A DETAILED FINITE-CARRY PROOF OF A CONJECTURE ON PERMUTATION BINOMIALS IN CHARACTERISTIC TWO

YI LI

ABSTRACT. Let $q = 2^m$, where $m \geq 5$ is odd and $3 \mid m$. Tu, Zeng, Jiang and Li formulated a conjecture asserting that if a family of Hermite-type sums $S_{r,\alpha}(y)$, attached to the binomial $x^r(a + x^{3(q-1)})$, vanishes for every α with $3 \mid (1 + \alpha)$, then $y^3 = 1$. We give a detailed proof, including all exceptional and boundary cases. In fact, seven indices suffice: $\alpha \in \{2, 8, 14, 20, 26, 32, 38\}$. The first two indices reduce a hypothetical counterexample to a primitive seventh root of unity. Lucas's theorem then turns the remaining equations into six-bit conditions, and an explicit finite carry elimination completes the proof. The paper records the complete residue tables, their derivation, and a short SageMath verification certificate.

hexagon:2611.00510v1

1. Introduction and statement of the result

Consider the binomial

$$f(X) = X^r\big(a + X^{3(q-1)}\big) \in \mathbb{F}_{q^2}[X], \qquad q = 2^m. \tag{1.1}$$

In their study of the permutation property of (1.1), Tu, Zeng, Jiang and Li [1] reduced the remaining necessity question, for m odd and divisible by 3, to the simultaneous vanishing of certain sums $S_{r,\alpha}(y)$, where $y = a^{(q+1)/3}$. They posed the following assertion as Conjecture 1 of [1]. We state it for arbitrary nonzero y, which is the form useful below.

Theorem 1.1 (Conjecture 1 of Tu–Zeng–Jiang–Li)**.** *Let*

$$q = 2^m, \qquad m \geq 5 \text{ odd}, \qquad 3 \mid m,$$

and let $1 \leq r \leq q$ *and* $y \in \mathbb{F}_{q^2}^*$. *If*

$$S_{r,\alpha}(y) = 0 \quad \text{for every } 0 \leq \alpha \leq q - 1 \text{ such that } 3 \mid (1 + \alpha),$$

then $y^3 = 1$.

The proof below establishes the following stronger version.

Theorem 1.2 (Seven-index strengthening)**.** *Under the assumptions on* q, r, y *in Theorem 1.1, if*

$$S_{r,\alpha}(y) = 0 \quad \text{for } \alpha \in \{2, 8, 14, 20, 26, 32, 38\}, \tag{1.2}$$

then $y^3 = 1$.

The point is that the conclusion is uniform in m and r. Since $m \geq 5$ is odd and divisible by 3, necessarily $m \geq 9$. Thus all seven indices in (1.2) belong to the range $0 \leq \alpha \leq q - 1$.

We proceed as follows. Section 2 derives an exact two- or three-term formula from the original sums. Section 3 explains why $\alpha = 2, 8$ force any counterexample to be a primitive seventh root. Section 4 establishes the six-bit residue table. Sections 5 and 6 separately eliminate nonboundary and boundary values of a normalized real parameter. An appendix gives executable, exact-arithmetic certificates for the finite calculations.

2020 *Mathematics Subject Classification.* 11T06, 11T55, 05A05.

Key words and phrases. Permutation binomial, finite field, Lucas's theorem, binary carries, seventh roots of unity.

Affiliation: School of Computer Science, Shanghai Jiao Tong University,
Shanghai 200240, China. E-mail: yi.li@sjtu.edu.cn.

2. Exact reduction of the sums by Lucas's theorem

2.1. **The original notation.** Put

$$M = \frac{q+1}{3}. \tag{2.1}$$

For $0 \le \alpha \le q-1$ with $3 \mid (1+\alpha)$, define the integer interval

$$I_{r,\alpha} = [\,-r(1+\alpha) + 3\alpha - 3(q-1),\ -r(1+\alpha) + 3\alpha\,] \tag{2.2}$$

and let $\ell_{r,\alpha}$ be the least integer ℓ for which $\ell(q+1) \in I_{r,\alpha}$. Following equation (6) of [1], set

$$B_{r,\alpha} = q - 1 - \alpha + \frac{r(1+\alpha)}{3} + \ell_{r,\alpha} M. \tag{2.3}$$

The reduced sum is

$$S_{r,\alpha}(y) = \sum_{t \in T_{r,\alpha}} \sum_{i=0}^{\alpha} \binom{\alpha}{i} \binom{q-1-\alpha}{tM + B_{r,\alpha} - i} y^{t-3i}, \tag{2.4}$$

where $T_{r,\alpha} = \{0,1\}$ or $\{0,1,2\}$ according as $I_{r,\alpha}$ contains two or three multiples of $q+1$. We interpret a binomial coefficient with an out-of-range lower argument as zero and work in characteristic two.

For the chosen indices, write

$$\alpha_c = 3c - 1, \qquad C = \{1,3,5,7,9,11,13\}. \tag{2.5}$$

Choose x uniquely by

$$0 \le x < M, \qquad x \equiv r - 3 \pmod{M}, \tag{2.6}$$

and for each c write

$$cx = s_c M + w_c, \qquad s_c \in \mathbb{Z}, \quad 0 \le w_c < M. \tag{2.7}$$

The following exact computation is the basis of the proof.

Lemma 2.1 (Exact value of B_{r,α_c})**.** *For every c such that $0 \le \alpha_c \le q-1$, one has*

$$B_{r,\alpha_c} = B_c = \begin{cases} M-1, & w_c = 0, \\ w_c - 1, & 1 \le w_c < M, \end{cases} \tag{2.8}$$

and

$$T_{r,\alpha_c} = \begin{cases} \{0,1\}, & w_c = 0, \\ \{0,1,2\}, & w_c > 0. \end{cases} \tag{2.9}$$

Thus S_{r,α_c} has two terms exactly when $M \mid cx$.

Proof. Write $r - 3 = hM + x$ with $h \in \mathbb{Z}$. Since $1 + \alpha_c = 3c$, the upper endpoint of I_{r,α_c} is

$$-3cr + 3(3c-1) = -3c(r-3) - 3.$$

Also $q - 1 = 3M - 2$, so dividing the entire interval by 3 gives

$$\frac{1}{3} I_{r,\alpha_c} = [\,-c(r-3) - 3M + 1,\ -c(r-3) - 1\,]. \tag{2.10}$$

An integer multiple of $q+1 = 3M$ in I_{r,α_c} corresponds precisely to an integer multiple of M in (2.10). Using $c(r-3) = (ch + s_c)M + w_c$, the latter interval is

$$[\,-(ch + s_c + 3)M - w_c + 1,\ -(ch + s_c)M - w_c - 1\,].$$

If $w_c = 0$, its only multiples of M are $-(ch + s_c + 2)M$ and $-(ch + s_c + 1)M$. If $1 \le w_c < M$, its only multiples of M are $-(ch + s_c + 3)M$, $-(ch + s_c + 2)M$ and $-(ch + s_c + 1)M$. (The endpoint inequalities are inclusive; this is why the case $w_c = 0$ must be treated separately.) It follows that

$$\ell_{r,\alpha_c} = \begin{cases} -ch - s_c - 2, & w_c = 0, \\ -ch - s_c - 3, & w_c > 0. \end{cases}$$

Substitution in (2.3), with

$$B_{r,\alpha_c} = q - 3c + cr + \ell_{r,\alpha_c} M = q + c(r-3) + \ell_{r,\alpha_c} M,$$

gives $B_c = M - 1$ for $w_c = 0$ and $B_c = w_c - 1$ otherwise. The lists of multiples give (2.9) as well. □

2.2. **Why the binomial sum has exactly one Lucas term per layer.** For nonnegative integers u, v, let $u \,\&\, v$ denote their bitwise binary AND. For example, $14 = (1110)_2$ and $11 = (1011)_2$, so $14 \,\&\, 11 = (1010)_2 = 10$.

Lemma 2.2 (Unique Lucas contribution)**.** *Let $0 \le \alpha, \beta \le q-1$. Exactly one integer i gives a nonzero product in $\mathbb{F}_2$*

$$\binom{\alpha}{i}\binom{q-1-\alpha}{\beta-i},$$

namely

$$i = \alpha \,\&\, \beta. \tag{2.11}$$

Consequently,

$$S_{r,\alpha_c}(y) = \sum_{t=0}^{\nu_c - 1} y^{\,t-3(\alpha_c \& (B_c + tM))}, \qquad \nu_c = \begin{cases} 2, & w_c = 0, \\ 3, & w_c > 0. \end{cases} \tag{2.12}$$

Proof. Write α and β in m binary positions. Because $q - 1 = 2^m - 1$ has all m positions equal to 1, α and $q - 1 - \alpha$ have complementary binary supports. Lucas's theorem says that $\binom{\alpha}{i}$ is odd precisely when every 1-bit of i is in the support of α. Similarly, $\binom{q-1-\alpha}{\beta-i}$ is odd precisely when every 1-bit of $\beta - i$ is in the complementary support. There can be no binary carry between these disjoint supports; hence $\beta = i + (\beta - i)$ is the disjoint splitting of the 1-bits of β into the two complementary supports. It is unique, and the first part is exactly $i = \alpha \,\&\, \beta$.

For $w_c = 0$, the relevant lower binomial arguments $\beta_t = B_c + tM$ are $M - 1$ and $2M - 1$. For $w_c > 0$ they are $w_c - 1$, $M + w_c - 1$, $2M + w_c - 1$. All lie in $[0, q-1]$, since $q - 1 = 3M - 2$. Thus the unique-term statement applies to each t in (2.4), and yields (2.12). □

3. The first two indices: reduction to seventh roots

Because $m \ge 9$, the identity $3M = 2^m + 1$ implies

$$M \equiv 3 \pmod 4, \qquad M \equiv 11 \pmod{16}, \qquad M \equiv 43 \pmod{64}. \tag{3.1}$$

Indeed, $3M \equiv 1 \pmod{2^k}$ for $k \le m$, and 3^{-1} modulo $4, 16, 64$ is $3, 11, 43$, respectively.

3.1. **The four trinomials for $\alpha = 2$.** For $c = 1$ we have $\alpha_1 = 2$. If $x \ne 0$, then $B_1 = x - 1$ and

$$S_{r,2}(y) = y^{-3i_0} + y^{1-3i_1} + y^{2-3i_2}, \quad i_t = 2 \,\&\, (x - 1 + tM).$$

Since $2 = (10)_2$, only the bit of value 2 is tested. Using $M \equiv 3 \pmod 4$, we obtain the following complete table.

Table 1. The four possibilities for $S_{r,2}(y)$ when $x \ne 0$.

$x \bmod 4$	(i_0, i_1, i_2)	$S_{r,2}(y)$
0	$(2, 2, 0)$	$y^{-6}(1 + y + y^8)$
1	$(0, 2, 2)$	$y^{-5}(1 + y + y^5)$
2	$(0, 0, 2)$	$y^{-4}(1 + y^4 + y^5)$
3	$(2, 0, 0)$	$y^{-6}(1 + y^7 + y^8)$

Write

$$\begin{aligned} P_0(Y) &= 1 + Y + Y^8, \quad & P_1(Y) &= 1 + Y + Y^5, \\ P_2(Y) &= 1 + Y^4 + Y^5, \quad & P_3(Y) &= 1 + Y^7 + Y^8. \end{aligned} \tag{3.2}$$

Since $y \ne 0$, the vanishing of $S_{r,2}(y)$ in the trinomial case is equivalent to $P_i(y) = 0$ for one of these four polynomials.

TABLE 2. All 16 residues for the trinomial $S_{r,8}(y)$.

$b \bmod 16$	(i_0, i_1, i_2)	monomial-free polynomial
$0, 1$	$(0, 8, 0)$	H_6
$2, 3, 4$	$(0, 8, 8)$	H_2
$5, 6, 7$	$(0, 0, 8)$	H_3
$8, 9$	$(8, 0, 8)$	H_4
$10, 11, 12$	$(8, 0, 0)$	H_5
$13, 14, 15$	$(8, 8, 0)$	H_1

3.2. **The six trinomials for $\alpha = 8$.** For $c = 3$ we have $\alpha_3 = 8$. In its trinomial case, put $b = B_3 \bmod 16$. Since $8 = (1000)_2$, the value of $i_t = 8 \,\&\, (B_3 + tM)$ depends only on $b + 11t \pmod{16}$. One obtains:

Here

$$\begin{aligned} H_1(Y) &= 1 + Y + Y^{26}, & H_2(Y) &= 1 + Y + Y^{23}, \\ H_3(Y) &= 1 + Y^{22} + Y^{23}, & H_4(Y) &= 1 + Y^2 + Y^{25}, \\ H_5(Y) &= 1 + Y^{25} + Y^{26}, & H_6(Y) &= 1 + Y^{23} + Y^{25}. \end{aligned} \tag{3.3}$$

For example, if $b \equiv 13 \pmod{16}$ then $(i_0, i_1, i_2) = (8, 8, 0)$ and

$$S_{r,8}(y) = y^{-24} + y^{-23} + y^2 = y^{-24} H_1(y).$$

3.3. **All 24 common factors and the binomial exceptions.** Put $Q(Y) = Y^2 + Y + 1$. Euclid's algorithm in $\mathbb{F}_2[Y]$ gives Table 3, recording every pair, not merely the two exceptional pairs. An executable verification is included in Appendix A.

TABLE 3. The 24 gcds $\gcd(P_i, H_j)$ over $\mathbb{F}_2[Y]$; $Q = Y^2 + Y + 1$.

	H_1	H_2	H_3	H_4	H_5	H_6
P_0	Q	Q	Q	Q	Q	Q
P_1	P_1	Q	Q	Q	Q	Q
P_2	Q	Q	Q	Q	P_2	Q
P_3	Q	Q	Q	Q	Q	Q

The two exceptional entries can also be seen without a gcd program. Modulo P_1, one has $Y^5 = Y + 1$, whence

$$Y^{25} = (Y^5)^5 = (Y + 1)^5 \equiv Y^5 + Y^4 + Y + 1 \equiv Y^4,$$

and therefore $Y^{26} \equiv Y + 1$. Hence $P_1 \mid H_1$. Taking reciprocal polynomials shows that $P_2 \mid H_5$. Moreover,

$$\begin{aligned} P_1(Y) &= (Y^2 + Y + 1)(Y^3 + Y^2 + 1), \\ P_2(Y) &= (Y^2 + Y + 1)(Y^3 + Y + 1). \end{aligned} \tag{3.4}$$

We also need to check the possibility of two-term sums. If $S_{r,2}$ is a binomial, then $x = 0$, so $S_{r,8}$ is also binomial. Formula (2.12) gives

$$S_{r,2}(y) = y^{-6} + y, \qquad S_{r,8}(y) = y^{-24} + y.$$

Their simultaneous vanishing implies $y^7 = y^{25} = 1$ and hence $y = 1$. If $S_{r,2}$ is a trinomial but $S_{r,8}$ is a binomial, the second equation gives $y^{25} = 1$. However, $\operatorname{ord}(y)$ divides $q^2 - 1 = 4^m - 1$, and because m is odd,

$$4^m - 1 \equiv (-1)^m - 1 \equiv 3 \pmod{5}.$$

Thus $\gcd(25, q^2 - 1) = 1$, so $y = 1$. This is impossible for a three-term sum in characteristic two, since $S_{r,2}(1) = 1 + 1 + 1 = 1$.

We have proved the following key lemma.

Lemma 3.1 (Reduction to seventh roots)**.** *If $S_{r,2}(y) = S_{r,8}(y) = 0$ and $y^3 \neq 1$, then precisely one of*

$$y^3 + y + 1 = 0, \qquad y^3 + y^2 + 1 = 0 \tag{3.5}$$

holds. In either case $y \in \mathbb{F}_8^*$ has multiplicative order 7.

Proof. The binomial possibilities have just been excluded. If both sums are trinomials, y is a common root of some P_i, H_j. Table 3 shows that either $Q(y) = 0$ or $P_1(y) = 0$ or $P_2(y) = 0$. The first possibility gives $y^3 = 1$, contrary to the hypothesis. Factoring the latter two polynomials as in (3.4) gives (3.5). Each cubic in (3.5) has no root in $\mathbb{F}_2$ and hence is irreducible. Its nonzero roots lie in $\mathbb{F}_8^*$, a cyclic group of prime order 7. The roots are not 1, so their order is 7. They cannot satisfy both cubics, since subtracting the equations would give $y^2 + y = 0$, which is incompatible with either cubic. □

4. Fano-plane relations and the six-bit table

Suppose from now on, for contradiction, that all seven sums in (1.2) vanish but $y^3 \neq 1$. By Lemma 3.1, y is a primitive seventh root. We use the terminology

$$\begin{aligned} &\text{type } +: \quad y^3 + y + 1 = 0, \\ &\text{type } -: \quad y^3 + y^2 + 1 = 0. \end{aligned} \tag{4.1}$$

4.1. **Reduction to six binary positions.** Set

$$\theta = \frac{x}{M} \in [0, 1), \qquad \rho = x \pmod{64}, \tag{4.2}$$

where ρ is always represented by an integer in $\{0, \ldots, 63\}$. For each $c \in C$ put $k_c = \lfloor c\theta \rfloor$. If $c\theta \notin \mathbb{Z}$, then $w_c = cx - k_c M$ lies in $\{1, \ldots, M-1\}$, so (2.8) and (3.1) yield

$$b_c := B_c \pmod{64} \equiv c\rho - 43k_c - 1 \pmod{64}. \tag{4.3}$$

If $c\theta \in \mathbb{Z}$, the sum is instead a binomial, with

$$B_c \equiv M - 1 \equiv 42 \pmod{64}. \tag{4.4}$$

Since $\alpha_c = 3c - 1 \leq 38 < 64$, the binary AND with α_c uses only the lowest six bits of $B_c + tM$. Thus, in the trinomial case, the exponents may be reduced modulo 7 as

$$e_t \equiv t - 3\left(\alpha_c \,\&\, \left((b_c + 43t) \bmod 64\right)\right) \pmod{7}, \quad t = 0, 1, 2. \tag{4.5}$$

The vanishing condition is exactly

$$y^{e_0} + y^{e_1} + y^{e_2} = 0. \tag{4.6}$$

4.2. **Why the exponent sets are translates of two triples.**

Lemma 4.1 (The seven additive lines)**.** *Let $y \in \mathbb{F}_8^*$ have order 7. For three integers e_0, e_1, e_2, the equality* (4.6) *holds if and only if the residues e_0, e_1, e_2 are distinct and, for some $h \in \mathbb{Z}/7\mathbb{Z}$,*

$$\{e_0, e_1, e_2\} \equiv \begin{cases} h + \{0, 1, 3\} \pmod{7}, & \textit{type } +, \\ h + \{0, 2, 3\} \pmod{7}, & \textit{type } -. \end{cases} \tag{4.7}$$

Proof. For type +, the defining equation is $1 + y + y^3 = 0$. Multiplying by y^h gives $y^h + y^{h+1} + y^{h+3} = 0$, which proves sufficiency of the seven translates of $\{0, 1, 3\}$. Similarly, type − gives the seven translates of $\{0, 2, 3\}$.

For necessity, if two of the three exponents agree modulo 7, their two equal powers cancel in characteristic two and the remaining nonzero power cannot vanish. Hence all three powers are distinct. In $\mathbb{F}_8$, each unordered pair of distinct nonzero elements a, b uniquely determines the zero-sum triple $\{a, b, a + b\}$. There are $\binom{7}{2} = 21$ pairs, and every triple contains three pairs, so there are exactly $21/3 = 7$ zero-sum triples. The seven translates above are distinct (a nonzero translation of $\mathbb{Z}/7\mathbb{Z}$ cannot stabilize a three-element subset), so they exhaust all possibilities. □

For reference, the type + lines are

$$\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\\ \{0,4,5\},\{1,5,6\},\{0,2,6\}, \tag{4.8}$$

whereas the type − lines are

$$\{0,2,3\},\{1,3,4\},\{2,4,5\},\{3,5,6\},\\ \{0,4,6\},\{0,1,5\},\{1,2,6\}. \tag{4.9}$$

These are the seven lines of the additive Fano plane of $\mathbb{F}_8$.

4.3. **Derivation and complete statement of the residue table.** For each $c \in C$, let $\mathcal{R}_c^+$ (respectively $\mathcal{R}_c^-$) denote the set of residues b_c mod 64 for which the trinomial vanishes at a type + (respectively type −) seventh root. Equations (4.5) and (4.7) make this a finite test of 64 residues for each c. For a set $A \subseteq \mathbb{Z}/64\mathbb{Z}$, the notation $A + d\mathbb{Z}_{64}$ means all residues congruent modulo d to some member of A.

TABLE 4. Complete permissible trinomial residues $b_c \pmod{64}$.

c	$\mathcal{R}_c^+$	$\mathcal{R}_c^-$
1	$1 + 4\mathbb{Z}_{64}$	$4\mathbb{Z}_{64}$
3	$\{10,11,12\} + 16\mathbb{Z}_{64}$	$\{13,14,15\} + 16\mathbb{Z}_{64}$
5	$\{10,12,14\} + 16\mathbb{Z}_{64}$	$\{11,13,15\} + 16\mathbb{Z}_{64}$
7	$\{9,16,18,19\} + 32\mathbb{Z}_{64}$	$\{0,22,23,25\} + 32\mathbb{Z}_{64}$
9	$\{1,7,9,11,13,16,19\} + 32\mathbb{Z}_{64}$	$\{0,2,8,22,25,28,30\} + 32\mathbb{Z}_{64}$
11	$\{32,33,\ldots,41\}$	$\{0,1,\ldots,9\}$
13	$\{0,8,13,15,38,49,58,60\}$	$\{3,26,28,33,41,45,47,56\}$

Here are three hand-checkable examples.

(i) $c = 1$. Here $\alpha_1 = 2$ and $43 \equiv 3 \pmod 4$. For $b_1 \equiv 0,1,2,3 \pmod 4$, respectively, the triples $(e_0, e_1, e_2) \pmod 7$ are

$$(0,2,3), \qquad (0,1,3), \qquad (1,1,2), \qquad (1,2,2).$$

Thus $\mathcal{R}_1^+ = 1 + 4\mathbb{Z}_{64}$ and $\mathcal{R}_1^- = 4\mathbb{Z}_{64}$.

(ii) $c = 3$. Here $\alpha_3 = 8$ and only $b_3 \pmod{16}$ matters. The six groups of b_3 in Table 2 give the exponent triples

$$(0,5,2),\ (0,5,6),\ (0,1,6),\ (4,1,6),\ (4,1,2),\ (4,5,2).$$

Only the fifth group is a type + line: $\{4,1,2\} = 1 + \{0,1,3\}$. Only the sixth group is a type − line: $\{4,5,2\} = 2 + \{0,2,3\}$. This gives the second row of Table 4.

(iii) $c = 13$, *one entry.* Here $\alpha_{13} = 38$. If $b_{13} = 0$, the three six-bit inputs $b_{13} + 43t \pmod{64}$ are $0, 43, 22$. Their ANDs with 38 are $0, 34, 6$, so

$$(e_0, e_1, e_2) = (0, 1 - 3 \cdot 34, 2 - 3 \cdot 6) \equiv (0,4,5) \pmod 7.$$

Since $\{0,4,5\} = 4 + \{0,1,3\}$, the residue $b_{13} = 0$ belongs to $\mathcal{R}_{13}^+$. The other entries are obtained by the same six-bit calculation, as verified in Appendix A.

Notice that the seven residues b_c in Table 4 are *not independent*: by (4.3), all depend on the same pair (θ, ρ). This dependence drives the elimination.

5. Elimination of the nonboundary carry states

We first assume that

$$c\theta \notin \mathbb{Z} \quad \text{for every } c \in C. \tag{5.1}$$

Equivalently, θ is not any breakpoint j/c with $0 \le j \le c$ and $c \in C$. Hence all seven sums under consideration are trinomials, so Table 4 applies without exception.

5.1. **Deriving the four surviving regions.** Since $0 \le \theta < 1$, we have $k_1 = 0$, and therefore

$$b_1 \equiv \rho - 1, \qquad b_3 \equiv 3\rho - 43k_3 - 1, \qquad b_5 \equiv 5\rho - 43k_5 - 1 \pmod{64}. \tag{5.2}$$

The $c = 1$ row of Table 4 gives

$$\rho \equiv \begin{cases} 2 \pmod 4, & \text{type } +, \\ 1 \pmod 4, & \text{type } -. \end{cases} \tag{5.3}$$

Now $k_3 = \lfloor 3\theta \rfloor \in \{0, 1, 2\}$. For $c = 3$ only reduction modulo 16 is needed, and $43 \equiv 11 \pmod{16}$ gives

$$b_3 \equiv 3\rho - 11k_3 - 1 \pmod{16}.$$

Checking $\rho = 2, 6, 10, 14 \pmod{16}$ for type + and $\rho = 1, 5, 9, 13 \pmod{16}$ for type − yields:

TABLE 5. Survivors after imposing $c = 1, 3$; an empty entry means no residue survives.

k_3	interval for θ	type +: $\rho \pmod{16}$	type −: $\rho \pmod{16}$
0	$(0, \frac{1}{3})$	none	5
1	$(\frac{1}{3}, \frac{2}{3})$	2	9
2	$(\frac{2}{3}, 1)$	6	none

To illustrate: for type + and $k_3 = 1$, the four possible values $\rho \equiv 2, 6, 10, 14 \pmod{16}$ give $3\rho - 12 \equiv 10, 6, 2, 14 \pmod{16}$. Only 10 lies in $\{10, 11, 12\}$, so $\rho \equiv 2 \pmod{16}$.

Next $k_5 = \lfloor 5\theta \rfloor$, where $k_5 = j$ corresponds to the open interval $(j/5, (j+1)/5)$. The $c = 5$ condition is

$$b_5 \equiv 5\rho - 11k_5 - 1 \pmod{16}, \qquad \begin{cases} b_5 \in \{10, 12, 14\}, & \text{type } +, \\ b_5 \in \{11, 13, 15\}, & \text{type } -. \end{cases} \tag{5.4}$$

For each of the four nonempty entries in Table 5, testing the compatible k_5's leaves just the rows below. The displayed b_5 values are reduced modulo 16.

TABLE 6. All survivors after $c = 1, 3, 5$: the carry indices and resulting intervals.

Type	k_3	k_5	interval for θ	$\rho \pmod{16}$	$b_5 \pmod{16}$
+	1	1	$(\frac{1}{3}, \frac{2}{5})$	2	14
+	2	3	$(\frac{2}{3}, \frac{4}{5})$	6	12
−	0	1	$(\frac{1}{5}, \frac{1}{3})$	5	13
−	1	3	$(\frac{3}{5}, \frac{2}{3})$	9	11

For example, in the first row, $\rho \equiv 2 \pmod{16}$ gives $b_5 \equiv 9 - 11k_5 \pmod{16}$. Of the compatible values $k_5 = 1, 2, 3$, only $k_5 = 1$ gives a permitted type + residue (14), and

$$(\tfrac{1}{3}, \tfrac{2}{3}) \cap (\tfrac{1}{5}, \tfrac{2}{5}) = (\tfrac{1}{3}, \tfrac{2}{5}).$$

The other three rows follow by exactly the same calculation.

Because we ultimately work modulo 64, each class modulo 16 corresponds to four residues. Thus Table 6 is precisely the following table.

TABLE 7. The four nonboundary states after $c = 1, 3, 5$.

Type	interval for θ	possible $\rho \pmod{64}$
+	$(\frac{1}{3}, \frac{2}{5})$	$\{2, 18, 34, 50\}$
+	$(\frac{2}{3}, \frac{4}{5})$	$\{6, 22, 38, 54\}$
−	$(\frac{1}{5}, \frac{1}{3})$	$\{5, 21, 37, 53\}$
−	$(\frac{3}{5}, \frac{2}{3})$	$\{9, 25, 41, 57\}$

We now eliminate these four regions. Each numerical residue below is obtained from (4.3), and the permissible residues are given in Table 4.

5.2. **Eliminating the type-plus regions.**
First region: $1/3 < \theta < 2/5$. Here $k_7 = \lfloor 7\theta \rfloor = 2$ and $\rho \in \{2, 18, 34, 50\}$. The four values of $b_7 \pmod{32}$ are

ρ		2	18	34	50
b_7	(mod 32)	23	7	23	7

But the type + row for $c = 7$ allows only $\{9, 16, 18, 19\} \pmod{32}$, so this region is empty.
Second region: $2/3 < \theta < 4/5$. Initially $\rho \in \{6, 22, 38, 54\}$. The carry k_7 changes at $\theta = 5/7$. If $2/3 < \theta < 5/7$, then $k_7 = 4$, and

$$(b_7 \bmod 32)_{\rho=6,22,38,54} = (29, 13, 29, 13).$$

None is permitted, so this subinterval is empty.

For $5/7 < \theta < 4/5$, one has $k_7 = 5$, giving

ρ		6	22	38	54
b_7	(mod 32)	18	2	18	2

$$\implies \quad \rho \in \{6, 38\}. \tag{5.5}$$

The next carry k_9 changes at $\theta = 7/9$. For $5/7 < \theta < 7/9$, $k_9 = 6$ and

$$(b_9 \bmod 32)_{\rho=6,38} = (19, 19),$$

which is permitted for both residues. For $7/9 < \theta < 4/5$, $k_9 = 7$ and the two values are $(8, 8) \pmod{32}$, so both are excluded.

It remains to treat $5/7 < \theta < 7/9$. The carry k_{11} changes at $\theta = 8/11$:

(a) If $5/7 < \theta < 8/11$, then $k_{11} = 7$. For $\rho = 6, 38$ formula (4.3) gives $(b_{11} \bmod 64) = (20, 52)$, outside $\mathcal{R}_{11}^+ = \{32, \dots, 41\}$. Hence this interval is empty.

(b) If $8/11 < \theta < 7/9$, then $k_{11} = 8$, giving $(b_{11} \bmod 64) = (41, 9)$. This keeps only $\rho = 6$. Here $k_{13} = 9$ or 10, depending on whether $\theta < 10/13$ or $\theta > 10/13$. In either case,

$$b_{13} \equiv 13 \cdot 6 - 43k_{13} - 1 \equiv \begin{cases} 10, & k_{13} = 9, \\ 31, & k_{13} = 10 \end{cases} \pmod{64}.$$

Neither 10 nor 31 belongs to $\mathcal{R}_{13}^+ = \{0, 8, 13, 15, 38, 49, 58, 60\}$. Thus this interval is empty as well.

We conclude that *both* type + regions are impossible.

5.3. **Eliminating the type-minus regions.**
First region: $1/5 < \theta < 1/3$. Initially $\rho \in \{5, 21, 37, 53\}$. The carry k_7 changes at $2/7$. If $2/7 < \theta < 1/3$, then $k_7 = 2$ and

$$(b_7 \bmod 32)_{\rho=5,21,37,53} = (12, 28, 12, 28),$$

none of which is permitted by $\mathcal{R}_7^- = \{0, 22, 23, 25\} + 32\mathbb{Z}_{64}$. If $1/5 < \theta < 2/7$, then $k_7 = 1$ and

$$(b_7 \bmod 32)_{\rho=5,21,37,53} = (23, 7, 23, 7), \qquad \rho \in \{5, 37\}.$$

The carry k_9 changes at $2/9$. For $1/5 < \theta < 2/9$, one has $k_9 = 1$ and $(b_9 \bmod 32)_{\rho=5,37} = (1, 1)$, which is outside the permitted set $\{0, 2, 8, 22, 25, 28, 30\}$. Thus there is no solution there. For $2/9 < \theta < 2/7$, one has $k_9 = 2$ and $(b_9 \bmod 32)_{\rho=5,37} = (22, 22)$, so both remain.

The carry k_{11} changes at $3/11$ inside this interval. If $3/11 < \theta < 2/7$, then $k_{11} = 3$ and $(b_{11} \bmod 64)_{\rho=5,37} = (53, 21)$, neither of which belongs to $\mathcal{R}_{11}^- = \{0, 1, \dots, 9\}$. If $2/9 < \theta < 3/11$, then $k_{11} = 2$ and $(b_{11} \bmod 64)_{\rho=5,37} = (32, 0)$, so only $\rho = 37$ remains. For this last residue,

$$b_{13} \equiv 13 \cdot 37 - 43k_{13} - 1 \pmod{64}.$$

Here $k_{13} = 2$ or 3, according as $\theta < 3/13$ or $\theta > 3/13$; consequently

$$b_{13} \equiv 10 \text{ or } 31 \pmod{64}.$$

Neither value lies in $\mathcal{R}_{13}^- = \{3, 26, 28, 33, 41, 45, 47, 56\}$. Hence the first type − region is impossible.

Second region: $3/5 < \theta < 2/3$. Here $k_7 = 4$ and $\rho \in \{9, 25, 41, 57\}$. The values of $b_7 \pmod{32}$ are $(18, 2, 18, 2)$, none of which lies in $\{0, 22, 23, 25\}$. This last region is therefore empty.

We have proved the following conclusion.

Proposition 5.1 (No nonboundary seventh-root solutions)**.** *Under* (5.1)*, it is impossible for all seven sums* (1.2) *to vanish at a primitive seventh root of either type.*

6. Elimination of the boundary carry states

The previous section assumed that every $c\theta$ was nonintegral. We now remove that restriction. Suppose that

$$\theta = \frac{x}{M} = \frac{j}{d} \in [0, 1) \tag{6.1}$$

is a breakpoint in lowest terms. Because $dx = jM$ and $\gcd(j, d) = 1$, Euclid's lemma gives $d \mid M$. Since the breakpoint is j'/c for some $c \in C$, the reduced denominator d also divides one of the integers in C. Therefore

$$d \in \{1, 3, 5, 7, 9, 11, 13\}.$$

Lemma 6.1 (Possible breakpoint denominators)**.** *Under the hypotheses $m \geq 9$ odd and $3 \mid m$, any breakpoint that can arise from x/M has reduced denominator*

$$d \in \{1, 3, 9, 11\}. \tag{6.2}$$

Proof. If $d \mid M$, then $2^m = 3M - 1 \equiv -1 \pmod{d}$. For $d = 5$, the multiplicative order of 2 (mod 5) is 4, and $2^m = -1 \pmod 5$ would require $m \equiv 2 \pmod 4$, contrary to m odd. For $d = 7$, the powers of 2 are $1, 2, 4 \pmod 7$ and never -1. For $d = 13$, the order of 2 is 12 and $2^6 \equiv -1 \pmod{13}$; thus $2^m \equiv -1 \pmod{13}$ would require $m \equiv 6 \pmod{12}$, again impossible for odd m. Consequently $d \notin \{5, 7, 13\}$, proving (6.2). □

6.1. **The boundary residue ρ is determined.** For $d \in \{1, 3, 9, 11\}$, the integer d is odd and therefore invertible modulo 64. Reducing $dx = jM$ modulo 64 gives

$$\boxed{\rho \equiv 43j\, d^{-1} \pmod{64}.} \tag{6.3}$$

The inverses for $d = 1, 3, 9, 11$ are $1, 43, 57, 35$, respectively. For example, $\theta = 2/9$ gives $\rho \equiv 43 \cdot 2 \cdot 57 \equiv 38 \pmod{64}$.

For $\theta > 0$ we have $c = 1$ in the trinomial case, and thus Table 4 imposes

$$\rho \equiv \begin{cases} 2 \pmod 4, & \text{type } +, \\ 1 \pmod 4, & \text{type } -. \end{cases} \tag{6.4}$$

Using (6.3), this produces the short list in Table 8. For instance, when $d = 11$, equation (6.3) becomes $\rho \equiv 33j \pmod{64}$, hence $\rho \equiv j \pmod 4$. For type + this allows $j = 2, 6, 10$; for type $-$ it allows $j = 1, 5, 9$. The cases $d = 3$ and $d = 9$ are just as elementary.

The point $\theta = 0$ needs a special comment: then $x = 0$, and $S_{r,2}(y) = y^{-6} + y = 0$ for any primitive seventh root y. Thus it survives the first filter for both types, despite being binomial rather than trinomial.

6.2. **Excluding the remaining boundary states with $c = 3$.** For every trinomial entry in Table 8, one has $k_3 = \lfloor 3\theta \rfloor$ and $b_3 \equiv 3\rho - 43k_3 - 1 \pmod{64}$. The four type + entries give

$$b_3 \equiv 5, 49, 38, 7 \pmod{64}, \quad b_3 \bmod 16 \in \{5, 1, 6, 7\},$$

whereas $\mathcal{R}_3^+$ requires $b_3 \bmod 16 \in \{10, 11, 12\}$. Likewise, the four type $-$ entries give

$$b_3 \equiv 34, 3, 56, 36 \pmod{64}, \quad b_3 \bmod 16 \in \{2, 3, 8, 4\},$$

whereas $\mathcal{R}_3^-$ requires $\{13, 14, 15\} \pmod{16}$. Thus all eight trinomial entries are excluded.

The only remaining distinct boundary values are $\theta = 0, 1/3, 2/3$, for which $3\theta \in \mathbb{Z}$. The corresponding $c = 3$ sums are binomials with

$$B_3 \equiv 42 \pmod{64}, \qquad B_3 + M \equiv 21 \pmod{64}.$$

TABLE 8. All boundary states surviving $c = 1$, and their $c = 3$ data. For a trinomial entry, b_3 is shown modulo 64.

Type	θ	ρ	$c = 3$ value
$+$	0	0	binomial: $B_3 \equiv 42$
$+$	2/11	2	$b_3 \equiv 5$
$+$	2/9	38	$b_3 \equiv 49$
$+$	6/11	6	$b_3 \equiv 38$
$+$	2/3	50	binomial: $B_3 \equiv 42$
$+$	10/11	10	$b_3 \equiv 7$
$-$	0	0	binomial: $B_3 \equiv 42$
$-$	1/11	33	$b_3 \equiv 34$
$-$	1/3	57	binomial: $B_3 \equiv 42$
$-$	5/11	37	$b_3 \equiv 3$
$-$	7/9	5	$b_3 \equiv 56$
$-$	9/11	41	$b_3 \equiv 36$

Since $\alpha_3 = 8$, the two Lucas indices are

$$i_0 = 8 \,\&\, 42 = 8, \qquad i_1 = 8 \,\&\, 21 = 0.$$

Thus the exponents are -24 and 1. For a primitive seventh root, these are 4 and 1 modulo 7, which are distinct, and two nonzero powers of a characteristic-two field cannot add to zero unless they agree. Equivalently, $y^{-24} + y = 0$ would imply $y^{25} = 1$, incompatible with $\mathrm{ord}(y) = 7$.

Proposition 6.2 (No boundary seventh-root solutions)**.** *No breakpoint $\theta = x/M$ can satisfy all seven vanishing conditions* (1.2) *at a primitive seventh root of either type.*

7. Proof of the theorems

Proof of Theorem 1.2. Assume (1.2). Suppose, for contradiction, that $y^3 \neq 1$. Lemma 3.1 then forces y to have order 7 and to be of type $+$ or type $-$. The number $\theta = x/M$ is either a breakpoint or is not. Proposition 5.1 rules out the nonboundary case; Proposition 6.2 rules out the boundary case. Both possibilities give a contradiction. Therefore $y^3 = 1$. □

Proof of Theorem 1.1. The hypotheses of Theorem 1.1 include the seven indices in (1.2). Apply Theorem 1.2. □

Remark 7.1. *For $m \geq 9$, the only congruence about M needed for the final elimination is $M \equiv 43 \pmod{64}$. The reduction is thus uniform in the original field size, and the remaining checks are exact calculations on six binary digits. The proof uses finite enumerations as explicit certificates, not a numerical search over arbitrarily large finite fields.*

Appendix A. Reproducible finite certificates in SageMath

For completeness, the short SageMath code below verifies Tables 3 and 4, then checks every open carry cell and every arithmetically possible boundary. It uses integer modular arithmetic and exact rational arithmetic; no floating-point comparisons are involved. The code is supplementary to the case-by-case elimination in Sections 5–6.

A.1. The 24 polynomial gcds.

```
R.<Y> = PolynomialRing(GF(2))
P = [1+Y+Y^8, 1+Y+Y^5, 1+Y^4+Y^5, 1+Y^7+Y^8]
H = [1+Y+Y^26, 1+Y+Y^23, 1+Y^22+Y^23,
     1+Y^2+Y^25, 1+Y^25+Y^26, 1+Y^23+Y^25]
Q = Y^2+Y+1
for i in range(4):
    for j in range(6):
        expected = P[1] if (i, j) == (1, 0) else (
                   P[2] if (i, j) == (2, 4) else Q)
```

```
        assert gcd(P[i], H[j]) == expected
assert P[1] == Q * (Y^3+Y^2+1)
assert P[2] == Q * (Y^3+Y+1)
```

A.2. The six-bit residue table and all carry states. The predicate `zero` uses Lemma 4.1 for three terms and equality of the two exponent classes for two terms. The last loops cover all the breakpoints j/c, all the open intervals between consecutive breakpoints, and both root types.

```
from fractions import Fraction
C = (1, 3, 5, 7, 9, 11, 13)
BASE = {'+': (0, 1, 3), '-': (0, 2, 3)}
LINES = {t: {frozenset((h+a) % 7 for a in base)
             for h in range(7)}
         for t, base in BASE.items()}

def zero(c, b, typ, n=3):
    A = 3*c-1
    e = [(t-3*(A & ((b+43*t) % 64))) % 7
         for t in range(n)]
    if n == 2:
        return e[0] == e[1]
    return len(set(e)) == 3 and frozenset(e) in LINES[typ]

# Reconstruct Table 1 (all seven rows and both types).
for c in C:
    for typ in ('+', '-'):
        allowed = [b for b in range(64) if zero(c,b,typ)]
        print(c,typ,allowed)

# Each open cell has fixed floor(c*theta), for all c in C.
D = sorted({Fraction(j,c) for c in C for j in range(c+1)})
assert len(D) == 42

def is_survivor(theta, rho, typ):
    for c in C:
        v = c*theta
        if v.denominator == 1:
            b,n = 42,2
        else:
            k = v.numerator // v.denominator
            b,n = (c*rho-43*k-1) % 64,3
        if not zero(c,b,typ,n):
            return False
    return True

for typ in ('+', '-'):
    for a,b in zip(D,D[1:]):
        mid = (a+b)/2
        assert not any(is_survivor(mid,rho,typ)
                       for rho in range(64))
    for theta in D[:-1]:
        d,j = theta.denominator,theta.numerator
        if d not in (1,3,9,11):
            continue                # not realizable as x/M
        rho = (43*j*pow(d,-1,64)) % 64
        assert not is_survivor(theta,rho,typ)
print('All six-bit checks passed.')
```

References

[1] Z. Tu, X. Zeng, Y. Jiang and Y. Li, *Binomial permutations over finite fields with even characteristic*, Designs, Codes and Cryptography **89** (2021), 2869–2888, https://doi.org/10.1007/s10623-021-00959-4.