DISTINCT COVERING SYSTEMS OF $\mathbb{F}_q[x]$: MINIMAL LEAST COMMON MULTIPLES, AND AN EXPLICIT SYSTEM OVER $\mathbb{F}_3$

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. A covering system of $\mathbb{F}_q[x]$ is a finite family of congruence classes $f \equiv r_i \pmod{m_i}$, the m_i monic and non-constant, whose union is all of $\mathbb{F}_q[x]$; it is *distinct* when the moduli are pairwise different. Recent work of B. Wang shows that no such system exists for $q > 73$, and Li, Wang, Wang and Yi ask for an explicit example in the range that is left; the only examples we have found in print are Azlin's, all of them over $\mathbb{F}_2$. We introduce the quantity $\Lambda(q, d)$, the least degree of the least common multiple of a distinct covering system of $\mathbb{F}_q[x]$ all of whose moduli have degree at least d, and determine or bound it in five cases. Our main result is an explicit distinct covering system of $\mathbb{F}_3[x]$ with eleven congruences and least common multiple $x^2(x-1)(x-2)$, together with the proof that no distinct covering system of $\mathbb{F}_3[x]$ has a least common multiple of smaller degree: $\Lambda(3,1) = 4$. We also show $\Lambda(2,1) = 2$ and $\Lambda(2,2) = 4$ — so that Azlin's two systems are optimal for their minimum modulus degree — prove $7 \le \Lambda(2,3) \le 8$ by exhibiting a system of 25 congruences with all moduli of degree at least 3, prove $\Lambda(3,2) \ge 6$, and give the first lower bound for the $\mathbb{F}_q[x]$ analogue of the Erdős–Selfridge odd covering problem: over $\mathbb{F}_2$, no distinct covering system has its moduli dividing a common multiple of degree less than 11 that is divisible by no linear polynomial. All statements are machine-checked in Lean 4.

1. INTRODUCTION

Let q be a prime power and let $\mathbb{F}_q[x]$ be the polynomial ring over the field with q elements. A *covering system* of $\mathbb{F}_q[x]$ is a finite family of congruence classes

$$f \equiv r_i \pmod{m_i}, \qquad i = 1, \dots, k,$$

with each modulus m_i monic and non-constant, such that every $f \in \mathbb{F}_q[x]$ satisfies at least one of the congruences. The system is *distinct* when the m_i are pairwise different — equivalently, in Azlin's phrasing, pairwise non-associate, since a monic representative of each associate class is unique. This is the exact transcription to $\mathbb{F}_q[x]$ of Erdős's covering systems of $\mathbb{Z}$ [7], with the norm $|m| = q^{\deg m}$ playing the role of the modulus.

The subject over $\mathbb{F}_q[x]$ begins with Azlin's thesis [1], which sets up the definitions, proves that a system covers $\mathbb{F}_q[x]$ as soon as it covers one period, and displays a list of explicit systems, *all of them over* $\mathbb{F}_2$. The recent literature transfers the distortion method of Balister, Bollobás, Morris, Sahasrabudhe and Tiba [2] — itself the successor of Hough's solution [9] of Erdős's minimum modulus problem — to global function fields. Li, Wang, Wang and Yi [11] prove that the minimum modulus degree of a covering system of $\mathbb{F}_q[x]$ is bounded, disproving a conjecture of Azlin, and in [12] prove that no covering system of $\mathbb{F}_q[x]$ with distinct moduli exists for $q \ge 759$, improved in a remark of the same paper to $q \ge 720$; B. Wang [17] sharpens this to the following.

Theorem 1.1 ([17, Theorem 1.3])**.** *There is no covering system of $\mathbb{F}_q[x]$ with distinct moduli for $q > 73$.*

So the existence question is alive exactly in the range $3 \le q \le 73$, and [12] asks for it in as many words: *"An interesting problem is to find examples of covering systems of $\mathbb{F}_q[x]$ with distinct moduli for $3 \le q < 720$"*. The two examples printed in [12, §1] are Azlin's, and both are over $\mathbb{F}_2$. We are not aware of any explicit distinct covering system of $\mathbb{F}_q[x]$ in the literature for any $q > 2$.

Two features of the problem are worth separating before we state results. First, distinctness carries the whole content: without it, two classes modulo x already cover $\mathbb{F}_q[x]$. Second, the natural

refinement of "does a system exist" is quantitative, and the literature has so far quantified the *minimum modulus*: [11] bounds $\min_i \deg m_i$, and R. Wang [16] studies the least degree missed by a non-covering family; the same author [15] proves the $\mathbb{F}_q[x]$ analogue of the theorem of Crittenden and Vanden Eynden [4]. The quantity we study instead is the size of the ambient period, that is, of the least common multiple. Over $\mathbb{Z}$ this is an actively studied quantity: writing $L_{\min}(m)$ for the smallest least common multiple of a distinct covering system of $\mathbb{Z}$ with minimum modulus m, one has $L_{\min}(3) = 120$, $L_{\min}(4) = 360$ [5], $L_{\min}(5) = 1440$, $L_{\min}(6) = 5040$ [10], and $L_{\min}(7) = 10080$ has recently been claimed [18]. Its analogue over $\mathbb{F}_q[x]$ is the object of this paper.

Definition 1.2. For $d \geq 1$ let $\Lambda(q, d)$ be the least degree of a monic common multiple of the moduli of a distinct covering system of $\mathbb{F}_q[x]$ all of whose moduli have degree at least d, and $\Lambda(q, d) = \infty$ if there is no such system.

Since the least common multiple of the moduli is the monic common multiple of least degree, $\Lambda(q, d)$ is exactly the least degree of $\operatorname{lcm}_i m_i$ over such systems; we use the two descriptions interchangeably. We are not aware of any minimality question of this kind having been posed for $\mathbb{F}_q[x]$: the quantity is new, and so are all the values below. Our results are the following.

- $\Lambda(3, 1) = 4$ (Theorem 3.1). The upper bound is an explicit distinct covering system of $\mathbb{F}_3[x]$ with eleven congruences and least common multiple $x^2(x-1)(x-2)$, printed in full in Table 1 and verified by hand in Remark 3.2. This settles the question of [12] at $q = 3$, with the smallest possible period.
- $\Lambda(2, 1) = 2$ and $\Lambda(2, 2) = 4$ (Proposition 4.1, Theorem 4.2). The upper bounds are Azlin's two systems; the content is that they are optimal, which is a statement the earlier literature could not make, having no minimality quantity for the least common multiple.
- $7 \leq \Lambda(2, 3) \leq 8$ (Theorem 5.1), the upper bound witnessed by a system of 25 congruences over $\mathbb{F}_2$ with all moduli of degree at least 3 (Table 3). Azlin's systems reach minimum modulus degree 2 and no further, and [11] proves that the minimum modulus degree is bounded without producing a value, so such a system is itself a new object.
- $\Lambda(3, 2) \geq 6$ (Theorem 5.3).
- The $\mathbb{F}_q[x]$ analogue of the Erdős–Selfridge odd covering problem (Theorem 6.1). Erdős and Selfridge asked whether a distinct covering system of $\mathbb{Z}$ exists with all moduli odd and greater than 1, that is, coprime to the smallest prime; the problem is open, and a recent machine-checked exclusion shows that the least common multiple of such a system would exceed 10^4 [14]. In $\mathbb{F}_q[x]$ the primes of smallest norm are the q linear polynomials, so the analogue asks for a distinct covering system no modulus of which is divisible by a linear polynomial. We show that over $\mathbb{F}_2$ no such system has its moduli dividing a common multiple of degree less than 11. We are not aware of the question having been asked; the word "linear" does not occur in [1].

All of these are finite statements, and all of them are proved by finite computation: either by a reciprocal-sum inequality summed over the divisors of a candidate least common multiple, or, in one cell, by an exhaustive search over residue assignments. Every such computation has been carried out inside the Lean 4 proof assistant — the reasoning in the kernel, the finite searches in Lean's compiled evaluator; Section 9 says exactly which claim rests on which search. Where a proof is short enough to be checked by a reader, we give it: the lower bounds $\Lambda(2, 1) \geq 2$, $\Lambda(2, 2) \geq 4$ and $\Lambda(3, 1) \geq 4$ all admit hand arguments, which we include, and the eleven-congruence system of Table 1 is verified by hand in half a page.

2. The reduction to a finite problem

Throughout, $K = \mathbb{F}_q$, moduli are monic and non-constant, and $d \geq 1$ is a lower bound imposed on the degrees of the moduli. We write a system as a pair (M, a) where M is a finite set of monic polynomials of degree at least d and a assigns to each $m \in M$ a residue a_m; the system *covers* if

every $f \in K[x]$ satisfies $m \mid f - a_m$ for some $m \in M$. Holding the moduli in a *set* is what makes the system distinct.

The following four facts reduce the existence question for a fixed common multiple L to a finite one. They are transcriptions to $K[x]$ of arguments that are standard over $\mathbb{Z}$; we record them because everything below is an instance of them.

Lemma 2.1 (one period suffices)**.** *Let L be monic and let (M, a) be a system all of whose moduli divide L. If every f with $\deg f < \deg L$ satisfies one of the congruences, then (M, a) covers $K[x]$. Moreover, if f lies in the class of m modulo m and $\deg f < \deg L = D$, then $f = r + mh$ where $r = a_m \bmod m$ has degree $< \deg m$ and $\deg h < D - \deg m$.*

Proof. Given f, divide by L: $f = Lg + f_0$ with $\deg f_0 < \deg L$. Some $m \in M$ satisfies $m \mid f_0 - a_m$, and $m \mid L \mid f - f_0$, so $m \mid f - a_m$. The second assertion is the division algorithm applied to a_m and then to $f - r$, together with the degree count $\deg(f - r) = \deg m + \deg h$. □

The first assertion is [1, Theorem 5.4], stated there for L the least common multiple of the moduli. The period is the set of the q^D polynomials of degree $< D$, where $D = \deg L$; it is in bijection with $\mathbb{F}_q^D$ by reading off coefficients, so each cell below is a finite combinatorial problem of size q^D.

Lemma 2.2 (the finite model)**.** *For every $D \geq 0$ the map $\mathbb{F}_q^D \to K[x]$ sending $(c_0, \dots, c_{D-1})$ to $\sum_i c_i x^i$ is a bijection onto the set of polynomials of degree $< D$, and for monic g, L one has $g \mid L$ if and only if $gh = L$ for some monic h with $\deg h = \deg L - \deg g$.*

The second half is the observation that makes the computations below division-free: divisibility among monic polynomials is decided by trial multiplication, and a congruence class inside a period is enumerated as $\{r + mh\}$ rather than through a remainder.

Lemma 2.3 (divisor completion)**.** *Let (M, a) be a covering system with all moduli of degree $\geq d$ dividing L, and let g be a monic divisor of L with $\deg g \geq d$ and $g \notin M$. Then $M \cup \{g\}$, with any residue attached to g, is again a distinct covering system with all moduli of degree $\geq d$ dividing L.*

Consequently, for the purpose of deciding whether *some* system with common multiple L exists, the set of moduli may be taken to be *all* monic divisors of L of degree at least d: the moduli are determined by the pair (d, L), which we call a *cell*, and only the residues are free. This is the same one-line argument as over $\mathbb{Z}$.

Lemma 2.4 (capacity, or the reciprocal-sum bound)**.** *Let L be monic of degree D and let $\mathcal{D}$ be the monic divisors of L of degree at least d. If some assignment of one residue to each element of $\mathcal{D}$ covers the period, then*

$$\sum_{m \in \mathcal{D}} q^{\,D - \deg m} \;\geq\; q^D, \qquad \textit{equivalently} \qquad \sum_{m \in \mathcal{D}} q^{-\deg m} \;\geq\; 1.$$

Proof. The class of m inside the period has exactly $q^{D - \deg m}$ elements, by Lemma 2.1; a union of $|\mathcal{D}|$ sets of these sizes cannot exhaust q^D points otherwise. □

This is the analogue of the Mirsky–Newman density obstruction over $\mathbb{Z}$, and it is Azlin's counting argument in the present notation: [1, Lemma 6.1] is the size $q^{\,D - \deg m}$ of one class inside a period, and the proof of [1, Theorem 6.2] sums it over the moduli. It costs one sum over divisor degrees and constructs no classes at all, which is what makes sweeps over many L affordable: all but one of the lower bounds below are proved by Lemma 2.4 alone.

When the capacity bound fails to decide a cell, the cell is decided exactly.

Proposition 2.5 (exhaustive search)**.** *Fix a cell (d, L) with divisor set $\mathcal{D}$ as above and let $D = \deg L$. Consider the search that maintains a list of still-uncovered points of the period and a list of unused moduli, and at each node takes the first uncovered point y and branches over the pairs (m, C) with m unused and C the class of m containing y. This search is complete: if any assignment of one residue to each $m \in \mathcal{D}$ covers the period, the search finds one.*

Proof. The $q^{\deg m}$ classes of a fixed modulus m partition the period, so the class of m through a given point is unique; hence for each uncovered point the branching over unused moduli, one class each, is exhaustive. The depth is at most $|\mathcal{D}|$. □

Finally, in the other direction, a table of congruences is turned into a theorem by a finite check.

Lemma 2.6 (witness tables)**.** *Let L be monic of degree D and let $(m_1, r_1), \dots, (m_k, r_k)$ be pairs with the m_i monic, pairwise distinct, of degree at least d, and each dividing L. If every f of degree $< D$ satisfies $m_i \mid f - r_i$ for some i, then the m_i form a distinct covering system of $K[x]$ with exactly k congruences, all moduli of degree at least d and common multiple L. In particular $\Lambda(q, d) \le D$.*

Proof. Immediate from Lemma 2.1; the cardinality claim is that the m_i, being monic and pairwise distinct, remain distinct as elements of $K[x]$. □

In each of the tables below the modulus L itself occurs among the m_i, so the common multiple exhibited is the least common multiple of the system.

3. A distinct covering system of $\mathbb{F}_3[x]$

Theorem 3.1. $\Lambda(3, 1) = 4$. *The eleven congruences of Table 1 form a distinct covering system of $\mathbb{F}_3[x]$ whose moduli are the eleven monic divisors of $x^2(x-1)(x-2)$ of positive degree, so its least common multiple is $x^2(x-1)(x-2)$, of degree 4; and no distinct covering system of $\mathbb{F}_3[x]$ has a common multiple of degree less than 4.*

Table 1. A distinct covering system of $\mathbb{F}_3[x]$ with eleven congruences and least common multiple $L = x^2(x-1)(x-2)$. The moduli are all eleven monic divisors of L of positive degree. Right: the same system in the coordinates $(u, v, w) = (f \bmod x^2,\ f(1),\ f(2))$ of the Chinese remainder isomorphism $\mathbb{F}_3[x]/(L) \cong \mathbb{F}_3[x]/(x^2) \times \mathbb{F}_3 \times \mathbb{F}_3$, with $u = u_0 + u_1 x$.

modulus m	residue r	u	v	w
x	0	$u_0 = 0$	—	—
$x - 1$	2	—	$v = 2$	—
$x - 2$	1	—	—	$w = 1$
x^2	$2x + 1$	$u = 1 + 2x$	—	—
$x(x-1)$	$x + 2$	$u_0 = 2$	$v = 0$	—
$x(x-2)$	2	$u_0 = 2$	—	$w = 2$
$(x-1)(x-2)$	$2x + 2$	—	$v = 1$	$w = 0$
$x^2(x-1)$	1	$u = 1$	$v = 1$	—
$x^2(x-2)$	$2x^2 + x + 1$	$u = 1 + x$	—	$w = 2$
$x(x-1)(x-2)$	$2x^2 + 1$	$u_0 = 1$	$v = 0$	$w = 0$
$x^2(x-1)(x-2)$	$2x^3 + 1$	$u = 1$	$v = 0$	$w = 2$

Proof of the upper bound. The eleven moduli are monic, pairwise distinct, of positive degree, and are exactly the divisors $x^a(x-1)^b(x-2)^c$ of L with $0 \le a \le 2$, $0 \le b, c \le 1$ and $a + b + c \ge 1$. By Lemma 2.6 it suffices to check that the eleven classes cover the 81 polynomials of degree < 4, which is the content of Remark 3.2; the machine-checked proof evaluates all 81 cases directly. The reciprocal sum of the system is $3 \cdot \frac{1}{3} + 4 \cdot \frac{1}{9} + 3 \cdot \frac{1}{27} + \frac{1}{81} = \frac{127}{81}$, so the eleven classes have 127 elements counted with multiplicity, against a period of 81: they overlap in 46 points, and the covering is not an exact one. □

Remark 3.2 (the covering, by hand). Since x^2, $x-1$ and $x-2$ are pairwise coprime, the Chinese remainder theorem gives

$$\mathbb{F}_3[x]/(L) \;\cong\; \mathbb{F}_3[x]/(x^2)\times\mathbb{F}_3[x]/(x-1)\times\mathbb{F}_3[x]/(x-2), \qquad f\mapsto (u,v,w)=(f \bmod x^2,\ f(1),\ f(2)),$$

a set of $9\cdot 3\cdot 3=81$ triples; write $u=u_0+u_1x$. A congruence modulo $x^a(x-1)^b(x-2)^c$ constrains only the coordinates whose exponent is positive, and constrains u to a single value if $a=2$ and to the three u with a prescribed u_0 if $a=1$. The right-hand half of Table 1 lists the resulting constraints. Now read the table in order. The first three congruences cover everything with $u_0=0$, everything with $v=2$ and everything with $w=1$, leaving the box $u_0\in\{1,2\}$, $u_1\in\mathbb{F}_3$, $v\in\{0,1\}$, $w\in\{0,2\}$ of 24 triples. Inside that box: $x(x-2)$ covers $u_0=2,\ w=2$ and $x(x-1)$ covers $u_0=2,\ v=0$, and what is left of $u_0=2$ is $v=1,\ w=0$, which $(x-1)(x-2)$ covers. For $u_0=1$: x^2 covers all of $u_1=2$; the congruence modulo $x(x-1)(x-2)$ covers $v=0,\ w=0$ and $(x-1)(x-2)$ covers $v=1,\ w=0$, so only $w=2$ is left, where $x^2(x-2)$ covers $u_1=1$, the last congruence covers $u_1=0,\ v=0$, and $x^2(x-1)$ covers $u_1=0,\ v=1$. Every triple has been covered.

Proof of the lower bound. We must rule out every monic L of degree $D\le 3$; there are $1+3+9+27=40$ of them, and by Lemma 2.3 the moduli of the cell $(1,L)$ are all monic divisors of L of positive degree. For 39 of the 40 the capacity bound of Lemma 2.4 already fails: the reciprocal sum $\sum_{m\mid L,\ \deg m\ge 1} 3^{-\deg m}$ is less than 1. The single exception is $L=x(x-1)(x-2)$, where the sum is $\frac{37}{27}>1$ and the cell must be decided exactly. The machine-checked proof runs the search of Proposition 2.5 on that cell — a search whose naive size is $3^{12}=531441$ residue assignments, over the seven divisors of degrees $1,1,1,2,2,2,3$ — and it reports that no assignment covers.

That cell also succumbs to a hand argument, which we record because it is the shape of the obstruction. By the Chinese remainder theorem $\mathbb{F}_3[x]/(L)\cong\mathbb{F}_3^3$, and by Lemma 2.3 the three linear moduli are present; their classes are the three "planes" $\{u_i=r_i\}$, and what they leave uncovered is a product box of $2\cdot 2\cdot 2=8$ points. A quadratic modulus $(x-c_i)(x-c_j)$ fixes the coordinates i and j, so its class meets the box in at most $1\cdot 1\cdot 2=2$ points, and the cubic modulus meets it in at most 1. The three quadratics and the cubic therefore remove at most $3\cdot 2+1=7<8$ points, and the cell fails. □

4. Optimality of Azlin's systems over $\mathbb{F}_2$

Azlin's thesis displays sixteen distinct covering systems of $\mathbb{F}_2[x]$, numbered (6.1)–(6.16); two of them are reprinted as examples (1) and (2) of [12, §1], and every explicit system we have found in print, there or anywhere else, is over $\mathbb{F}_2$. The first is

$$f\equiv 0 \pmod{x}, \qquad f\equiv 0 \pmod{x+1}, \qquad f\equiv 1 \pmod{x^2+x}, \tag{1}$$

with least common multiple $x(x+1)$ of degree 2, and the second is the six-congruence system of Table 2, with least common multiple $x^2(x+1)^2$ of degree 4 and every modulus of degree at least 2. What is new here is that neither can be improved.

Proposition 4.1. $\Lambda(2,1)=2$, *attained by* (1).

Proof. The upper bound is (1), checked on the four polynomials of degree <2. For the lower bound, a monic L over $\mathbb{F}_2$ of degree ≤ 1 has at most one monic divisor of positive degree, of reciprocal weight at most $\frac12<1$, so Lemma 2.4 excludes all three such L. □

Theorem 4.2. $\Lambda(2,2)=4$. *That is, Azlin's system of Table 2 has the smallest possible least common multiple among distinct covering systems of* $\mathbb{F}_2[x]$ *all of whose moduli have degree at least* 2.

Proof. The upper bound is Table 2, checked on the sixteen polynomials of degree <4 (reciprocal sum $\frac{17}{16}$). For the lower bound we must exclude the 15 monic L of degree $D\le 3$, and in every case the capacity bound suffices; the machine-checked proof evaluates it on all 15. By hand: if $D\le 1$ there is no divisor of degree ≥ 2 at all; if $D=2$ the only one is L itself, of weight $\frac14$; and if $D=3$

TABLE 2. Azlin's system with all moduli of degree ≥ 2, least common multiple $L = x^2(x+1)^2$; the moduli are all six monic divisors of L of degree ≥ 2. By Theorem 4.2 no distinct covering system of $\mathbb{F}_2[x]$ with all moduli of degree ≥ 2 has a common multiple of smaller degree.

modulus	residue	modulus	residue
x^2	0	$x(x+1)^2$	1
$(x+1)^2$	x	$x^2(x+1)$	x^2+x
$x(x+1)$	$x+1$	$x^2(x+1)^2$	x^3+x^2+x

then the divisors of degree 2 are in bijection with the monic linear divisors of L, of which there are at most two, since x and $x+1$ are the only monic linear polynomials over $\mathbb{F}_2$, so the reciprocal sum is at most $2 \cdot \frac{1}{4} + \frac{1}{8} = \frac{5}{8} < 1$. Lemma 2.4 then excludes every cell. □

5. Minimum modulus degree three

Azlin's systems reach minimum modulus degree 2 and go no further, and his Conjecture 6.3 — that distinct covering systems of $\mathbb{F}_2[x]$ exist with arbitrarily large minimum modulus degree — was disproved by [11, Theorem 1.4], which bounds the minimum modulus degree of a covering system of multiplicity s without producing a value for it. A distinct covering system of $\mathbb{F}_2[x]$ with every modulus of degree at least 3 is therefore an object about which nothing explicit was known. There is one, with 25 congruences.

Theorem 5.1. $7 \leq \Lambda(2,3) \leq 8$. *The upper bound is witnessed by the* 25 *congruences of Table 3, whose moduli are the* 25 *monic divisors of degree at least* 3 *of* $L = x^3(x+1)^3(x^2+x+1)$*, so that the system is distinct, has all moduli of degree at least* 3*, and has least common multiple* L *of degree* 8*.*

TABLE 3. A distinct covering system of $\mathbb{F}_2[x]$ with all moduli of degree at least 3: 25 congruences, least common multiple $L = x^3(x+1)^3(x^2+x+1)$ of degree 8. The moduli are all 25 monic divisors of L of degree at least 3 (six each of degrees $3, 4, 5$, four of degree 6, two of degree 7 and L itself); the reciprocal sum is $357/256$.

modulus	residue	modulus	residue
x^3	0	$x^3(x+1)^2$	$x^4+x^3+x^2+1$
$(x+1)(x^2+x+1)$	1	$(x+1)^3(x^2+x+1)$	x^4+x^2+1
$x(x+1)^2$	x	$x(x+1)^2(x^2+x+1)$	$x^4+x^3+x^2+x+1$
$x^2(x+1)$	$x+1$	$x^3(x^2+x+1)$	$x^4+x^3+x^2$
$x(x^2+x+1)$	x^2	$x^2(x+1)^3$	x^4+x^3+1
$(x+1)^3$	x^2+1	$x^3(x+1)(x^2+x+1)$	x^4+x
$x(x+1)(x^2+x+1)$	x^2+x	$x(x+1)^3(x^2+x+1)$	x^5+x+1
$x^2(x+1)^2$	x^2+x+1	$x^2(x+1)^2(x^2+x+1)$	$x^5+x^4+x^3+x$
$x^3(x+1)$	x^3+1	$x^3(x+1)^3$	$x^5+x^3+x^2+1$
$(x+1)^2(x^2+x+1)$	x^3+x+1	$x^2(x+1)^3(x^2+x+1)$	$x^4+x^3+x^2+x$
$x^2(x^2+x+1)$	x^3+x^2	$x^3(x+1)^2(x^2+x+1)$	$x^6+x^5+x^4+x^3+x^2+x$
$x(x+1)^3$	x^3+x^2+1	$x^3(x+1)^3(x^2+x+1)$	$x^7+x^6+x^5+x^3+x^2+x$
$x^2(x+1)(x^2+x+1)$	x^3+x^2+x		

Proof. For the upper bound, the 25 moduli are monic, pairwise distinct, of degree at least 3 and divide L; by Lemma 2.6 it remains to check that their classes cover the 256 polynomials of degree < 8, which the machine-checked proof does by evaluating all 256 cases. For the lower bound we must exclude every monic L over $\mathbb{F}_2$ of degree $D \leq 6$. There are 127 of them, and for every one the capacity bound of Lemma 2.4 fails: the reciprocal sum $\sum_{m \mid L,\ \deg m \geq 3} 2^{-\deg m}$ is always less than 1,

its maximum over the 127 cells being $\frac{53}{64} = 0.828\ldots$, attained at $L = x^2(x+1)^2(x^2+x+1)$. No exact search is needed anywhere in the lower bound. □

Remark 5.2. The gap in Theorem 5.1 is exactly two cells. Among the 128 monic L over $\mathbb{F}_2$ of degree 7, all but two have reciprocal sum below 1 at $d = 3$ and are excluded by Lemma 2.4; the two exceptions are $L = x^3(x+1)^2(x^2+x+1)$ and $L = x^2(x+1)^3(x^2+x+1)$, each with 17 moduli of degree at least 3 and reciprocal sum $\frac{141}{128}$. The two are exchanged by the automorphism $x \mapsto x+1$ of $\mathbb{F}_2[x]$, which fixes x^2+x+1 and carries monic divisors to monic divisors, so either both carry a distinct covering system or neither does. So $\Lambda(2,3) = 7$ if they do and $\Lambda(2,3) = 8$ if they do not. See Question 8.2 for what it costs to decide them. This census of the 128 cells of degree 7, and the remark about the automorphism, are outside the formal development; Theorem 5.1 does not depend on either.

Theorem 5.3. *If (M, a) is a distinct covering system of $\mathbb{F}_3[x]$ with every modulus of degree at least 2, then every monic common multiple of its moduli has degree at least 6; that is, $\Lambda(3,2) \geq 6$.*

Proof. There are 364 monic L over $\mathbb{F}_3$ of degree $D \leq 5$, and for each of them the reciprocal sum $\sum_{m|L,\ \deg m \geq 2} 3^{-\deg m}$ is less than 1; the maximum is $\frac{190}{243} = 0.781\ldots$, attained at $L = x^2(x-1)^2(x-2)$. Lemma 2.4 excludes every cell. □

We emphasise that Theorem 5.3 is one-sided: no distinct covering system of $\mathbb{F}_3[x]$ with all moduli of degree at least 2 is known, and it is not known whether one exists, so $\Lambda(3,2)$ may well be ∞. The statement proved is the lower bound in the form given, which is independent of that.

6. The Erdős–Selfridge analogue

Erdős and Selfridge asked whether there is a distinct covering system of $\mathbb{Z}$ all of whose moduli are odd and greater than 1 — equivalently, all coprime to the smallest prime. It is problem #7 in Bloom's catalogue of Erdős's problems, stated there as *"Is there a distinct covering system all of whose moduli are odd?"* and carrying Erdős's $25 for a proof that there is none [3]; Guy's section on covering systems of congruences is [8, F13]. The problem is open; recent machine-checked exclusions show that the least common multiple of such a system would have to exceed 10^4 [14].

In $\mathbb{F}_q[x]$ the primes of smallest norm are the q linear polynomials $x - c$, so the analogue of "odd" is "divisible by no linear polynomial", and the analogous question is whether a distinct covering system of $\mathbb{F}_q[x]$ exists none of whose moduli has a linear factor. We are not aware of the question having been raised. Azlin states the integer question itself — his Conjecture 3.2 reads "There exists a distinct covering system with all moduli m_i odd, distinct, and greater than one" — but does not transfer it: the word "linear" does not occur anywhere in [1], whose restrictions on systems of $\mathbb{F}_2[x]$ are always on how many moduli of low degree are used and never on their divisibility. None of [11, 12, 15, 16, 17] raises it either.

Theorem 6.1. *Let $L \in \mathbb{F}_2[x]$ be monic with $\deg L < 11$ and divisible by no linear polynomial, and let (M, a) be a system whose moduli are monic, non-constant, pairwise distinct and all divisors of L. Then (M, a) does not cover $\mathbb{F}_2[x]$.*

Proof. Since L has no linear factor, neither has any divisor of L, so the cells to be excluded are the pairs $(1, L)$ with L monic of degree ≤ 10 having no root in $\mathbb{F}_2$. There are 512 of them, and for each the capacity bound of Lemma 2.4 fails: the reciprocal sum $\sum_{m|L,\ \deg m \geq 1} 2^{-\deg m}$ is less than 1 throughout, its maximum being $\frac{677}{1024} = 0.661\ldots$, attained at $L = (x^2+x+1)^2(x^3+x+1)(x^3+x^2+1)$ of degree 10. No exact search is used. □

Remark 6.2. If every modulus of a distinct covering system is divisible by no linear polynomial, then neither is their least common multiple, since $x - c$ is prime and divides a least common multiple only if it divides one of the moduli. So Theorem 6.1 reads: the least common multiple of a distinct covering system of $\mathbb{F}_2[x]$ with no modulus divisible by a linear polynomial has degree at least 11.

We state the theorem in the common-multiple form because that is the form that has been machine-checked; the deduction just given is three lines of standard algebra and is not part of the verified development.

The bound 11 is a limit of enumeration, not of the method: the sweep runs over all 2^D monic polynomials of each degree D. Question 8.3 says how far the same capacity bound would reach if it were run over factorisation shapes instead.

7. Sharpness and controls

The values above are the exact limits of the method used to prove them, and the hypotheses are not vacuous. We record this explicitly, since every lower bound here is a statement that a search found nothing.

Proposition 7.1. (1) *The lower bounds of Theorems 3.1 and 4.2 cannot be raised: the assertions $\Lambda(3,1) \geq 5$ and $\Lambda(2,2) \geq 5$ are both false, refuted by the systems of Tables 1 and 2 respectively.*

(2) *The exclusion method stops exactly where the object is, not where the computation was cut off: the cell $(2, x^2(x+1)^2)$ is not excluded by the cell test, and the sweep over all monic L of degree < 5 at $d = 2$ over $\mathbb{F}_2$ fails.*

(3) *A single non-constant modulus never covers, whatever residue it is given.*

(4) *Two classes with the same modulus x already cover $\mathbb{F}_2[x]$; distinctness is what the question is about, and it is the only reason $\Lambda(2,1)$ is 2 rather than 1.*

8. Questions

We close with the four questions the present method leaves open, each with the cost that was measured for it. The computations quoted in this section were carried out outside the formal development and are reported as measurements, not as theorems; each of them was run or rerun on 2026-08-28.

Question 8.1. Is $\Lambda(5,1) = 7$? More generally, for which q in the range $3 \leq q \leq 73$ left open by Theorem 1.1 does a distinct covering system of $\mathbb{F}_q[x]$ exist?

Here the following refinement of Lemma 2.4 locates the frontier. Write $L = \prod_i P_i^{e_i}$ with the P_i distinct monic irreducibles, $\deg P_i = f_i$. By Lemma 2.3 the moduli P_i themselves are in the system, and by the Chinese remainder theorem what their classes leave uncovered is a product box of $\prod_i \bigl(q^{e_i f_i} - q^{(e_i-1)f_i}\bigr)$ points; a modulus $\prod_i P_i^{a_i}$ meets that box in at most $\prod_i h_i(a_i)$ points, where $h_i(0) = q^{e_i f_i} - q^{(e_i-1)f_i}$ and $h_i(a) = q^{(e_i-a)f_i}$ for $a \geq 1$, because fixing $u \bmod P_i^a$ with $a \geq 1$ already determines $u \bmod P_i$. Summing over all moduli other than 1 and the P_i must reach the box size. This test depends only on the multiset of pairs (f_i, e_i), so it disposes of all L of a given degree at once, and it is the hand argument of Section 3 in general form. Over $\mathbb{F}_3$ it kills every shape of degree ≤ 3 — including $x(x-1)(x-2)$, box 8 against bound 7 — and leaves exactly one shape of degree 4, namely that of $x^2(x-1)(x-2)$, which is where the system of Table 1 lives. Over $\mathbb{F}_5$ it kills every shape of degree ≤ 6, and at degree 7 exactly one survives: $L = (x-a)^2(x-b)^2(x-c)(x-d)(x-e)$ with five distinct roots, box 25 600 against bound 26 900. So, granted the box test, $\Lambda(5,1) \geq 7$, and a single cell decides whether $\Lambda(5,1) = 7$; that cell has $5^7 = 78\,125$ points and 71 moduli, and an exhaustive search of it did not terminate in twenty minutes of CPU time. If it carries no covering system, three shapes remain open at degree 8.

Question 8.2. Is $\Lambda(2,3)$ equal to 7 or to 8?

By Remark 5.2 this is two cells, $L = x^3(x+1)^2(x^2+x+1)$ and $L = x^2(x+1)^3(x^2+x+1)$, each with 17 moduli and 2^{74} residue assignments — and, by the automorphism of that remark, really one cell. Each survived 2×10^9 nodes of the search of Proposition 2.5, about half an hour of compiled C apiece, without resolving. The box refinement described above settles neither; we give the numbers

for $L = x^3(x+1)^2(x^2+x+1)$, the other cell repeating them under the automorphism. Run over the three prime-power coordinates at once, the refinement leaves a box of $7 \cdot 4 \cdot 4 = 112$ points — of the seventeen moduli only x^3 lives in a single coordinate — and charges the other sixteen moduli $122 > 112$. Run over a coprime split into two coordinates it fails on each of the three splits: for $L_1 = x^3$, $L_2 = (x+1)^2(x^2+x+1)$ the box has at least $7 \cdot 13 = 91$ points against a charge of 101; for $L_1 = x^3(x+1)^2$, $L_2 = x^2+x+1$ it has at least 60 against 73, and capping each class at the size of the box — the only place in this cell where the cap bites at all — lowers the charge only to 71.

Question 8.3. How far does the capacity bound reach for the Erdős–Selfridge analogue over $\mathbb{F}_2$?

Theorem 6.1 stops at degree 11 because the sweep enumerates polynomials. Enumerating factorisation shapes instead — multisets of pairs (irreducible degree, exponent), weighted by the true numbers $I_2(f) = 1, 2, 3, 6, 9, 18, 30, \ldots$ of monic irreducibles of degree $f \geq 2$ over $\mathbb{F}_2$ — makes each degree cost a dynamic program rather than 2^D cell tests. Run this way, the maximum of $\sum_{m \mid L,\ \deg m \geq 1} 2^{-\deg m}$ over linear-factor-free L of degree D stays below 1 for every $D \leq 23$ (it is 0.681 at $D = 12$, rises to 0.992 at $D = 22$, and is not monotone: 0.934 at $D = 23$) and first exceeds 1 at $D = 24$, where it is 1.016, attained by $(x^2+x+1)^3$ times two distinct irreducible cubics and three distinct irreducible quartics. So the capacity bound alone would give degree at least 24 in Theorem 6.1, more than doubling the present bound, once the sweep is run over shapes; what that costs to verify formally is a factorisation bridge — monic divisors as sub-multisets of the factorisation, and the counts $I_q(f)$. Beyond any bound, of course, stands the question itself: does a distinct covering system of $\mathbb{F}_q[x]$ with no modulus divisible by a linear polynomial exist for some q?

Question 8.4. What are $\Lambda(4, d)$, $\Lambda(8, d)$, $\Lambda(9, d)$?

Everything in Sections 2–6 is stated for an arbitrary finite field, and the computations instantiate it at $\mathbb{F}_p$ for a prime p only because the model of the field is a list of its elements. The case $q = 4$ is the smallest untouched one, and no argument changes.

9. Verification

Every theorem, proposition and lemma of Sections 2–7 has been formally verified in Lean 4 [6] (toolchain `v4.32.0`) against *Mathlib* [13]; the development is free of `sorry`, and the repository reference is to be added at submission. The assertions in this paper outside that development are the elementary deduction of Remark 6.2, the census of the degree-7 cells and the automorphism of Remark 5.2, and the measurements reported in Section 8; each is flagged where it occurs. The reasoning layer — the finite model of $\mathbb{F}_q[x]$ of Lemma 2.2, the one-period reduction of Lemma 2.1, divisor completion (Lemma 2.3), the capacity bound (Lemma 2.4), the completeness of the search (Proposition 2.5), the witness principle (Lemma 2.6) and the deduction of each displayed value from them — is kernel-checked and depends on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`; the development contains no polynomial division anywhere outside the proofs, divisibility being decided by trial multiplication and a congruence class being enumerated as $\{r + mh\}$. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the finite searches, one per displayed claim: the four witness tables ((1), Tables 2, 1, 3), checked on 4, 16, 81 and 256 points respectively; the capacity sweeps behind the lower bounds, over 3, 15, 40, 127, 364 and 512 cells respectively for Proposition 4.1 and Theorems 4.2, 3.1, 5.1, 5.3 and 6.1; and, in the single cell $L = x(x-1)(x-2)$ of Theorem 3.1, the exhaustive residue search of Proposition 2.5. Each such evaluation enters the proof as its own `native_decide` axiom, alongside the three named above, and no other axiom occurs in the development. Every table and every numerical value quoted was produced outside Lean first and the formal statement written against it afterwards: the system of Table 1 was found and rechecked by two independent implementations, a C search and a Python re-implementation with a different branching order, and the two systems attributed to Azlin were recomputed from the source's own data before any of the present work was formalised.

References

[1] M. W. Azlin, *Covering systems of polynomial rings over finite fields*, M.Sc. thesis, University of Mississippi, May 2011; eGrove Electronic Theses and Dissertations 39, `https://egrove.olemiss.edu/etd/39`.

[2] P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe and M. Tiba, *On the Erdős covering problem: the density of the uncovered set*, Invent. Math. **228** (2022), no. 1, 377–414; arXiv:1811.03547.

[3] T. F. Bloom, *Erdős problem #7*, `https://www.erdosproblems.com/7`, accessed 28 August 2026.

[4] R. B. Crittenden and C. L. Vanden Eynden, *Any n arithmetic progressions covering the first 2^n integers cover all integers*, Proc. Amer. Math. Soc. **24** (1970), 475–481.

[5] J. Dalton and O. Trifonov, *Extreme covering systems*, J. Integer Seq. **25** (2022), Article 22.9.1.

[6] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635.

[7] P. Erdős, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.

[8] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004; Section F13, "Covering systems of congruences".

[9] B. Hough, *Solution of the minimum modulus problem for covering systems*, Ann. of Math. (2) **181** (2015), no. 1, 361–382.

[10] J. Klein, *On a conjecture of Krukenberg and a problem of Dalton and Trifonov*, Integers **26** (2026), #A38; arXiv:2508.18062.

[11] H. Li, B. Wang, C. Wang and S. Yi, *On covering systems of polynomial rings over finite fields*, Proc. Amer. Math. Soc. **152** (2024), no. 9, 3731–3742; arXiv:2308.05378.

[12] H. Li, B. Wang, C. Wang and S. Yi, *On Erdős covering systems in global function fields*, J. Number Theory **266** (2025), 269–280; arXiv:2402.03810.

[13] The mathlib Community, *The Lean mathematical library*, in: CPP 2020, ACM, 2020, pp. 367–381.

[14] I. Mian and S. Siddique, *Kernel-checked exclusions for the Erdős–Selfridge odd covering problem: any odd covering of $\mathbb{Z}$ has lcm exceeding 10000*, arXiv:2607.25628 (2026).

[15] R. Wang, *On an Erdős-type conjecture on $\mathbb{F}_q[x]$*, Finite Fields Appl. **109** (2026), Paper No. 102720, 12 pp.; arXiv:2407.15146. (The first arXiv version carries the title with $\mathbb{F}_2[x]$ in place of $\mathbb{F}_q[x]$.)

[16] R. Wang, *An asymptotic bound for non-covering congruence systems over $\mathbb{F}_q[x]$*, arXiv:2607.27538 (2026).

[17] B. Wang, *Bounds for Erdős covering systems in global function fields*, Int. J. Number Theory **22** (2026), no. 6, 1327–1336; arXiv:2408.10460v1, whose numbering is the one cited above.

[18] J. Zhang and S. Zhang, *A distinct covering system with minimum modulus 7 and minimal least common multiple 10080*, arXiv:2607.19029 (2026).