ROOT FAMILIES FOR OPTIMAL TERNARY CYCLIC CODES: DING–HELLESETH'S OPEN PROBLEM 7.11 FOR $m \le 16$, AND WHY THE EXCEPTION AT $(m,h) = (10,8)$ IS NOT SPORADIC

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For $q = 3^m$ and $n = q - 1$, let $\mathcal{C}_{(1,e)}$ be the ternary cyclic code of length n with generator polynomial $m_\alpha(x)m_{\alpha^e}(x)$. Ding and Helleseth reduced the question of when $\mathcal{C}_{(1,e)}$ attains the sphere-packing-optimal parameters $[n,\, n-2m,\, 4]$ to two root conditions on the polynomials $(x+1)^e \pm x^e \mp 1$ over $\mathbb{F}_q$, and left nine open problems; the fifth of these asks for the conditions on m and h under which $e = (3^h - 5)/2$ is optimal for even m. We answer it for every even $m \le 16$, and then explain the answer. The computed rows have exactly one irregular cell, $(m,h) = (10,8)$. We show that this cell is not sporadic: for *every* $h \equiv 8 \pmod{10}$ the equation $(x+1)^e - x^e - 1 = 0$ has the same eleven solutions in $\mathbb{F}_{3^{10}}$, ten of them of degree exactly 10 over $\mathbb{F}_3$, so the criterion fails whenever $10 \mid m$. The next cell this reaches, $(m,h) = (20,18)$, lies beyond every computed row and has $h \equiv 2 \pmod 4$, which refutes the congruence pattern that the computed rows alone suggest. We record the complementary family — for $h \equiv 0 \pmod 4$ an extra root already lives in the 81-element field, hence the criterion fails in $\mathbb{F}_{3^m}$ for every $m \equiv 0 \pmod 4$ — and a sweep of the subfield lattice showing that any third family needs a root of degree at least 13. Along the way we answer Bao and Zou's Problem 6.2 at $m = 2, 6, 10, 14$, where exactly 2, 6, 20 and 42 of the admissible exponents are optimal, and tabulate Ding–Helleseth's Open Problem 7.15 at every odd $m \le 13$, where the top exponent $h = m - 1$ always fails. All statements are machine-checked in Lean 4, apart from five steps — two elementary arguments, two external computations, and the identification of the fast search engine with the criterion — each flagged where it occurs.

1. INTRODUCTION

Fix $q = 3^m$, put $n = q - 1$, and let α generate $\mathbb{F}_q^*$. For $a \in \mathbb{F}_q$ write m_a for the minimal polynomial of a over $\mathbb{F}_3$. For e with $1 \le e \le n$, the ternary cyclic code

$$\mathcal{C}_{(1,e)} \subseteq \mathbb{F}_3^n$$

is the cyclic code of length n whose generator polynomial is $m_\alpha(x)\, m_{\alpha^e}(x)$. When the two minimal polynomials are distinct and both of degree m, the code has dimension $n-2m$, and the sphere-packing bound then forbids a minimum distance above 4; so $[n,\, n-2m,\, 4]$ is the optimal parameter set, and the question of which exponents e achieve it is a natural and much-studied one. Ding and Helleseth [1] settled it for several monomial families and reduced the general question to a root count. Write

$$P_e^+(x) = (x+1)^e + x^e + 1, \qquad P_e^-(x) = (x+1)^e - x^e - 1 \qquad \in \mathbb{F}_3[x].$$

For even e one has $P_e^+(1) = 0$ and $P_e^-(0) = 0$ always; these are the *forced* roots. Their criterion, quoted in Section 2, says that (under two standing hypotheses on the 3-cyclotomic coset of e) the code $\mathcal{C}_{(1,e)}$ is optimal precisely when e is even and neither polynomial acquires a root in $\mathbb{F}_q$ beyond its forced one.

Ding and Helleseth close [1] with nine open problems — their Open Problems 7.5, 7.8, 7.9, 7.10, 7.11, 7.12, 7.13, 7.14 and 7.15 — and several have been attacked since: Wu, You, Zha and Zhang [3] give two families of exponents supporting the third of them, and partial answers to the eighth and the ninth are given in [5] and [4] respectively. The fifth is the subject of most of this paper.

Problem 1.1 (Ding–Helleseth, Open Problem 7.11)**.** Let $e = (3^h - 5)/2$, where $2 \le h \le m - 1$, and let m be even. What are the conditions on m and h under which the ternary cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1,\, 3^m - 1 - 2m,\, 4]$?

Two features make this problem the one to attack. It asks for a characterisation rather than for a yes or a no; and it comes with no computational data at all. Ding and Helleseth append to each of their six yes-or-no problems a line reporting a Magma confirmation over a stated range of m, and to none of the three that ask instead for a characterisation — Open Problems 7.11, 7.14 and 7.15. Nothing in the literature we could find answers any part of 7.11; the searches behind that negative are described in the paragraph *What is new, and what is not* below.

What is settled here. We write $e_h = (3^h - 5)/2$ throughout.

(1) **The table.** For every even m with $4 \le m \le 16$ we determine exactly which h in the range $2 \le h \le m-1$ are optimal (Theorems 4.1 and 4.2). The rows are

m	optimal h
4	2
6	2, 4
8	2, 6
10	2, 4, 6
12	2, 6, 10
14	2, 4, 6, 8, 10, 12
16	2, 6, 10, 14

Odd h never occurs, for the elementary reason that e_h is then odd. Evenness of h is not sufficient either: $h = 4$ fails at $m = 8$ and $m = 12$, and $h = 8$ fails at $m = 10$.

(2) **The irregular cell, explained.** Read as congruences, six of the seven rows are regular: at $m \equiv 0 \pmod 4$ the optimal h are exactly those with $h \equiv 2 \pmod 4$, and at $m \equiv 2 \pmod 4$ every even h is optimal — except at $(m, h) = (10, 8)$. Our main result (Theorem 5.3) is that this exception is the first member of an infinite family. For every $h \equiv 8 \pmod{10}$, the polynomial $P^-_{e_h}$ has, in $\mathbb{F}_{3^{10}}$, precisely eleven roots: the forced 0 and ten fixed elements of degree exactly 10 over $\mathbb{F}_3$, the *same* ten for every such h. Consequently the criterion fails at every cell with $10 \mid m$ and $h \equiv 8 \pmod{10}$. The first cell this reaches beyond $(10, 8)$ that is not already excluded on other grounds is $(m, h) = (20, 18)$, and $18 \equiv 2 \pmod 4$: the congruence reading of the computed rows is therefore false at the first modulus past the computed range where it can be tested (Corollary 5.4).

(3) **The complementary family.** For every $h \equiv 0 \pmod 4$ an extra root of $P^+_{e_h}$ or of $P^-_{e_h}$ already lies in the 81-element field, and $\mathbb{F}_{3^4}$ embeds in $\mathbb{F}_{3^m}$ exactly when $4 \mid m$; so for all $h \equiv 0 \pmod 4$ and all $m \equiv 0 \pmod 4$ the criterion fails (Theorem 6.2). This turns the four computed rows $m = 4, 8, 12, 16$ into a statement about every $m \equiv 0 \pmod 4$, and it is stated over the abstract field $\mathbb{F}_{3^m}$ rather than over any presentation of it.

(4) **How far the remaining half is checked.** For every degree $d \le 12$ and every even h outside the two families above, both polynomials have only their forced root in $\mathbb{F}_{3^d}$ — for every h, not for a sample (Proposition 7.1). So a third family, which is what a full answer to Problem 1.1 must rule out, needs a root of degree at least 13. Such a family exists: an independent factorisation, outside the formal development, exhibits roots of degrees $18, 21, 26, 28$ (Remark 7.3).

(5) **Two further published questions.** Bao and Zou [2] close their paper with a question about their own construction, and report that optimal codes exist "for certain t" at $m \in \{2, 6, 10, 14, 18\}$ without printing which. We print them for the first four moduli, as exhaustive characterisations of the whole range of t (Theorem 4.3); the counts are $2, 6, 20, 42$. For Ding–Helleseth's ninth problem, Open Problem 7.15, we observe that the exponent is odd for every even m, which settles half of the (m, h) plane by a one-line argument, and tabulate the odd $m \le 13$, where the top exponent $h = m - 1$ always fails (Theorem 4.4).

What is new, and what is not. The criterion is Ding and Helleseth's, and it is used here exactly as they state it; nothing below is a new proof of it, and nothing below is a statement about a code's minimum distance that does not pass through it. The tables of item (1) and the lists of item (5) are

finite computations that anybody with a computer algebra system could redo; their value is that they were not on record, not that they are new mathematics, and they should not be read as such. The statement of item (3) is, once the roots have been located in $\mathbb{F}_{3^4}$, the step a specialist would take without comment; we record it because it converts four computed rows into infinitely many cells, and because it is the one statement here about $\mathbb{F}_{3^m}$ itself.

What we do put forward as new is item (2): that the $(10, 8)$ cell is the $h \equiv 8 \pmod{10}$ member of a family with a fixed eleven-element root set, and the consequence at $(20, 18)$. The search behind that claim was re-run on 28 August 2026, and with its limits stated it was: the works citing [1] enumerated and inspected at title level — 133 of them on OpenAlex, of which exactly one title names any of the nine problems by its ordinal, and that one names the seventh; the 22 arXiv hits for "optimal ternary cyclic codes" read in full; zero forward citations of [2], counted on two citation services and against both its preprint and its journal version; no match in the OEIS for the exponent sets computed here, with controls confirming that the query distinguishes a miss from a failure; and a full-text sweep of a local mirror of some $8.8 \cdot 10^5$ arXiv sources for the exponent $(3^h - 5)/2$, which returns eleven hits in seven papers — two in [1] itself, three in [2], and six in six papers that use the same expression for an unrelated quantity. No source found by any of these mentions the $(10, 8)$ cell, a congruence criterion in h and m for this exponent, or an $h \equiv 8 \pmod{10}$ family. The limits: the citation sweep was at title level, and the two services disagree on how many citing works there are — Semantic Scholar reports 145 against OpenAlex's 133 on the same day — so the list read was the shorter one; and the typeset journal versions of [1] and [2], and non-arXiv journal papers generally, were not read. Not found is not the same as new.

2. Preliminaries

Throughout, $m \geq 2$, $q = 3^m$, $n = q-1$, and α is a fixed generator of $\mathbb{F}_q^*$. For $j \in \mathbb{Z}_n$ the 3-*cyclotomic coset* of j modulo n is

$$C_j = \{\, j,\ 3j,\ 9j,\ \ldots,\ 3^{\ell_j - 1} j \,\} \subseteq \mathbb{Z}_n,$$

where $\ell_j = |C_j|$ is the least positive integer with $3^{\ell_j} j \equiv j \pmod{n}$. The minimal polynomial of α^j has degree ℓ_j, so $\deg m_{\alpha^e} = m$ exactly when $\ell_e = m$, and $m_\alpha \neq m_{\alpha^e}$ exactly when $e \notin C_1$. Under those two standing hypotheses $\mathcal{C}_{(1,e)}$ has dimension $n - 2m$.

Theorem 2.1 (Ding–Helleseth [1, Theorem 4.1])**.** *Let $e \notin C_1$ and $\ell_e = |C_e| = m$. The cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1,\ 3^m - 1 - 2m,\ 4]$ if and only if the following conditions are satisfied:*

- **C1:** *e is even;*
- **C2:** *the equation $(x+1)^e + x^e + 1 = 0$ has the only solution $x = 1$ in $\mathrm{GF}(q)^*$;*
- **C3:** *the equation $(x+1)^e - x^e - 1 = 0$ has the only solution $x = 0$ in $\mathrm{GF}(q)$.*

We refer to C1, C2, C3 by those names and call the conjunction of C1, C2, C3 and the two standing hypotheses the *Ding–Helleseth criterion at* (m, e). Theorem 2.1 is used as a citation and is not reproved here; every statement below is a statement about the criterion, and the passage from it to a minimum distance is exactly the content of that theorem. We say "e is optimal at m" for "the criterion holds at (m, e)", and the reader who wants the coding-theoretic reading should append: *and therefore, by Theorem 2.1, $\mathcal{C}_{(1,e)}$ has parameters $[n, n - 2m, 4]$.*

Note the asymmetry of C2 and C3, which is the source's: C2 excludes $x = 1$ and quantifies over $\mathbb{F}_q^*$, while C3 excludes only $x = 0$ and quantifies over all of $\mathbb{F}_q$. It is harmless. For even e one has $2^e = (-1)^e = 1$ in characteristic 3, so $P_e^+(0) = 2 \neq 0$ and $P_e^-(1) = 2 \neq 0$; excluding $\{0, 1\}$ from both equations therefore quantifies over the same effective set as the source's convention.

Three families of exponents occur below.

(1)
$$e_h = \tfrac{1}{2}\big(3^h - 5\big), \qquad 2 \le h \le m-1,\ m \text{ even} \qquad \text{(Open Problem 7.11)},$$

(2)
$$b_{m,t} = \tfrac{1}{2}\big(3^h + 1\big) + \big(3^h + 1\big)t, \quad h = m/2,\ 0 \le t \le 3^h - 2,\ m \equiv 2 \pmod 4 \quad \text{(Problem 6.2 of [2])},$$

(3)
$$g_{m,h} = \tfrac{1}{2}\big(3^{m-1} - 1\big) + 3^h + 1, \quad 0 \le h \le m-1 \qquad \text{(Open Problem 7.15)}.$$

The following observation is elementary and is what removes odd h from Problem 1.1: $3^h \equiv 1 \pmod 4$ for even h and $3^h \equiv 3 \pmod 4$ for odd h, so $e_h = (3^h - 5)/2$ is even if and only if h is even. Hence C1 fails at every odd h, and every table below lists even h only.

Finally, the reformulation that organises Sections 5–7. A root of a polynomial over $\mathbb{F}_3$ lies in $\mathbb{F}_{3^m}$ exactly when the degree of its minimal polynomial divides m. So the set of m at which a fixed exponent e violates C2 or C3 is determined by the multiset of degrees of the non-forced roots of P_e^+ and P_e^-, and the (m, h) table of Problem 1.1 is nothing but a divisibility relation between those degrees and m. The whole of Section 5 is the exploitation of this remark: instead of scanning fields of growing size, one locates roots in fields of *fixed* small size.

3. The presented field, and two engines

Every claim in this paper about a specific (m, e) is decided by an exhaustive search over $\mathbb{F}_{3^m}$, so the presentation of the field is part of the mathematics and not an implementation detail. We present $\mathbb{F}_{3^m}$ as

$$\mathbb{F}_3[x]/\big(x^m - r(x)\big), \qquad \deg r < m,$$

an element being encoded by the natural number whose m base-3 digits are its coefficients: $v = \sum_{k<m} c_k 3^k$ stands for $\sum_{k<m} c_k x^k$. Addition is digitwise in $\mathbb{F}_3$ and multiplication is Horner's rule over the digits with the reduction $x^m = r(x)$ applied at each step. The moduli used are $x^2 - x - 1$, $x^4 - x - 1$, $x^6 - x - 1$, $x^8 - x^3 - 1$, $x^{10} - x^3 - x - 1$, $x^{12} - x^4 - x^3 - x^2 - 2x - 1$, $x^{14} - x - 1$ and $x^{16} - x^4 - x^3 - 2x^2 - x - 1$ for the even m, together with $x^m - r$ for the odd $m \le 13$ used in Section 4; in each case r is the first modulus, in the order induced by the encoding, for which the class of x is primitive.

Proposition 3.1. *For each $m \in \{2, 3, \dots, 14\}$ and each r above, the class of x in $\mathbb{F}_3[x]/(x^m - r(x))$ has multiplicative order exactly $3^m - 1$; the relation $x^m = r(x)$ holds in the quotient; and the digitwise operation on encodings is coefficientwise addition in $\mathbb{F}_3$, for every index and every pair of arguments. Consequently each quotient is a field and each modulus is irreducible over $\mathbb{F}_3$. Moreover the Ding–Helleseth criterion is a decidable predicate of (m, r, e), and the decision procedure — one pass over the 3^m encodings, computing x^e and $(x+1)^e$ at each — is equivalent to the criterion as stated.*

Primitivity is checked by outright enumeration of all $3^m - 1$ powers of x, requiring them pairwise distinct and nonzero and requiring the walk to close at 1; this is stronger than the usual test "$x^{n/p} \neq 1$ for each prime $p \mid n$" and it is deliberately so, see Section 8. Primitivity gives irreducibility at once: $3^m - 1$ distinct nonzero powers together with 0 exhaust the quotient, so every nonzero element is a unit. That last inference is the elementary argument just given and is not itself part of the formal development; what is enumerated there is the primitivity. The one place where the field structure is needed as a formal object rather than as a fact about the search space is Lemma 6.1, where it is established outright, at 81 elements.

The direct scan costs two field exponentiations per element, that is $\Theta(3^m m^2 \log e)$ per cell, and is affordable up to $m = 8$; a single cell at $m = 10$ was measured at over twenty minutes. The second engine replaces field arithmetic by table lookups. With α the class of x and z the *Zech logarithm* [7], defined by $1 + \alpha^i = \alpha^{z(i)}$ and undefined exactly at the i with $\alpha^i = -1$, one has for even e and $x = \alpha^i$, writing $A = z(i)e \bmod n$ and $B = ie \bmod n$:

- the element $x = -1$ may be skipped, since $(-1)^e = 1$ makes $P_e^+(-1) = 2$ and $P_e^-(-1) = 1$;
- the case $B = n/2$ may be skipped, since then $x^e = -1$ and both equations demand $(x+1)^e = 0$ with $x + 1 \neq 0$;
- otherwise P_e^- vanishes at x iff $A = z(B)$, and P_e^+ vanishes at x iff $A \equiv z(B) + n/2 \pmod n$.

This costs $\Theta(3^m)$ per cell and reaches $m = 16$. Both steps are narrowings of the search, so they are derived above rather than observed, and they are checked as well.

Proposition 3.2. *The tables* exp, log *and* z *built for a modulus satisfy, by enumeration:* $\exp(0) = 1$*;* $\exp(i+1) = x \cdot \exp(i)$ *for all* $i < n-1$*;* $x \cdot \exp(n-1) = 1$*;* log *inverts* exp *in both directions, so* exp *enumerates* $\mathbb{F}_q^*$*; and* $z(i) = \log(1+\alpha^i)$*, with the sentinel value exactly at the unique* i *with* $1 + \alpha^i = 0$*. The two engines return the same verdict at every exponent* $0 \leq e < 3^m - 1$ *for* $m = 2, 4, 6$ *— all* $8+80+728$ *of them — and at every cell of Problem 1.1 for* $m = 8$*. Ding–Helleseth's Theorem 7.6, an "if and only if" with a published proof, is reproduced in both directions on the direct scan at* $m = 5, 6, 7$ *and on the table engine at* $m = 10, 12, 13, 14$*; and the criterion holds at the cell of their Example 7.7 —* $(m, h) = (5, 2)$*,* $e = 8$*, the* $[242, 232, 4]$ *code — on the field the source itself specifies.*

Theorem 7.6 of [1] states that for $e = 3^h - 1$ with $1 \leq h \leq m-1$ the code $\mathcal{C}_{(1,e)}$ is optimal if and only if $\gcd(h, m) = 1$ and $\gcd(3^h - 2, 3^m - 1) = 1$. It is the strongest external control available: a published equivalence, checked in both directions, at exactly the moduli where the table engine has to be trusted. Example 7.7 fixes $(m, h) = (5, 2)$ and α with $\alpha^5 + 2\alpha + 1 = 0$; our modulus at $m = 5$ is $x^5 - x - 2$, which is the same relation after clearing signs. Grassl's tables [6] give lower and upper bounds 4 and 4 for the minimum distance of a ternary $[242, 232]$ code, confirming that cell independently of both.

One link in the chain above is not a theorem, and it is worth saying where it breaks. For the direct scan, the equivalence of the decision procedure with the criterion is proved (Proposition 3.1). For the table route it is not: that the facts the self-check verifies entail the three identities above would need a ring structure on the packed carrier, and that is established only at 81 elements (Lemma 6.1). Every result below that is computed through the tables — the rows $m = 10, 12, 14$ of Theorem 4.1, Theorem 4.2, the rows $m = 10, 14$ of Theorem 4.3, the rows $m = 9, 11, 13$ of Theorem 4.4, and the root sets of Lemma 5.2, Theorem 5.3 and Proposition 7.1 — is therefore machine-checked as a statement about the table route's verdict, and its reading as a statement about the criterion rests on the derivation above together with the agreement of Proposition 3.2. The rows at $m \leq 8$ carry no such caveat, and neither does Theorem 6.2, which uses no table at all.

4. The tables

Theorem 4.1. *Let* $e_h = (3^h - 5)/2$*. For each even* m *with* $4 \leq m \leq 14$*, the set of* h *with* $2 \leq h \leq m-1$ *for which the Ding–Helleseth criterion holds at* (m, e_h) *is exactly*

m	$\{h\}$
4	$\{2\}$
6	$\{2, 4\}$
8	$\{2, 6\}$
10	$\{2, 4, 6\}$
12	$\{2, 6, 10\}$
14	$\{2, 4, 6, 8, 10, 12\}$

In particular: at $m = 4, 8, 12$ *the optimal* h *are exactly those with* $h \equiv 2 \pmod 4$*; at* $m = 6$ *and* $m = 14$ *every even* h *in range is optimal; and at* $m = 10$ *every even* h *in range is optimal except* $h = 8$*.*

Proof sketch. Each row is an exhaustive computation and nothing else. For a fixed (m, h) the criterion is decided by one pass over all 3^m elements of $\mathbb{F}_{3^m}$, computing x^{e_h} and $(x+1)^{e_h}$ at each and testing the two equations; the two coset hypotheses and C1 are arithmetic in $\mathbb{Z}_n$. The rows $m = 4, 6, 8$ were computed on the direct scan of Section 3 and $m = 10, 12, 14$ on the table engine, whose agreement

with the direct scan is exhaustive at $m = 2, 4, 6$ and cell-by-cell at $m = 8$ (Proposition 3.2). The searched ranges are the full ranges $2 \le h \le m-1$: 2, 4, 6, 8, 10 and 12 cells respectively, each cell a complete scan of $\mathbb{F}_{3^m}$, so the statement is a characterisation and not a list of examples. □

Theorem 4.2. *At $m = 16$, presented as $\mathbb{F}_3[x]/(x^{16} - x^4 - x^3 - 2x^2 - x - 1)$, the set of h with $2 \le h \le 15$ for which the criterion holds is exactly $\{2, 6, 10, 14\}$; that is, exactly the h with $h \equiv 2 \pmod 4$. Moreover Ding–Helleseth's Theorem 7.6 is reproduced at this modulus for all fifteen exponents $e = 3^h - 1$, $1 \le h \le 15$.*

Proof sketch. Exhaustive, on the table engine, over a field of $3^{16} = 43\,046\,721$ elements. The content of the row is not that $h = 2, 6, 10, 14$ pass — the pattern of Theorem 4.1 would have had to be badly wrong for that to fail — but that the three even exponents $h = 4, 8, 12$ fail, each of which was an independent opportunity for the pattern to die. The modulus is the first primitive one in the encoding order; the same search reproduces the moduli used at $m = 8, 10, 12, 13, 14$, so the selection rule was validated on five known answers before being used for a sixth. The self-check of Proposition 3.2 is what certifies that the carrier is a field here, and the Theorem 7.6 control is what tests it against published mathematics; the row itself and the control were computed together because the cost is dominated by building the tables once. Before this row was formalised it was computed five further ways that all agree: the same engine in C; the same engine over two further primitive moduli; the same engine with the tables rebuilt from the generator α^7 in place of α; and, for $h \le 12$, root counting by $\deg \gcd(P, x^q - x)$, an algorithm with no field enumeration in it at all. □

Theorem 4.3. *Let $m \equiv 2 \pmod 4$, $h = m/2$, and $b_{m,t}$ as in (2). For $m = 2, 6, 10, 14$ the set of t in the full range $0 \le t \le 3^h - 2$ for which the criterion holds at $(m, b_{m,t})$ is exactly*

$$
\begin{aligned}
m = 2: &\quad \{0, 1\},\\
m = 6: &\quad \{3, 5, 10, 16, 18, 23\},\\
m = 10: &\quad \{24, 30, 32, 48, 50, 56, 73, 91, 97, 99, 145, 151, 153, 169, 171, 177, 194, 212, 218, 220\},\\
m = 14: &\quad \{195, 219, 273, 275, 291, 293, 429, 437, 455, 461, 507, 533, 586, 658, 666, 820, 826,\\
&\qquad 874, 880, 882, 906, 1288, 1312, 1366, 1368, 1384, 1386, 1522, 1530, 1548,\\
&\qquad 1554, 1600, 1626, 1679, 1751, 1759, 1913, 1919, 1967, 1973, 1975, 1999\},
\end{aligned}
$$

of sizes 2, 6, 20 and 42. In particular the count at $m = 14$ is not $\binom{8}{4} = 70$.

Proof sketch. Exhaustive over the whole range of t — 2, 26, 242 and 2186 cells, each a complete scan of a field of 9, 729, 59 049 and 4 782 969 elements. The rows $m = 2$ and $m = 6$ are on the direct scan and are stated as equivalences over the whole range; the rows $m = 10$ and $m = 14$ are on the table engine. Each optimal set is closed under the map induced by $e \mapsto 3e \bmod n$, as it must be since $m_{\alpha^e} = m_{\alpha^{3e}}$ makes $\mathcal{C}_{(1,e)} = \mathcal{C}_{(1,3e)}$; that closure was used as a check on the output and never as a shortcut in the search, so the counts are counts of full scans. The final sentence is a comparison of two integers. □

Bao and Zou write, of the family (2): "Computational evidence suggests that in this case optimal codes $\mathcal{C}_{(1,e)}$ do exist for specific choices of e. For example, when $m \in \{2, 6, 10, 14, 18\}$ and $h = m/2$, the exponents $e = (3^h + 1)/2 + (3^h + 1)t$ (for certain t) yield optimal codes", and then ask which t these are. Theorem 4.3 answers that for the first four of their five moduli; $m = 18$ needs 19 682 cells over a field of $3.9 \cdot 10^8$ elements and is out of our reach, and it is also where their own evidence stopped. The quotation, and the label "Problem 6.2", are from arXiv:2601.12427v1, which is the only version on arXiv; the paper has since appeared in *Finite Fields and Their Applications*, and we have not seen the typeset version, so a reader working from it should expect the numbering to be checked.

The final sentence of Theorem 4.3 is worth one remark. The counts $2, 6, 20$ at $m = 2, 6, 10$ are the central binomial coefficients $\binom{2}{1}, \binom{4}{2}, \binom{6}{3}$, which predict $\binom{8}{4} = 70$ at $m = 14$. The prediction is false; the answer is 42.

Theorem 4.4. *Let $g_{m,h} = (3^{m-1}-1)/2 + 3^h + 1$ as in (3).*

(1) *For every even $m \geq 2$ and every $h \geq 0$, the integer $g_{m,h}$ is odd. Hence C1 fails and the criterion holds at no cell with m even.*

(2) *For odd $m \leq 13$, the set of h with $0 \leq h \leq m-1$ for which the criterion holds is*

m	$\{h\}$
3	$\{0,1\}$
5	$\{0,1,2,3\}$
7	$\{0,\ldots,5\}$
9	$\{0,1,3,4,7\}$
11	$\{0,\ldots,9\}$
13	$\{0,\ldots,11\}$

In every one of these rows the top exponent $h = m-1$ is absent.

Proof sketch. Part (1) is an argument and involves no computation. For m even, $m-1$ is odd, so $3^{m-1} \equiv 3 \pmod 8$ and $(3^{m-1}-1)/2$ is odd; 3^h+1 is even; the sum is odd. This disposes of half the (m,h) plane in one step. Part (2) is exhaustive: for each odd $m \leq 13$ all m cells were scanned, on the direct scan for $m = 3, 5, 7$ and on the table engine for $m = 9, 11, 13$. □

Part (1) is elementary and is surely known to everyone who has worked on Open Problem 7.15; we record it because it explains every empty row rather than as a contribution. Part (2) has one published point of contact: Zheng, He and Liao [4] give counterexamples at $(m,h) = (5,4)$ and $(7,6)$, both of them exactly $h = m-1$, and both are reproduced by the corresponding rows. The row $m = 9$ is the interesting one: $3 \mid m$ and the set drops to $\{0,1,3,4,7\}$, so $h = m-1$ is not the only failure there.

5. Root location, and the second family

We now prove the main result. The instrument is the observation at the end of Section 2: the whole (m,h) table is a divisibility relation between m and the degrees of the extra roots, so it is enough to work in small fixed fields. What makes this practical is that the exponent e_h, which grows like 3^h, is periodic in h modulo 3^d-1 with a very short period.

Lemma 5.1. *Let $d \geq 1$ and let $h, h' \geq 2$ with $h \equiv h' \pmod{2d}$. Then $e_h \equiv e_{h'} \pmod{3^d-1}$. Consequently the solution sets of $P^+_{e_h}$ and $P^-_{e_h}$ in $\mathbb{F}_{3^d}$ depend on h only through $h \bmod 2d$.*

Proof. Since $3^{2d}-1 = (3^d-1)(3^d+1)$ and 3^d+1 is even, $2(3^d-1)$ divides $3^{2d}-1$, so $3^h \equiv 3^{h'} \pmod{2(3^d-1)}$ whenever $h \equiv h' \pmod{2d}$. For $h \geq 2$ one has $2e_h + 5 = 3^h$; subtracting the two instances and cancelling the factor 2 gives $3^d - 1 \mid e_h - e_{h'}$. The consequence is immediate, because y^e for $y \in \mathbb{F}^*_{3^d}$ depends on e only modulo 3^d-1, and $y = 0$ contributes 0 to both sides. □

Lemma 5.1 is what turns each of the finite computations below into a statement about infinitely many h: at degree d there are only d even residue classes to inspect, and inspecting them decides the whole h-axis at that degree. At $d = 4$ the period is 8 and at $d = 10$ it is 20. We record the $d = 4$ computation first, because it is small enough to print.

Lemma 5.2. *Present $\mathbb{F}_{3^4}$ as $\mathbb{F}_3[x]/(x^4 - x - 1)$ and encode elements as in Section 3, so that 10 denotes x^2+1. For $h \geq 2$ even, the solution sets in $\mathbb{F}_{3^4}$ are*

$h \bmod 8$	$P^+_{e_h} = 0$	$P^-_{e_h} = 0$
2, 6	$\{1\}$	$\{0\}$
4	$\{1, 10, 16, 19, 22, 31, 34, 37, 43, 58, 61, 73, 76\}$	$\{0\}$
0	$\{1\}$	$\{0, 10, 16, 37, 58\}$

and in the two irregular classes every non-forced root has degree exactly 4 over $\mathbb{F}_3$. In particular x^2+1 is a non-forced root of $P^+_{e_h}$ for every $h \equiv 4 \pmod 8$ and of $P^-_{e_h}$ for every $h \equiv 0 \pmod 8$ with $h \geq 8$; and for every $h \equiv 2 \pmod 4$ both polynomials have only their forced root in $\mathbb{F}_{3^4}$.

Proof sketch. Four exhaustive computations over the 81 elements of the field, one for each even residue class modulo the period 8, at the representatives $h = 2, 4, 6, 8$; Lemma 5.1 transports each to its whole class. The degree claim is the statement that only the forced root is fixed by $y \mapsto y^9$, which is again a check over the listed roots. □

The second family lives one lattice level up, in $\mathbb{F}_{3^{10}}$, and it is invisible at every smaller degree.

Theorem 5.3. *Present $\mathbb{F}_{3^{10}}$ as $\mathbb{F}_3[x]/(x^{10} - x^3 - x - 1)$ and encode elements as in Section 3. Let*

$$S = \{11257,\ 12232,\ 12277,\ 32416,\ 35024,\ 39486,\ 40584,\ 42752,\ 48893,\ 56165\} \subseteq \mathbb{F}_{3^{10}},$$

a set of ten elements, each of degree exactly 10 over $\mathbb{F}_3$. Then for every $h \equiv 8 \pmod{10}$ with $h \geq 8$, the solution set of

$$(x+1)^{e_h} - x^{e_h} - 1 = 0$$

in $\mathbb{F}_{3^{10}}$ is exactly $\{0\} \cup S$. In particular condition C3 fails in $\mathbb{F}_{3^{10}}$ for every such h, and the set of extra solutions is the same for all of them.

Proof sketch. By Lemma 5.1 with $d = 10$, the solution set depends on h only through $h \bmod 20$, and $h \equiv 8 \pmod{10}$ is the union of the two classes $h \equiv 8$ and $h \equiv 18 \pmod{20}$. Each of the two representatives $h = 8$ and $h = 18$ is settled by one exhaustive pass over all 59 049 elements of the field, and the two passes return the same list, element for element. That every member of S has degree exactly 10 is the statement that no member is fixed by $y \mapsto y^{3^5}$ or by $y \mapsto y^{3^2}$, the maximal proper subfields being $\mathbb{F}_{3^5}$ and $\mathbb{F}_{3^2}$; this too is checked on the listed elements. Finally, the other eight even residue classes modulo 20 were scanned as well, and in each of them both polynomials have only their forced root in $\mathbb{F}_{3^{10}}$; so $h \equiv 8 \pmod{10}$ is exactly the part of the h-axis that this field sees. □

For the reader who wants them explicitly, the encoding $v = \sum_k c_k 3^k \leftrightarrow \sum_k c_k x^k$ turns S into

$11257 = x^8 + 2x^7 + x^5 + 2x^3 + 2x^2 + 2x + 1,$
$12232 = x^8 + 2x^7 + x^6 + 2x^5 + x^4 + 1,$
$12277 = x^8 + 2x^7 + x^6 + 2x^5 + x^4 + x^3 + 2x^2 + 1,$
$32416 = x^9 + x^8 + 2x^7 + 2x^6 + x^5 + x^4 + x^2 + 2x + 1,$
$35024 = x^9 + 2x^8 + x^7 + x^3 + x + 2,$
$39486 = 2x^9 + x^4 + x^3 + x^2 + x,$
$40584 = 2x^9 + x^6 + 2x^5 + x,$
$42752 = 2x^9 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + x^2 + 2,$
$48893 = 2x^9 + x^8 + x^7 + x^6 + x^3 + 2x^2 + x + 2,$
$56165 = 2x^9 + 2x^8 + x^7 + 2x^6 + x^3 + x + 2.$

Corollary 5.4. *Condition C3 fails in $\mathbb{F}_{3^m}$ for every m divisible by 10 and every $h \equiv 8 \pmod{10}$, $h \geq 8$. In particular it fails at $h = 18$, where $18 \equiv 2 \pmod 4$; since $18 \leq 20 - 1$, the cell $(m, h) = (20, 18)$ lies inside the range of Problem 1.1, and the criterion fails there.*

Proof. The elements of S have degree 10 over $\mathbb{F}_3$, so they lie in $\mathbb{F}_{3^m}$ whenever $10 \mid m$; they are nonzero, so they violate C3 there. (The passage from $\mathbb{F}_{3^{10}}$ to $\mathbb{F}_{3^m}$ is the classical statement that $\mathbb{F}_{3^{10}} \subseteq \mathbb{F}_{3^m}$ when $10 \mid m$; it is the one step of this corollary that is not part of the machine-checked development.) The statement at $h = 18$ is Theorem 5.3 with $h = 18$, together with $18 \bmod 4 = 2$. □

Corollary 5.4 is the point of this section, so it is worth saying what it does to the computed rows. Read as congruences, Theorems 4.1 and 4.2 suggest that at $m \equiv 0 \pmod 4$ the optimal h are exactly the $h \equiv 2 \pmod 4$; four rows, $m = 4, 8, 12, 16$, and thirty-two cells, are consistent with that. The suggestion is false at the next modulus: $20 \equiv 0 \pmod 4$ and $18 \equiv 2 \pmod 4$, yet $(20, 18)$ fails. The failure is invisible from the computed rows because the constraint $h \leq m - 1$ keeps $h = 18$ out of every row with $m \leq 16$: the family exists in the data as the single cell $(10, 8)$ and nowhere else, which is exactly why it reads as sporadic. It is not.

Remark 5.5. Corollary 5.4 is a statement about condition C3, and by our convention that is what "the criterion fails" means. To convert it into non-optimality of a code through Theorem 2.1, the two standing hypotheses must also hold at that cell. At $(m, h) = (20, 18)$ the exponent is $e_{18} = 193\,710\,242$; a computation outside the formal development records that it is even, that $e_{18} \notin C_1$ and that $|C_{e_{18}}| = 20$, so Theorem 2.1 does apply and $\mathcal{C}_{(1,e_{18})}$ over $\mathbb{F}_{3^{20}}$ is not optimal. These are three short arithmetic checks in $\mathbb{Z}_n$ with $n = 3^{20} - 1 = 3\,486\,784\,400$ — a parity test, twenty comparisons

against $C_1 = \{3^i \bmod n\}$, and the least ℓ with $3^\ell e_{18} \equiv e_{18}$ — and they remain external here, but they have been redone independently for this paper and agree.

6. The complementary family, over the abstract field

Lemma 5.2 locates a root of degree 4 for every $h \equiv 0 \pmod 4$. Since all of Section 4 is computed inside a presentation of $\mathbb{F}_{3^m}$, it is worth paying once, at 81 elements, for the statement over the abstract field.

Lemma 6.1. *Let F denote the 81-element field $\mathbb{F}_3[x]/(x^4 - x - 1)$, with its ring operations given by the encoded arithmetic of Section 3 and its field structure established from the commutative-ring laws together with finiteness and the absence of zero divisors. Then for every $m \neq 0$,*

$$\text{there is an } \mathbb{F}_3\text{-algebra map } F \to \mathbb{F}_{3^m} \qquad \Longleftrightarrow \qquad 4 \mid m.$$

Proof sketch. The commutative-ring laws of the encoded arithmetic at $m = 4$ are verified on all $81^3 = 531\,441$ triples; with finiteness this makes F a finite integral domain, hence a field, so no table of inverses is needed. From $|F| = 81$ one gets $\operatorname{char} F = 3$ and $\dim_{\mathbb{F}_3} F = 4$. The equivalence is then the standard criterion that a finite field embeds in another exactly when its degree divides the other's, applied with $\dim_{\mathbb{F}_3} \mathbb{F}_{3^m} = m$. The "only if" half is what confines the argument below to $m \equiv 0 \pmod 4$. □

Theorem 6.2. *Let $h \equiv 0 \pmod 4$ with $h \geq 4$, and let $m \neq 0$ with $4 \mid m$. Then C2 or C3 fails in $\mathbb{F}_{3^m}$ at the exponent $e_h = (3^h - 5)/2$.*

Proof sketch. Let $x_0 = x^2 + 1 \in F$. Since $|F^*| = 80$, powers of x_0 depend on the exponent only modulo 80, and Lemma 5.1 at $d = 4$ gives $e_h \equiv 38 \pmod{80}$ for $h \equiv 4 \pmod 8$ and $e_h \equiv 78 \pmod{80}$ for $h \equiv 0 \pmod 8$, $h \geq 8$. Two identities in F, each a finite computation, then say $(x_0+1)^{38} + x_0^{38} + 1 = 0$ and $(x_0 + 1)^{78} - x_0^{78} - 1 = 0$. Transport along the algebra map supplied by Lemma 6.1: a ring map out of a field is injective, so the image of x_0 is still different from 0 and from 1, and it satisfies the same equation. The two branches of the argument say which of the two conditions fails — C2 when $h \equiv 4 \pmod 8$ and C3 when $h \equiv 0 \pmod 8$, with the image of x_0 the witness in both cases — but the conclusion is stated as the disjunction, because that is the form of the machine-checked statement, and nothing below needs more. □

Theorem 6.2 covers infinitely many cells of Problem 1.1 at once, of which $m = 4, 8, 12, 16$ are the four that Section 4 verifies one at a time. Two cautions. First, as everywhere here, the conclusion is the failure of Ding–Helleseth's conditions; non-optimality of the corresponding code follows through Theorem 2.1 at those cells where its standing hypotheses hold, and we do not check them cell by cell. Second, we do not claim the statement as new mathematics: once Lemma 5.2 has located the roots in an 81-element field, the passage to every $m \equiv 0 \pmod 4$ is the obvious next line. The complementary family of Theorem 5.3 has no counterpart here: the same ring-law verification in $\mathbb{F}_{3^{10}}$ would be $59\,049^3 \approx 2 \cdot 10^{14}$ triples, so that family remains a statement about the presented field, which is why Corollary 5.4 carries its containment step by hand.

7. The open half, and a rule that fails

What Problem 1.1 still asks, after Theorem 5.3 and Theorem 6.2, is the other direction: that for the remaining h the two polynomials acquire *no* extra root in *any* extension of $\mathbb{F}_3$. We can bound how far that has been verified, and the bound is a statement about all h, not about a sample.

Proposition 7.1. *Let $1 \leq d \leq 12$ and let h be even, excluding $h \equiv 0 \pmod 4$ when $4 \mid d$ and $h \equiv 8 \pmod{10}$ when $10 \mid d$. Then $P^+_{e_h}$ has only the root 1 and $P^-_{e_h}$ only the root 0 in $\mathbb{F}_{3^d}$. Consequently, any further cell at which the criterion fails requires an extra root of degree at least 13.*

Proof sketch. For each $d \le 12$ the period of Lemma 5.1 is $2d$, so the d even residue classes modulo $2d$ exhaust the even h; the computation runs one exhaustive scan of $\mathbb{F}_{3^d}$ per class, at the representatives $2, 4, \dots, 2d$, and skips exactly the classes belonging to the two known families. The largest scans are $3^{11} = 177\,147$ and $3^{12} = 531\,441$ elements. The consequence follows because a root of degree $d \le 12$ would have shown up in the corresponding scan. □

The two families of Sections 5 and 6 can be packaged as a divisibility test. Say that h has *bad degrees* $B(h) \subseteq \{4, 10\}$, with $4 \in B(h)$ iff $4 \mid h$ and $10 \in B(h)$ iff $h \equiv 8 \pmod{10}$, and let $R(m, h)$ be the predicate "h is even and no element of $B(h)$ divides m".

Proposition 7.2. *$R(m, \cdot)$ reproduces every row of Theorems 4.1 and 4.2: for each even m with $4 \le m \le 16$, the set of $h \in [2, m-1]$ with $R(m, h)$ is exactly the set computed there. Its values at the next two even moduli congruent to 0 modulo 4 are $\{2, 6, 10, 14\}$ at $m = 20$ and $\{2, 6, 10, 14, 18, 22\}$ at $m = 24$.*

Proof sketch. The first sentence is a comparison of two explicitly computed lists at each of the seven moduli; it adds no field computation to Theorems 4.1 and 4.2, it restates them. The second is arithmetic in the definition of R, with no field of 3^{20} or 3^{24} elements built anywhere. □

Remark 7.3 (R is a fit, not a characterisation). Proposition 7.2 must not be read as an answer to Problem 1.1, and the reason is not caution but a counterexample. A computation performed outside the formal development — distinct-degree factorisation of $P^+_{e_h}$ and $P^-_{e_h}$ over $\mathbb{F}_3$, which returns the complete multiset of root degrees and therefore decides every m at once — gives, for the small even h:

h	degrees of the roots of $P^+_{e_h}$	degrees of the roots of $P^-_{e_h}$
2	1	1
4	1, $4^{(3)}$, $8^{(3)}$	1, 8, 28
6	1, $28^{(3)}$, $92^{(3)}$	1, $21^{(2)}$, $159^{(2)}$
8	1, $26^{(6)}$, $38^{(3)}$, $57^{(2)}$, $87^{(2)}$, $98^{(3)}$, $114^{(3)}$, $225^{(2)}$, $544^{(3)}$	1, 4, 10, 18, $118^{(2)}$, $214^{(2)}$, $364^{(2)}$, $582^{(2)}$, 688
10	no root of degree ≤ 40 beyond the forced one, for either polynomial	

(the entries are the degrees of the *distinct* irreducible factors, a superscript saying how many factors carry that degree; multiplicities are not shown). Degrees 18, 21, 26 and 28 are outside $B(h)$, so R is false as a characterisation: it fails first at $(m, h) = (18, 8)$, where $P^-_{e_8}$ has 19 roots in $\mathbb{F}_{3^{18}}$, and again at $(26, 8)$, $(28, 6)$, $(38, 8)$ and $(42, 6)$. The cell $(28, 6)$ is the sharpest, since $6 \equiv 2 \pmod 4$: it refutes at one stroke both R and the congruence reading of the computed rows. The values of R at $m = 20, 24$ recorded in Proposition 7.2 therefore carry no evidential weight as *rows*. What survives of them is this. The cells the rule excludes are not conjectural: $h = 4, 8, 12, 16$ at $m = 20$ and $h = 4, 8, 12, 16, 20$ at $m = 24$ fail by Theorem 6.2, and $h = 18$ at $m = 20$ fails by Corollary 5.4. Of the cells it includes, the same external computation finds $h = 2, 6, 10$ clean at $m = 20$ and at $m = 24$; $h = 14$ at either modulus, and $h = 18, 22$ at $m = 24$, are beyond it, the exponent $e_{14} = 2\,391\,482$ putting the polynomial out of reach. Note that none of this touches Theorem 6.2, which concerns the failing direction only, and that it is consistent with Proposition 7.1: the new degrees are $18, 21, 26, 28$, all at least 13.

Two entries of the table above, and the cells they refute, were recomputed from scratch for this paper by a second implementation: $P^-_{e_8}$ has exactly 19 distinct roots in $\mathbb{F}_{3^{18}}$ and $P^+_{e_6}$ exactly 85 in $\mathbb{F}_{3^{28}}$, so $(18, 8)$ violates C3 and $(28, 6)$ violates C2. So were the $h \le 8$ rows of the table, at every degree up to 40, and the three counts 11, 5 and 13 — the roots of $P^-_{e_8}$ in $\mathbb{F}_{3^{10}}$ and in $\mathbb{F}_{3^4}$, and of $P^+_{e_4}$ in $\mathbb{F}_{3^4}$ — which reproduce Theorem 5.3 and Lemma 5.2 from outside the development; and so was the cleanness of $h = 2, 6, 10$ at $m = 20$ and at $m = 24$. The rest — the degrees above 40, the $h = 10$ row of the table, and the cells $(26, 8)$, $(38, 8)$ and $(42, 6)$ — stays external and is recorded as such.

Open Problem 7.11 therefore remains open, and it is now known to be harder than the computed rows make it look: any characterisation must account for at least three families of extra roots, at degrees 4, 10 and 18 or above. The instrument that would settle it is not more rows — the fields grow

by a factor of 9 per row and $m = 18$ is already out of reach — but a proof that for $h \equiv 2 \pmod 4$ outside the known families the polynomials $(x+1)^{e_h} \pm x^{e_h} \mp 1$ are, apart from the forced root, without roots in any extension.

8. Controls

Every verdict in Sections 4–7 is a Boolean computed in a presented ring. If that ring were not a field the computation would not fail; it would return plausible wrong answers. The following collects the checks that this did not happen, together with the refutations of the natural overstatements of our results.

Proposition 8.1. (1) Wrong field. *Take $m = 6$ and the modulus $x^6 - 1$. The class of x has order 6, so $x^{n/p} \neq 1$ for every prime p dividing $n = 728 = 2^3 \cdot 7 \cdot 13$ and the customary primitivity test passes; the clause that catches it is $x^n = 1$, which fails. The quotient has the zero divisor $4 \cdot 455 = 0$, so $x^6 - 1$ is reducible. Over this carrier the answer to Bao and Zou's question at $m = 6$ comes out* empty *instead of the six values of Theorem 4.3. A second reducible modulus, $x^6 - 2$, makes the same point.*

(2) C1 and the coset hypotheses are not sufficient. *At $m = 6$, $t = 0$, the exponent $e = 14$ is even, satisfies $|C_e| = 6$ and $e \notin C_1$, and fails the root conditions.*

(3) Neither root condition is redundant. *At $m = 6$ the exponent $e = 4$ satisfies C2 and fails C3, and $e = 26$ satisfies C3 and fails C2.*

(4) Evenness of h is not sufficient in Problem 1.1, *witnessed at $(m, h) = (8, 4)$ and $(10, 8)$.*

(5) The results are not vacuous. *At $m = 10$ some t works, $t = 24$ being the smallest; and Problem 1.1 has optimal cells at every even m we reach, so no blanket nonexistence theorem is available for it as it is for Open Problem 7.15.*

Item (1) is not hypothetical. The primitivity test with the $x^n = 1$ clause dropped is what an earlier version of this computation used, and at $m = 6$ it accepted the reducible $x^6 - 1$ and produced three confident optimality verdicts that contradicted Theorem 7.6 of [1]. The contradiction with published mathematics is what exposed it, which is the argument for keeping the external controls of Proposition 3.2 in the loop at every modulus where a new engine or a new carrier is introduced.

9. Verification

Every statement in this paper has been formally verified in Lean 4 (toolchain `v4.32.0`) against *Mathlib* [8], with five exceptions, each flagged where it occurs: the passage from the enumerated primitivity check to "the quotient is a field" (Section 3); the identification of the table route's verdict with the criterion, derived and checked in Section 3 but not proved, which every result past $m = 8$ inherits; the subfield containment step of Corollary 5.4; the coset arithmetic of Remark 5.5; and the factorisation of Remark 7.3. The development contains no `sorry`, and no axiom beyond Lean's own `propext`, `Quot.sound` and `Classical.choice` together with the per-call axiom that `native_decide` emits. Repository reference to be added at submission. What is proved by argument, depending on nothing beyond `propext` and `Quot.sound`: Lemma 5.1 and the arithmetic behind it, part (1) of Theorem 4.4, the equivalence of the decision procedure with the criterion in Proposition 3.1, and the digitwise description of addition there, whose $\mathbb{Z}/3$-valued form additionally uses `Classical.choice`. What is delegated to compiled evaluation, through Lean's `native_decide` and its per-call axiom, is exactly the finite searches: one Boolean per cell in Theorems 4.1, 4.2, 4.3 and 4.4(2), one per residue class in Lemma 5.2, Theorem 5.3 and Proposition 7.1, one per modulus for the primitivity and table self-checks, and one for the 531 441 ring-law triples underlying Lemma 6.1. It is worth recording that Theorem 6.2, which covers infinitely many cells, rests on that single ring-law computation and on Mathlib's finite field theory, and on nothing else; Proposition 7.2 adds no computation at all, inheriting only the searches of the rows it restates.

The searches are large but not extravagant. The full set of 2186 cells at $m = 14$ takes 695 seconds through the table engine, against an aborted single cell at $m = 10$ on the direct scan after twenty

minutes; the $m = 16$ row of Theorem 4.2, with its control, takes 56 minutes and 4.0 GiB of memory, of which the tables themselves are about 1 GB. The same row runs in 15 seconds in C, the interpreter being some 400 times slower per multiplication. Every numerical value quoted in this paper was first produced by an independent implementation — in Python for the small moduli and in C for $m = 14, 16$ — and the formal statement was written against it afterwards; the root lists of Theorem 5.3 and Lemma 5.2 were in addition reproduced element for element by a third implementation sharing no code with either.

References

[1] C. Ding and T. Helleseth, *Optimal ternary cyclic codes from monomials*, IEEE Trans. Inform. Theory **59** (2013), no. 9, 5898–5904; doi:10.1109/TIT.2013.2260795. Preprint: arXiv:1305.0061. The labels used here — Theorem 4.1, Theorem 7.6, Example 7.7, and the nine Open Problems 7.5 and 7.8–7.15 — are collated against arXiv:1305.0061v1, which is the only version on arXiv; we have not seen the typeset version. Three papers that cite the typeset version use the same labels: [2] for Theorem 4.1 and Open Problems 7.9 and 7.10, [3] for Open Problems 7.9, 7.12 and 7.13, and [4] for Theorem 4.1.

[2] J. Bao and H. Zou, *Counterexamples, constructions, and nonexistence results for optimal ternary cyclic codes*, Finite Fields Appl. **112** (2026), Paper No. 102795; doi:10.1016/j.ffa.2026.102795. Preprint: arXiv:2601.12427 (18 January 2026), v1 the only version on arXiv, and the version quoted here.

[3] G. Wu, Z. You, Z. Zha and Y. Zhang, *Several new classes of optimal ternary cyclic codes with two or three zeros*, Des. Codes Cryptogr. **93** (2025), no. 3, 769–786; doi:10.1007/s10623-024-01541-4. Preprint: arXiv:2407.07332. The attribution in Section 1 is their Remark 5 in arXiv:2407.07332v1: "Theorems 5 and 6 give positive support of the open problem 7.9 in [2]", reference [2] there being [1].

[4] P. Zheng, D. He and Q. Liao, *On the Ding and Helleseth's 9th open problem about optimal ternary cyclic codes*, arXiv:2511.01306 (3 November 2025). The two counterexamples used in Section 4 are their Examples 3.1 and 3.2 in v1.

[5] D. He, P. Zheng and Q. Liao, *On the Ding and Helleseth's 8th open problem about optimal ternary cyclic codes*, arXiv:2506.09651 (11 June 2025). Cited only for context, as a partial answer to the eighth of the nine problems.

[6] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, online database, http://www.codetables.de. Entry for a ternary $[242, 232]$ code, accessed 28 August 2026.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1996; doi:10.1017/CBO9780511525926.

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