaced by 1, $\beta_1 = 1$, $\beta_2 = w^{Q+1}$, and to $H = R$ with the given w and the same β_i. On the P side one of (A) $u^{s-1} = 1$ on P or (B) $u^{s+1} = w^{Q+1}$ on P holds throughout; (B) at $u = 1$ forces $w^{Q+1} = 1$, and then $u^{s+1} = 1$ on P. On the R side one of (A′) $(wh)^{s-1} = 1$ on R, i.e. $w^{s-1} = 1$ and $h^{s-1} = 1$ on R, or (B′) $(wh)^{s+1} = w^{Q+1}$ on R, i.e. $w^{s+1} = w^{Q+1}$ and $h^{s+1} = 1$ on R, holds throughout. Using $u^{Q-1} = 1$ on P and $h^{Q+1} = 1$ on R: (A)∧(A′) gives that $s-1$ annihilates P, R and w, so $E \mid s-1$; (A)∧(B′) gives the same for $s-Q$; (B)∧(A′) gives $w^{Q+1} = 1$ and $E \mid s+Q$; (B)∧(B′) gives $w^{Q+1} = 1$ and $E \mid s+1$. (2)⇒(1) is the same bookkeeping read backwards: for instance $E \mid s-Q$ gives $u^{s-1} = u^{s-Q}u^{Q-1} = 1$ on P and $(wh)^{s+1} = (wh)^{s-Q}(wh)^{Q+1} = w^{Q+1}$ on wR. □

In the application P and R are the n-coprime parts of μ_{q-1} and μ_{q+1}, $w^{Q+1} = \alpha$ with $Q = q$, $E = \pi_2$, and condition (2) is exactly $s \in K_\alpha$ modulo π_2. Lemma 4.2 of [1] is the case $P = \mu_{q-1}$, $R = \mu_{q+1}$ of the theorem; the point of the general form is that it applies to the periodic points alone.

Theorem 4.3 (the dichotomy)**.** *Let M be a commutative monoid, $x \in M$, and $S \subseteq M$ a set containing 1, closed under multiplication, and with $y^2 = 1$ for all $y \in S$. Let d be the least $t \geq 1$ with $x^t \in S$ (assumed to exist) and let k be the order of x. Then x has finite order, $d \mid k$ and $k \mid 2d$; moreover $2d = k$ if and only if k is even and $x^{k/2} \in S$, and one of $d = k$, $2d = k$ holds.*

Proof. $x^{dm} \in S$ for all $m \geq 0$ by closure, and $x^{2d} = (x^d)^2 = 1$, so x has finite order k dividing $2d$. Write $k = d\lfloor k/d \rfloor + \rho$ with $0 \leq \rho < d$; then $x^\rho = x^k \, (x^{d\lfloor k/d \rfloor})^{-1} \in S$ (using $y^{-1} = y$ on S), so minimality of d forces $\rho = 0$. Thus $k = dm$ with $m \mid 2$. If $m = 2$ then k is even and $x^{k/2} = x^d \in S$; if $m = 1$ and k were even with $x^{k/2} \in S$, then $k/2 < d$ would contradict minimality. □

Theorem 4.4 (the criterion, assembled)**.** *In the setting of Theorem 4.2 assume moreover $E \neq 0$ and $w^{Q+1} \in P$, let $n \in \mathbb{Z}$ be coprime to $|P|$, $|R|$ and E, and let d be the least $t \geq 1$ such that every $u \in P$ satisfies $u^{n^t-1} = 1$ or $u^{n^t+1} = w^{Q+1}$ and*

every $h \in R$ satisfies $(wh)^{n^t-1} = 1$ or $(wh)^{n^t+1} = w^{Q+1}$. Let k be the order of $\bar{n}$ in $\mathbb{Z}/E\mathbb{Z}$ and

$$K = \{1, \bar{Q}\} \cup \big(\{-1, -\bar{Q}\} \text{ if } w^{Q+1} = 1\big) \subseteq \mathbb{Z}/E\mathbb{Z}.$$

Then $d \mid k$, $k \mid 2d$, and $2d = k$ if and only if k is even and $\bar{n}^{\,k/2} \in K$.

Proof. Since E annihilates P, R and w, and $w^{Q+1} \in P$, one gets $E \mid Q^2 - 1$, so $\bar{Q}^2 = 1$ and K is closed under multiplication with every element squaring to 1. By Theorem 4.2 applied to $s = n^t$ (coprime to $|P|$ and $|R|$), the fixing condition on t is equivalent to $\bar{n}^{\,t} \in K$. Now apply Theorem 4.3 to $x = \bar{n}$, which is a unit of $\mathbb{Z}/E\mathbb{Z}$ and so has finite order. □

Proposition 4.5 (controls)**.** (i) *Theorem 4.1 fails without the coprimality hypothesis: in the group of order two, with H the whole group, $s = 2$, $w = \beta_1 = 1$ and β_2 the non-trivial element, every element of H satisfies one of the two conditions and neither holds throughout.*

(ii) *Theorem 4.3 fails without the exponent-two hypothesis: in $\mathbb{Z}/7\mathbb{Z}$ with $S = \{1, 2, 4\}$ and $x = 3$, the least $t \geq 1$ with $x^t \in S$ is 2, the order of x is 6, and $6 \nmid 4$.*

(iii) *The hypothesis set of Theorem 4.4 is satisfiable and its halving branch is reachable: with G cyclic of order 3, P trivial, $R = G$, $w = 1$, $Q = 5$, $E = 3$, $n = 2$ (so $k = \mathrm{ord}_3(2) = 2$) every hypothesis is discharged and the theorem returns $d = 1 = k/2$. This is the smallest case in which the Dickson period actually halves, $q = 5$, $\alpha = 1$, $n = 2$ (Example 5.6).*

The verified statement of (iii) records the numerical conclusion ($\mathrm{ord}_3(2) = 2$, $1 \mid 2$, $2 \mid 2$, $2 \cdot 1 = 2$); its proof is the instantiation of Theorem 4.4 just described.

5. The criterion over $\mathbb{F}_q$

We now prove Theorem 1.1. This section is proved on paper; its group-theoretic content is Section 4, and the three lemmas below — the classical dictionary between $D_{n,\alpha}$ and the power map — are not part of the formal development.

Notation. $N = q^2 - 1$, $A = N_{(n)}$, $B = N^{(n)}$, $a = (q-1)_{(n)}$, $M_2 = (q+1)_{(n)}$, so $A = aM_2$. $G_2 \leq \mathbb{F}_{q^2}^{\times}$ is the subgroup of order A (the elements of order coprime to n), G_1 the subgroup of order B, so $\mathbb{F}_{q^2}^{\times} = G_1 \times G_2$; and $\mu_d = \{u : u^d = 1\}$ for $d \mid N$. Two facts:

(N1) $r = \mathrm{ord}(\alpha)$ divides a: $\alpha^{n-1} = 1$ gives $r \mid n-1$, coprime to n, and $r \mid q-1$. Hence $\alpha \in \mu_a \subseteq G_2$.

(N2) $\gcd(q+1, A) = M_2$: for a prime $\ell \nmid n$, $v_\ell(\gcd(q+1, A)) = \min(v_\ell(q+1), v_\ell(N)) = v_\ell(q+1) = v_\ell(M_2)$, and for $\ell \mid n$ both sides have $v_\ell = 0$.

Lemma 5.1 (the double cover)**.** *φ_α maps W onto $\mathbb{F}_q$, with fibres $\{u, \alpha/u\}$. The map $\psi(u) = u^n$ preserves U and V, commutes with ι, and $D_{n,\alpha}(\varphi_\alpha(u)) = \varphi_\alpha(u^n)$ for all $u \in W$.*

Proof. For $u \in U$ both u and α/u lie in $\mathbb{F}_q$. For $u \in V$, $u^q = \alpha/u$, so $\varphi_\alpha(u) = u + u^q = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(u) \in \mathbb{F}_q$. Since $u + \alpha/u - v - \alpha/v = (u-v)(1-\alpha/uv)$, $\varphi_\alpha(u) = \varphi_\alpha(v)$ on W iff $v \in \{u, \alpha/u\}$, and ι preserves W (as $(\alpha/u)^{q+1} = \alpha^2/\alpha$ for $u \in V$). The fixed points of ι on W are $U \cap V = \{u \in \mathbb{F}_q^{\times} : u^2 = \alpha\}$ (if $u \in V$ and $u^2 = \alpha$ then $u^{q-1} = 1$), and $|U| + |V| = (q-1) + (q+1) = 2q$, so ι has exactly $f + (2q - 2f)/2 = q$

orbits on W, $f = |U \cap V|$; hence $\varphi_\alpha(W) = \mathbb{F}_q$. Finally $(u^n)^{q+1} = \alpha^n = \alpha$, $\iota(u)^n = \alpha^n/u^n = \iota(u^n)$, and (2) with $\alpha^n = \alpha$ gives $D_{n,\alpha}(\varphi_\alpha(u)) = u^n + \alpha/u^n = \varphi_\alpha(u^n)$. □

Lemma 5.2 (the periodic set)**.** *Let $\Omega_W = \bigcap_{m\geq 0} \psi^m(W)$. Then $\Omega_W = \mu_a \cup V_2$ with $V_2 = \{v \in G_2 : v^{q+1} = \alpha\}$, and $V_2 = w\mu_{M_2}$ is a non-empty coset of $\mu_{M_2} \leq G_2$. Moreover $\Omega = \varphi_\alpha(\Omega_W)$, and*

$$\kappa = \min\{t \geq 1 : \ \forall u \in \mu_a \cup w\mu_{M_2},\ u^{n^t-1} = 1 \text{ or } u^{n^t+1} = \alpha\}. \tag{5}$$

Proof. On G_2 the map ψ is an automorphism; on G_1, ψ^m is trivial for m large. So for large m, $\psi^m(X) = \{x_2^{n^m} : x \in X\}$, x_2 the G_2-component of x. For $X = U$: $u^{q-1} = 1$ forces $u_2 \in G_2 \cap \mu_{q-1} = \mu_a$, and conversely every $v \in \mu_a$ is $(v^{n^{-m}})^{n^m}$ with $v^{n^{-m}} \in \mu_a \subseteq U$; so $\bigcap_m \psi^m(U) = \mu_a$. For $X = V$: $u^{q+1} = \alpha \in G_2$ (by N1) splits as $u_1^{q+1} = 1$, $u_2^{q+1} = \alpha$, and $V_2^n = V_2$ since $v \mapsto v^n$ is injective on G_2 and preserves the condition $v^{q+1} = \alpha$; so $\bigcap_m \psi^m(V) = V_2$. The norm $v \mapsto v^{q+1}$ maps G_2 into μ_a with kernel $G_2 \cap \mu_{q+1} = \mu_{M_2}$ by (N2), so its image has order $A/M_2 = a$ and is all of $\mu_a \ni \alpha$; thus V_2 is a coset $w\mu_{M_2}$. Since $\psi(W) \subseteq W$, the chain $\psi^m(W)$ decreases and is eventually constant, and $D_{n,\alpha}^m(\mathbb{F}_q) = \varphi_\alpha(\psi^m(W))$ by Lemma 5.1, whence $\Omega = \varphi_\alpha(\Omega_W)$. As Ω_W is ψ- and ι-stable, for $x = \varphi_\alpha(u)$ with $u \in \Omega_W$ we have $D_{n,\alpha}^t(x) = x$ iff $u^{n^t} \in \{u, \alpha/u\}$ (fibre description), and (5) follows from (4). □

Lemma 5.3 (the modulus)**.** *Let E be the exponent of the subgroup of G_2 generated by Ω_W. Then $E = \pi_2$.*

Proof. Let ζ generate G_2 and write $w = \zeta^i$. The subgroup generated by $\mu_a \cup w\mu_{M_2}$ contains $\mu_a = \langle \zeta^{M_2} \rangle$, $\mu_{M_2} = \langle \zeta^a \rangle$ (ratios of coset elements) and w, so it is $\langle \zeta^g \rangle$ with $g = \gcd(a, M_2, i)$, cyclic of order and exponent $E = A/g$. As $\gcd(a, M_2) \mid \gcd(q-1, q+1) \mid 2$, $g \in \{1, 2\}$. Now use Theorem 1.1 of [1] for π. *q even:* N is odd, $g = 1$, $E = A$, and $\pi = N$ gives $\pi_2 = A$. *q odd, n even:* a, M_2 are odd, so $g = 1$ and $E = A$; $r \mid n-1$ is odd, so $\alpha = (\alpha^{(r+1)/2})^2$ is a square and $\pi = N/2$; as $2 \mid n$ the prime 2 is absent from both $N_{(n)}$ and $(N/2)_{(n)}$, so $\pi_2 = A$. *q odd, n odd:* $\gcd(a, M_2) = 2$ and $g = \gcd(2, i)$. With ξ a generator of $\mathbb{F}_{q^2}^\times$, $\zeta = \xi^B$ and $\alpha = w^{q+1} = \xi^{Bi(q+1)}$, so α is a square in $\mathbb{F}_q$ iff $\alpha^{(q-1)/2} = 1$ iff $N \mid BiN/2$ iff $2 \mid i$ (B is odd since n is). If $2 \mid i$: $g = 2$, $E = A/2$, and $\pi = N/2$ gives $\pi_2 = N_{(n)}/2 = A/2$. If $2 \nmid i$: $g = 1$, $E = A$, and $\pi = N$ gives $\pi_2 = A$. □

Theorem 5.4 (the criterion; proved on paper, outside the formal development)**.** *Let q be a prime power, $\alpha \in \mathbb{F}_q^\times$, $n \geq 1$ with $\alpha^n = \alpha$, and let π_2, k, K_α be as in Section 2. Then $\kappa = k/|\langle n \rangle \cap K_\alpha|$ inside $(\mathbb{Z}/\pi_2\mathbb{Z})^\times$. Hence $\kappa \in \{k, k/2\}$, with $\kappa = k/2$ if and only if k is even and $n^{k/2} \in K_\alpha \pmod{\pi_2}$, and $\kappa = k$ if k is odd.*

Proof. Apply Theorem 4.4 with $G = \mathbb{F}_{q^2}^\times$, $P = \mu_a$, $R = \mu_{M_2}$, the w of Lemma 5.2, $Q = q$ and $E = \pi_2$. The hypotheses hold: $u^{q-1} = 1$ on μ_a since $a \mid q-1$; $h^{q+1} = 1$ on μ_{M_2} since $M_2 \mid q+1$; $w^{q+1} = \alpha \in \mu_a$; π_2 generates the annihilator of $\mu_a \cup w\mu_{M_2}$ by Lemma 5.3; and n is coprime to a, M_2, π_2 by construction. By (5), κ is the d of Theorem 4.4, k is the order of n modulo π_2, and K is K_α, the classes $-1, -q$ appearing exactly when $\alpha = w^{q+1} = 1$. Theorem 4.4 gives $\kappa \mid k$, $k \mid 2\kappa$, and $\kappa = k/2$ iff k is even and $n^{k/2} \in K_\alpha$. Finally, the set $T = \{t \in \mathbb{Z} : n^t \in K_\alpha\}$ is a subgroup of $\mathbb{Z}$ containing $k\mathbb{Z}$ whose image in $\mathbb{Z}/k\mathbb{Z} \cong \langle n \rangle$ is $\langle n \rangle \cap K_\alpha$; so $T = \kappa\mathbb{Z}$ with $\kappa = k/|\langle n \rangle \cap K_\alpha|$, and the intersection has order 1 or 2 because $\langle n \rangle$ is cyclic

and K_α has exponent dividing 2. A cyclic group of even order k has exactly one involution, $n^{k/2}$, and one of odd order has none. □

Corollary 5.5. (i) *(Proposition 4.5 of* [1]*) If k is odd then $\kappa = k$.*
(ii) *(the dichotomy) $\kappa \in \{k, k/2\}$ for every admissible (α, n).*
(iii) *(Corollary 4.3(1) of* [1]*, in the corrected form of Section 7) If* $\gcd(n, q^2-1) = 1$ *then $\pi_2 = \pi$ and the period of $D_{n,\alpha}$ is $k/2$ exactly when the kernel class (q, or for $\alpha = 1$ one of $-1, \pm q$) is a power of n modulo π, and k otherwise.*

Example 5.6. Over $\mathbb{F}_5$. ($\alpha = 1$, $n = 2$): $\pi = 12$, $\pi_1 = 4$, $\pi_2 = 3$, $k = \mathrm{ord}_3(2) = 2$, $n^{k/2} = 2 \equiv -1 \in K_1$, so $\kappa = 1 = k/2$. ($\alpha = 4$, $n = 3$): α is a square, $\pi = 12$, $\pi_1 = 3$, $\pi_2 = 4$, $k = \mathrm{ord}_4(3) = 2$, $n^{k/2} = 3 \equiv -1$, but $K_4 = \{1, 5 \bmod 4\} = \{1\}$, so $\kappa = 2 = k$. These are the two sides of the Question at the smallest field where both occur (Proposition 6.4). The witness of Theorem 8.1: over $\mathbb{F}_{13}$ with $n = 3$, $\pi_2 = 28$, $\langle 3\rangle = \{1, 3, 9, 27, 25, 19\}$; for $\alpha = 1$, $K_1 = \{1, 27, 13, 15\}$ meets $\langle 3\rangle$ in $\{1, 27\}$ and $\kappa = 3$, while for $\alpha = -1$, $K_{-1} = \{1, 13\}$ meets it trivially and $\kappa = 6$.

Remark 5.7. The direction "$n^{k/2} \in K_\alpha \Rightarrow \kappa \mid k/2$" has a two-line proof from the identities of §2.5 and Theorem 1.1 alone: with $\pi_1 \mid n^l$, $n^{l+k/2} \equiv \varepsilon n^l \pmod{\pi}$ for $\varepsilon = n^{k/2} \in K_\alpha$, and $D_{\varepsilon m} = D_m$ for $\varepsilon \in K_\alpha$ and $\alpha^m = \alpha$. The converse — nothing smaller works, and $\kappa = k$ when the involution misses K_α — is where the splitting lemma is needed, and it is what the source's Lemma 4.2 does not give outside the permutation range.

6. Exhaustive verification, and how the two branches split

Theorem 6.1 (the criterion, certified at seventeen fields)**.** *For each of the seventeen prime powers $q \in \{3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32\}$ (presented as in Section 3) and every admissible (α, n),*

$$\kappa = \frac{k}{|\langle n\rangle \cap K_\alpha|},$$

where κ is computed as the least common multiple of the cycle lengths of the functional graph of $D_{n,\alpha}$ built from (1)*, and the right-hand side as $k/2$ if k is even and $n^{k/2} \bmod \pi_2$ lies in K_α, else k. At $q = 3, 4, 5$ the check is performed by the kernel of the proof assistant; at the other fourteen fields by compiled evaluation.*

Theorems 3.3 and 6.1 are certified by the same seventeen Boolean statements, one per field: each asserts that the presented ring is a field and that, at every admissible pair, $\lambda = l$, the odd-k case gives $\kappa = k$, the even-k case gives $\kappa \in \{k, k/2\}$, and κ equals the criterion's prediction. The seventeen fields span both parities of the characteristic, prime and non-prime q, and square and non-square α.

Remark 6.2 (the external sweep). An independent C implementation (field arithmetic in $\mathbb{F}_p[X]/(f)$ with f found by an irreducibility search; functional graph by a colouring pass) checks Lemma 4.4, Proposition 4.5, the dichotomy, the criterion, and — at $q \le 32$ — Theorem 1.1, for all 4,385,984 admissible pairs at all seventy prime powers $2 \le q \le 256$ (2,096,688 pairs with $\gcd(n, q^2 - 1) > 1$ and 2,289,296 coprime ones), in 135 CPU-seconds, with zero violations of any of them. A third implementation, in Python, agrees with it on every quantity at every prime $q \le 43$. These are reported computations; nothing in this remark is certified.

Theorem 6.3 (how often the period halves)**.** *Over the admissible pairs (α, n) with $\gcd(n, q^2-1) > 1$ and k even, the pair $\big(\#\{\kappa = k/2\},\ \#\{\kappa = k\}\big)$ is*

q	3	4	5	7	8	9	11	13	16	17	19
$\#\{\kappa = k/2\}$	0	4	5	6	12	17	50	66	204	51	186
$\#\{\kappa = k\}$	0	0	1	8	0	7	32	32	16	69	108

(by the kernel at $q = 3, 4, 5$, by compiled evaluation at the other eight fields).

Chen and Peng print no data for their Question — their only tables are the coefficient blocks of Theorem 3.4 — so these values are new. Neither row is monotone in q: the split is governed by whether the Frobenius class q (and, at $\alpha = 1$, -1 and $-q$) lands in $\langle n \rangle$ modulo π_2, an arithmetic condition on q^2-1 rather than on the size of q. In the external sweep of Remark 6.2, the totals over all seventy prime powers $q \le 256$ are 661,371 halving and 1,151,089 non-halving pairs. Neither the sequence $0, 4, 5, 6, 12, 17, 50, 66, 204, 51, 186$ nor its segment $5, 6, 12, 17, 50, 66, 204$ was in the OEIS on 2026-09-03.

Proposition 6.4 (both answers occur, and $\mathbb{F}_5$ is minimal)**.** *Over $\mathbb{F}_5$ the split is $(5, 1)$. Hence neither "$\kappa = k$ always" nor "$\kappa = k/2$ whenever k is even" is the answer to the Question; and since $\mathbb{F}_3$ has no admissible pair with $\gcd(n, 8) > 1$ and k even, while $\mathbb{F}_4$ has only halving ones, $\mathbb{F}_5$ is the smallest field at which both branches occur.*

Over the eleven fields of Theorem 6.3, among the 874 admissible pairs with $\gcd(n, q^2-1) > 1$ and k even, the first reading fails at the 601 halving pairs and the second at the 273 others (the column sums of the certified table).

Proposition 6.5 (the hypotheses are load-bearing)**.**

(i) *Drop the standing hypothesis $\alpha^n = \alpha$: among the pairs (α, n) with $\alpha \in \mathbb{F}_q^\times$, $1 \le n \le \pi_q(\alpha)$, $\gcd(n, q^2-1) > 1$ and k even, the number with $\kappa \notin \{k, k/2\}$ is 2 over $\mathbb{F}_5$ and 9 over $\mathbb{F}_7$. (Under the hypothesis it is 0 at every field of Theorem 6.1.)*

(ii) *Use $K_\alpha = \{1, q\}$ at every α, i.e. drop the classes $-1, -q$ at $\alpha = 1$: the criterion then mispredicts κ at 3 admissible pairs over $\mathbb{F}_5$ and 6 over $\mathbb{F}_7$.*

(iii) *Replace $\pi_q(\alpha)$ by q^2-1 throughout, i.e. ignore the square case of Theorem 1.1: the criterion mispredicts at 2 admissible pairs over $\mathbb{F}_5$ and 10 over $\mathbb{F}_7$.*

(iv) *The field check refuses $\mathbb{F}_2[X]/(X^2+1)$, in which $X+1$ is a zero divisor; no sweep can run over a ring that is not a field.*

Control (i) is the trap a first reading of [1] falls into: the hypothesis is stated once, in the second paragraph of its Section 4. The external sweep continues the count of (i) to 157 over $\mathbb{F}_{11}$ and 408 over $\mathbb{F}_{13}$.

7. A correction to Corollary 4.3(1) of the source

Corollary 4.3 of [1], verbatim from the compiled version 3 (p. 10):

> **Corollary 4.3.** 1. Let $\alpha \in \mathbb{F}_q^\times$ satisfy $\alpha^n = \alpha$. The period of $D_{n,\alpha}(x) \pmod{x^q - x}$ is $\delta_{n,\alpha} k$, where k is the multiplicative order of n modulo $\pi_q(\alpha)$ with $\delta_{n,\alpha} = \frac{1}{2}$, if n and α satisfy the conditions we describe below, 1, otherwise. The condition is that when $\alpha = 1$, $-1, \pm q \notin \{n^i \pmod{q^2-1} \mid i = 1, 2, 3 \dots\}$, and that when $\alpha \neq 1$, $q \notin \{n^i \pmod{\pi_q(\alpha)} \mid i = 1, 2, 3 \dots\}$.

(The corollary sits in Section 4.1, "n is coprime to q^2-1".) Its proof reads "This naturally follows from Lemma 4.2", and Lemma 4.2 does give the corollary — with the condition the other way round.

Theorem 7.1 (the condition is inverted)**.** *Over $\mathbb{F}_5$ with $\alpha = 2$ (so $\pi_5(2) = 24$):*

- *(a) for $n = 5$: $k = \mathrm{ord}_{24}(5) = 2$, the period of $D_{5,2}$ under composition is $\kappa = 1$, and $q = 5$ is a power of n modulo 24; the printed condition gives $\delta_{n,\alpha} = 1$ and predicts period 2;*
- *(b) for $n = 13$: $k = \mathrm{ord}_{24}(13) = 2$, the period is $\kappa = 2$, and $q = 5$ is* not *a power of 13 modulo 24 ($\langle 13\rangle = \{13, 1\}$); the printed condition gives $\delta_{n,\alpha} = \frac{1}{2}$ and predicts period 1.*

Both are checked by the kernel of the proof assistant.

Since the printed rule fails in both directions, the defect is in the condition and not in an exponent: the period halves exactly when the kernel class *is* a power of n. Read that way, the corollary is Corollary 5.5(iii), and in the external sweep of Remark 6.2 it holds at all 2,289,296 coprime admissible pairs with $q \le 256$. Read exactly as printed, for $\alpha \neq 1$ the rule is wrong at every coprime admissible pair: when k is odd the cyclic group $\langle n\rangle$ has no involution, so $q \notin \langle n\rangle$ (as $q^2 \equiv 1$ and $q \not\equiv 1 \pmod{\pi}$) and the rule selects $\delta = \frac{1}{2}$, where δk is not an integer; when k is even its condition is the exact negation of the true one. (At $\alpha = 1$ the printed modulus is q^2-1 rather than $\pi_q(1) = (q^2-1)/2$ for odd q, and there the printed rule can agree with the true period by accident.) The two $k = 2$ witnesses above are the informative ones.

The same condition is printed in version 1 of [1] (35 pages) as Corollary 5.3(1): "The condition is that when $\alpha = 1$, $-1, \pm q \notin \{n^i \bmod q^2-1 \mid i = 1, 2, 3\dots\}$, and that when $\alpha \neq 1$, $q \notin \{n^i \bmod \pi(\alpha) \mid i = 1, 2, 3\dots\}$." It has thus survived two revisions. Version 3 (3 July 2026) is the latest, its arXiv comment reads "18 pages, under revision", no journal reference is recorded, and the arXiv listing carries no erratum. This is a correction to a printed statement, not to the mathematics behind it.

8. The case $\alpha = 1$, and what is prior

For odd q, $D_n(x, 1) = 2T_n(x/2)$ with T_n the Chebyshev polynomial, so the functional graph of $D_{n,1}$ on $\mathbb{F}_q$ is conjugate (by $x \mapsto 2x$) to that of T_n. Qureshi and Panario [2] describe the latter completely, for arbitrary n (their abstract: "We completely describe the functional graph associated to iterations of Chebyshev polynomials over finite fields"). Their preliminaries define, for $\gcd(n, d) = 1$, $o_d(n)$ and $\tilde{o}_d(n)$ as the orders of n in $(\mathbb{Z}/d\mathbb{Z})^\times$ and in $(\mathbb{Z}/d\mathbb{Z})^\times/\{\pm 1\}$, note that $\tilde{o}_d(n) = o_d(n)/2$ if $-1 \in \langle n\rangle$ and $o_d(n)$ otherwise, and write $m = \nu\omega$ with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(\omega, n) = 1$ (the n-decomposition, the same device as $\pi_1\pi_2$ here). Their proposition on periods reads, verbatim from the preprint: "Let $a \in \mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2}$ such that $a = \alpha + \alpha^{-1}$ and $\mathrm{ord}(\alpha) = ud$ the n-decomposition of the (multiplicative) order of α. Then $\mathrm{per}(a) = \tilde{o}_d(n)$ and $\mathrm{pper}(a) = \min\{k \ge 0 : u \mid n^k\}$." This is a *per-point* period; the least common multiple is never taken there. Aggregating over the orders realised in $\mathbb{F}_q^\times \cup \mu_{q+1}$ gives, with $\omega_0 = (q-1)_{(n)}$ and $\omega_1 = (q+1)_{(n)}$,

$$\text{lcm of the cycle lengths of } T_n \text{ on } \mathbb{F}_q = \mathrm{lcm}_{\,d\mid\omega_0 \text{ or } d\mid\omega_1}\, \tilde{o}_d(n). \tag{6}$$

Theorem 8.1 (the $\alpha = 1$ case is Qureshi–Panario's; α matters)**.** (i) *For every odd prime $q \le 19$ and every n with $1 \le n \le \pi_q(1)$, the κ of $D_{n,1}$ on $\mathbb{F}_q$, computed from the Dickson table, equals the right-hand side of* (6) *computed from the Qureshi–Panario formula and nothing else (by the kernel at $q = 3, 5, 7$, by compiled evaluation at $q = 11, 13, 17, 19$).*

(ii) *κ is not a function of (q, n) alone: over $\mathbb{F}_{13}$ with $n = 3$, the two squares $\alpha = 1$ and $\alpha = 12 = -1$ share $\pi_{13}(\alpha) = 84$ and give $\kappa = 3$ and $\kappa = 6$ respectively (by the kernel).*

Part (i) is the attribution boundary of Theorem 5.4, made checkable: at $\alpha = 1$ the criterion recovers known results by a known method, and [1] cites [2] (as [19], for the sentence "Qureshi and Panario completely described the functional graphs of Chebyshev polynomials over finite fields …") without connecting it to its own Question. Part (ii) is why the $\alpha \neq 1$ content cannot be obtained by conjugating the Chebyshev case. Beyond $\alpha = 1$ the located prior work is confined to the permutation case: Lidl and Mullen [3] give the cycle lengths of $D_n(x, 1)$ (their Theorem 2: a cycle of length m exists iff $q - 1$ or $q + 1$ has a divisor t with $n^m \equiv \pm 1 \pmod t$) and of $D_n(x, -1)$ for n, q odd (Theorem 3), for Dickson *permutation* polynomials, and note that these are closed under composition only for $\alpha \in \{0, \pm 1\}$; by the Chinese remainder theorem the least common multiple in their Theorem 2 is $\min\{m : n^m \in \{\pm 1, \pm q\} \pmod{q^2 - 1}\}$, the $\alpha = 1$ permutation case of Theorem 5.4. Charpin, Mesnager and Sarkar [4] prove in characteristic 2 that $D_k(x) \equiv x \pmod{x^{2^m} + x}$ exactly for $k \in \{1, 2^m, 2^{2m} - 2^m - 1, 2^{2m} - 2\}$ (Corollary 1 of the ePrint version, Corollary 1.1 of the HAL copy hal-01237332), which is $K_1 = \{1, q, -q, -1\}$ with $q = 2^m$; they present it as an instance of Theorem 3.8 of the monograph of Lidl, Mullen and Turnwald [5]. That monograph is reference [9] of [1], cited there ("see [5, 9, 11, 22]") for the standard properties of Dickson polynomials. No copy of it was available for this paper, so whether its Theorem 3.8 covers general α is left open here; if it does, Theorem 1.1 and Lemma 4.2 of [1] and the set K_α are classical, which would still not reach the iteration criterion outside the permutation range. The $\mathbb{Z}/n\mathbb{Z}$ analogue of the group of Dickson permutation functions is studied by Peña and Ortíz [6], with the same modulus $(p^2 - 1)/2$ appearing; it contains no iteration statement. None of these sources reaches $\alpha \neq 1$ with $\gcd(n, q^2 - 1) > 1$.

9. Verification

Every theorem of Sections 3, 4, 6–8 is stated and proved in Lean 4 against Mathlib [8, 7]; the exact statements are reproduced verbatim in Appendix A, and the repository reference is to be added at submission. Theorem 5.4 and Lemmas 5.1–5.3 are proved on paper only. Two kinds of formal statement occur. The group-theoretic theorems of Section 4 are ordinary Mathlib proofs over an arbitrary `CommGroup` (or `CommMonoid`); `#print axioms`, run on 2026-09-03, reports for each of the eight declarations exactly the three standard axioms `propext`, `Classical.choice`, `Quot.sound`. The finite-field statements are Boolean computations over a self-contained module that imports nothing (finite-field arithmetic on digit vectors, Dickson tables packed one byte per point, the functional graph, Floyd's cycle detection for (l, k), and the criterion), so that the small cases are affordable to the kernel's own `decide`: at $q = 3, 4, 5$ (the sweeps, Theorem 1.1, the Frobenius identity and the counts), for all six table statements, for the field control and the two witnesses of Theorem 7.1, and for parts of Theorem 8.1, `#print axioms` reports `[propext]`

alone. Every other finite-field statement — the fourteen sweeps at $7 \le q \le 32$, Theorem 1.1 at $7 \le q \le 16$, the Frobenius identity at $q = 7, 8, 9$, the counts at $7 \le q \le 19$, controls (i)–(iii) of Proposition 6.5, and part (i) of Theorem 8.1 at $q = 11, 13, 17, 19$ — is proved by `native_decide`, i.e. by evaluating the same Boolean with the compiled evaluator, and carries in addition the axiom `Lean.ofReduceBool` (printed as `<decl>._native.native_decide.ax_1_1`). The kernel/native boundary is a cost boundary only: the module holding the ten kernel theorems at $q \le 5$ (the sweeps, Theorem 1.1 and the Frobenius identity at $q = 3, 4, 5$, and the $\mathbb{F}_5$ counts) elaborates by `decide` in 12.5 CPU-seconds, while a file holding the $q = 7, 8, 9$ sweeps together with Theorem 1.1 at $q = 7$, all by `decide`, did not finish in two minutes (which of the four is the wall was not isolated). No `sorry` and no added axiom occur anywhere. The C and Python sweeps of Remark 6.2 are outside the formal development.

Appendix A. The Lean statements

The statements below are quoted verbatim from the development (proofs omitted; each is `:= by decide`, `:= by native_decide`, or a Mathlib tactic proof). All live in the namespace `LeanProblemSpec.DicksonEvenk`. `prime p` is $\mathbb{F}_p$; `f4`, `f8`, `f9`, `f16`, `f25`, `f27`, `f32` are the presentations of Section 3; `sweepOK F` is the Boolean of Theorems 3.3 and 6.1; `thm11OK`, `frobeniusOK`, `halfFullCounts` are those of Theorems 3.1, 3.2, 6.3; `noHypBad`, `badNoPM`, `badFullPi` count the failures in Proposition 6.5(i)–(iii); `cor43Data F α n` returns $(k, \kappa, [q \in \langle n \rangle \bmod \pi_q(\alpha)])$; `dpoly p α n` is the coefficient list of $D_n(x, \alpha)$ over $\mathbb{F}_p$ from (1); `qpAgrees` compares κ with (6); `kPair F α n` is (κ at α, κ at 1); and `kernelClasses E Q alphaOne` is the set K of Theorem 4.4.

Theorems 3.3 and 6.1 (kernel at $q = 3, 4, 5$).

```
theorem sweep_q3 : sweepOK (prime 3) = true
theorem sweep_q4 : sweepOK f4 = true
theorem sweep_q5 : sweepOK (prime 5) = true
theorem sweep_q7 : sweepOK (prime 7) = true
theorem sweep_q8 : sweepOK f8 = true
theorem sweep_q9 : sweepOK f9 = true
theorem sweep_q11 : sweepOK (prime 11) = true
theorem sweep_q13 : sweepOK (prime 13) = true
theorem sweep_q16 : sweepOK f16 = true
theorem sweep_q17 : sweepOK (prime 17) = true
theorem sweep_q19 : sweepOK (prime 19) = true
theorem sweep_q23 : sweepOK (prime 23) = true
theorem sweep_q25 : sweepOK f25 = true
theorem sweep_q27 : sweepOK f27 = true
theorem sweep_q29 : sweepOK (prime 29) = true
theorem sweep_q31 : sweepOK (prime 31) = true
theorem sweep_q32 : sweepOK f32 = true
```

Theorem 3.1 (kernel at $q = 3, 4, 5$) and Theorem 3.2 (kernel at $q = 3, 4, 5$).

```
theorem thm11_q3 : thm11OK (prime 3) = true
theorem thm11_q4 : thm11OK f4 = true
theorem thm11_q5 : thm11OK (prime 5) = true
theorem thm11_q7 : thm11OK (prime 7) = true
theorem thm11_q8 : thm11OK f8 = true
theorem thm11_q9 : thm11OK f9 = true
theorem thm11_q11 : thm11OK (prime 11) = true
theorem thm11_q13 : thm11OK (prime 13) = true
theorem thm11_q16 : thm11OK f16 = true
theorem frob_q3 : frobeniusOK (prime 3) = true
theorem frob_q4 : frobeniusOK f4 = true
theorem frob_q5 : frobeniusOK (prime 5) = true
theorem frob_q7 : frobeniusOK (prime 7) = true
theorem frob_q8 : frobeniusOK f8 = true
theorem frob_q9 : frobeniusOK f9 = true
```

Theorem 6.3 and Proposition 6.4 (kernel at $q = 3, 4, 5$).

```
theorem counts_q3 : halfFullCounts (prime 3) = (0, 0)
theorem counts_q4 : halfFullCounts f4 = (4, 0)
theorem counts_q5 : halfFullCounts (prime 5) = (5, 1)
theorem counts_q7 : halfFullCounts (prime 7) = (6, 8)
theorem counts_q8 : halfFullCounts f8 = (12, 0)
theorem counts_q9 : halfFullCounts f9 = (17, 7)
theorem counts_q11 : halfFullCounts (prime 11) = (50, 32)
theorem counts_q13 : halfFullCounts (prime 13) = (66, 32)
theorem counts_q16 : halfFullCounts f16 = (204, 16)
theorem counts_q17 : halfFullCounts (prime 17) = (51, 69)
theorem counts_q19 : halfFullCounts (prime 19) = (186, 108)
```

Proposition 6.5 (native for the first three, kernel for the fourth) and Theorem 7.1 (kernel).

```
theorem hypothesis_is_needed : noHypBad (prime 5) = 2 ∧ noHypBad (prime 7) = 9
theorem kernel_needs_plus_minus : badNoPM (prime 5) = 3 ∧ badNoPM (prime 7) = 6
theorem pi_needs_the_square_case : badFullPi (prime 5) = 2 ∧ badFullPi (prime 7) = 10
theorem notAField : (Fld.mk 2 [1, 0]).isField = false
theorem cor43_erratum_halved : cor43Data (prime 5) 2 5 = (2, 1, true)
theorem cor43_erratum_full : cor43Data (prime 5) 2 13 = (2, 2, false)
```

Theorem 3.4 (kernel).

```
theorem table1a : pick (dpoly 11 10 120) 2 2 60 =
    [3, 6, 2, 10, 1, 6, 0, 0, 0, 0,
     8, 1, 2, 8, 7, 4, 2, 0, 0, 0,
     0, 4, 6, 1, 4, 9, 2, 1, 0, 0,
     0, 0, 1, 7, 3, 1, 5, 6, 3, 0,
     0, 0, 0, 7, 5, 10, 7, 2, 9, 10,
     0, 0, 0, 0, 2, 3, 6, 2, 10, 1]
theorem table1b : (pick (dpoly 11 2 120) 2 2 60).map (fun v => 3 * v % 11) =
    [1, 10, 2, 6, 3, 2, 0, 0, 0, 0,
     10, 9, 2, 7, 10, 5, 7, 0, 0, 0,
     0, 3, 6, 5, 1, 3, 7, 1, 0, 0,
     0, 0, 1, 2, 9, 4, 1, 6, 4, 0,
     0, 0, 0, 2, 4, 7, 8, 2, 1, 8,
     0, 0, 0, 0, 6, 1, 10, 2, 6, 3]
theorem table2 :
    (pick (dpoly 11 10 120) 2 2 60).take 10 = [3, 6, 2, 10, 1, 6, 0, 0, 0, 0] ∧
    ((pick (dpoly 11 10 120) 2 2 60).drop 10).take 11 = [8, 1, 2, 8, 7, 4, 2, 0, 0, 0, 0] ∧
    ((pick (dpoly 11 10 120) 2 2 60).drop 54) = [2, 3, 6, 2, 10, 1]
theorem table3a : pickDown (dpoly 11 1 60) 60 2 30 =
    [1, 6, 5, 0, 0,
     10, 6, 2, 2, 0,
     0, 7, 9, 2, 0,
     0, 3, 4, 5, 5,
     0, 0, 3, 7, 4,
     0, 0, 10, 6, 2]
theorem table3b : (pickDown (dpoly 11 9 61) 59 2 30).map (fun v => 2 * v % 11) =
    [2, 6, 10, 0, 0,
     4, 7, 3, 0, 0,
     5, 5, 4, 3, 0,
     0, 2, 9, 7, 0,
     0, 2, 2, 6, 10,
     0, 0, 5, 6, 1]
theorem table3_is_a_rotation :
    pickDown (dpoly 11 1 60) 60 2 30 =
      ((pickDown (dpoly 11 9 61) 59 2 30).map (fun v => 2 * v % 11)).reverse
```

Theorem 8.1 (kernel for the first and third).

```
theorem qp_agrees_small :
    qpAgrees (prime 3) = true ∧ qpAgrees (prime 5) = true ∧ qpAgrees (prime 7) = true
theorem qp_agrees_larger :
    qpAgrees (prime 11) = true ∧ qpAgrees (prime 13) = true ∧
      qpAgrees (prime 17) = true ∧ qpAgrees (prime 19) = true
theorem alpha_matters :
    kPair (prime 13) 12 3 = (6, 3) ∧ piq (prime 13) 12 = 84 ∧ piq (prime 13) 1 = 84 ∧
      isSquareIn (prime 13) 12 = true
```

Theorems 4.1–4.4 and Proposition 4.5 (Mathlib proofs; `variable {G : Type*} [CommGroup G], {M : Type*} [CommMonoid M]`).

```
theorem coset_split (H : Subgroup G) [Finite H] (s : ℤ)
    (hs : IsCoprime s (Nat.card H : ℤ)) (w β₁ β₂ : G)
    (hcov : ∀ h ∈ H, (w * h) ^ (s - 1) = β₁ ∨ (w * h) ^ (s + 1) = β₂) :
    (∀ h ∈ H, (w * h) ^ (s - 1) = β₁) ∨ (∀ h ∈ H, (w * h) ^ (s + 1) = β₂)
theorem omega_criterion (P R : Subgroup G) [Finite P] [Finite R] (w : G) (Q s : ℤ) (E : ℕ)
    (hP : ∀ u ∈ P, u ^ (Q - 1) = 1) (hR : ∀ h ∈ R, h ^ (Q + 1) = 1)
    (hE : ∀ z : ℤ, ((E : ℤ) ∣ z ↔
      ((∀ u ∈ P, u ^ z = 1) ∧ (∀ h ∈ R, h ^ z = 1) ∧ w ^ z = 1)))
    (hsP : IsCoprime s (Nat.card P : ℤ)) (hsR : IsCoprime s (Nat.card R : ℤ)) :
    ((∀ u ∈ P, u ^ (s - 1) = 1 ∨ u ^ (s + 1) = w ^ (Q + 1)) ∧
     (∀ h ∈ R, (w * h) ^ (s - 1) = 1 ∨ (w * h) ^ (s + 1) = w ^ (Q + 1)))
    ↔ ((E : ℤ) ∣ s - 1 ∨ (E : ℤ) ∣ s - Q ∨
       (w ^ (Q + 1) = 1 ∧ ((E : ℤ) ∣ s + 1 ∨ (E : ℤ) ∣ s + Q)))
theorem period_dvd (x : M) (S : Set M) (hS1 : (1 : M) ∈ S)
    (hmul : ∀ y ∈ S, ∀ z ∈ S, y * z ∈ S) (hsq : ∀ y ∈ S, y * y = 1)
    (d : ℕ) (hd : IsLeast {t : ℕ | 0 < t ∧ x ^ t ∈ S} d) :
    d ∣ orderOf x ∧ orderOf x ∣ 2 * d
theorem period_halves_iff (x : M) (S : Set M) (hS1 : (1 : M) ∈ S)
    (hmul : ∀ y ∈ S, ∀ z ∈ S, y * z ∈ S) (hsq : ∀ y ∈ S, y * y = 1)
    (d : ℕ) (hd : IsLeast {t : ℕ | 0 < t ∧ x ^ t ∈ S} d) (hne : orderOf x ≠ 0) :
    (2 * d = orderOf x ↔ (2 ∣ orderOf x ∧ x ^ (orderOf x / 2) ∈ S)) ∧
      (d = orderOf x ∨ 2 * d = orderOf x)
def kernelClasses (E : ℕ) (Q : ℤ) (alphaOne : Prop) : Set (ZMod E) :=
  {y | y = 1 ∨ y = (Q : ZMod E) ∨ (alphaOne ∧ (y = -1 ∨ y = -(Q : ZMod E)))}
theorem eventual_period_formula (P R : Subgroup G) [Finite P] [Finite R] (w : G) (Q : ℤ)
    (E : ℕ) [NeZero E]
    (hP : ∀ u ∈ P, u ^ (Q - 1) = 1) (hR : ∀ h ∈ R, h ^ (Q + 1) = 1) (hwP : w ^ (Q + 1) ∈ P)
    (hE : ∀ z : ℤ, ((E : ℤ) ∣ z ↔
      ((∀ u ∈ P, u ^ z = 1) ∧ (∀ h ∈ R, h ^ z = 1) ∧ w ^ z = 1)))
    (n : ℤ) (hnP : IsCoprime n (Nat.card P : ℤ)) (hnR : IsCoprime n (Nat.card R : ℤ))
    (hnE : IsCoprime n (E : ℤ)) (d : ℕ)
    (hd : IsLeast {t : ℕ | 0 < t ∧
        ((∀ u ∈ P, u ^ (n ^ t - 1) = 1 ∨ u ^ (n ^ t + 1) = w ^ (Q + 1)) ∧
         (∀ h ∈ R, (w * h) ^ (n ^ t - 1) = 1 ∨ (w * h) ^ (n ^ t + 1) = w ^ (Q + 1)))} d) :
    d ∣ orderOf ((n : ZMod E)) ∧ orderOf ((n : ZMod E)) ∣ 2 * d ∧
      (2 * d = orderOf ((n : ZMod E)) ↔
        (2 ∣ orderOf ((n : ZMod E)) ∧
          (n : ZMod E) ^ (orderOf ((n : ZMod E)) / 2)
            ∈ kernelClasses E Q (w ^ (Q + 1) = 1)))
theorem formula_instance_q5 :
    orderOf ((2 : ℤ) : ZMod 3) = 2 ∧
      (1 : ℕ) ∣ orderOf ((2 : ℤ) : ZMod 3) ∧
      orderOf ((2 : ℤ) : ZMod 3) ∣ 2 * 1 ∧
      2 * 1 = orderOf ((2 : ℤ) : ZMod 3)
theorem split_needs_coprime :
    ∃ (H : Subgroup (Multiplicative (ZMod 2))) (s : ℤ) (w β₁ β₂ : Multiplicative (ZMod 2)),
      ¬ IsCoprime s (Nat.card H : ℤ) ∧
      (∀ h ∈ H, (w * h) ^ (s - 1) = β₁ ∨ (w * h) ^ (s + 1) = β₂) ∧
      ¬ ((∀ h ∈ H, (w * h) ^ (s - 1) = β₁) ∨ (∀ h ∈ H, (w * h) ^ (s + 1) = β₂))
theorem dichotomy_needs_exponent_two :
    IsLeast {t : ℕ | 0 < t ∧ (3 : ZMod 7) ^ t ∈ ({1, 2, 4} : Set (ZMod 7))} 2 ∧
      orderOf (3 : ZMod 7) = 6 ∧ ¬ (orderOf (3 : ZMod 7) ∣ 2 * 2)
```

Axioms, as printed by `#print axioms` on 2026-09-03.

```
sweep_q3, sweep_q4, sweep_q5, thm11_q3, thm11_q4, thm11_q5, frob_q3, frob_q4,
  frob_q5, counts_q3, counts_q4, counts_q5, notAField, cor43_erratum_halved,
  cor43_erratum_full, table1a, table1b, table2, table3a, table3b,
  table3_is_a_rotation, qp_agrees_small, alpha_matters              [propext]
sweep_q7 ... sweep_q32 (14), thm11_q7 ... thm11_q16 (6), frob_q7, frob_q8, frob_q9,
  counts_q7 ... counts_q19 (8), hypothesis_is_needed, kernel_needs_plus_minus,
  pi_needs_the_square_case, qp_agrees_larger
                                [propext, <decl>._native.native_decide.ax_1_1]
coset_split, omega_criterion, period_dvd, period_halves_iff,
  eventual_period_formula, formula_instance_q5, split_needs_coprime,
  dichotomy_needs_exponent_two     [propext, Classical.choice, Quot.sound]
```

References

[1] Yen-Ju Chen and Wayne Peng, Periodicity and dynamical systems of Dickson polynomials in finite fields, arXiv:2508.08621v3 [math.NT], 3 July 2026 (v1 12 August 2025), 18 pages, "under revision". Author order as on the title page of the compiled version 3; the arXiv metadata lists Wayne Peng, Yen-Ju Chen. All statement numbers cited above are those of the compiled version 3.

[2] Claudio Qureshi and Daniel Panario, The graph structure of Chebyshev polynomials over finite fields and applications, *Des. Codes Cryptogr.* **87** (2019), no. 2–3, 393–416, DOI 10.1007/s10623-018-0545-7; preprint arXiv:1803.06539.

[3] Rudolf Lidl and Gary L. Mullen, Cycle structure of Dickson permutation polynomials, *Math. J. Okayama Univ.* **33** (1991), 1–11, DOI 10.18926/mjou/33705, Zbl 0759.11044.

[4] Pascale Charpin, Sihem Mesnager and Sumanta Sarkar, Dickson polynomials that are involutions, in *Contemporary Developments in Finite Fields and Applications*, World Scientific, 2016, 22–47, DOI 10.1142/9789814719261_0003; preprint IACR ePrint 2015/434.

[5] Rudolf Lidl, Gary L. Mullen and Gerhard Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65, Longman Scientific & Technical, 1993. (Cited as printed in reference [9] of [1]; not consulted for this paper.)

[6] L. Peña and M. Ortíz, Cardinality of the Dickson permutation's group of polynomials on $\mathbb{Z}_n$, arXiv:1903.03923 [math.NT], 2019.

[7] The mathlib Community, The Lean mathematical library, in *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, 367–381, DOI 10.1145/3372885.3373824.

[8] L. de Moura and S. Ullrich, The Lean 4 theorem prover and programming language, in *Automated Deduction – CADE 28*, LNCS, Springer, 2021, 625–635, DOI 10.1007/978-3-030-79876-5_37.