

THE GENERALIZED COVERING RADII OF MELAS CODES AT $t \geq 3$: EXACT VALUES AT SIX CELLS, AND TWO DATA POINTS FOR $2t + 1$

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For an $[n, k]_q$ linear code C with parity-check columns $h_1, \dots, h_n \in \mathbb{F}_q^{n-k}$, the t -th generalized covering radius $\rho_t(C)$ of Elimelech, Firer and Schwartz is the least r such that any t syndromes lie together in the span of at most r of the columns. Li and Xiong have recently determined ρ_1 and ρ_2 for every Melas code $M(m, q)$ and have bracketed ρ_t for $t \geq 3$: in their asymptotic regime $m \geq t(2t - 1)$ one has $\rho_t(M(m, q)) \in \{2t, 2t + 1\}$ for $q \in \{2, 3\}$ and $= 2t$ for $q \geq 4$, and below that regime a wider interval. For $q \in \{2, 3\}$ no value of ρ_t with $t \geq 3$ is determined anywhere in their paper, at any cell; the only cells they pin down have $q \geq 4$ and $m \geq t(2t - 1)$, which at $t = 3$ means $m \geq 15$. We determine $\rho_t(M(m, q))$ exactly at six cells: $\rho_t(M(3, 2)) = 6$ and $\rho_t(M(3, 3)) = 6$ for all $t \geq 3$, $\rho_t(M(2, 3)) = 4$ for all $t \geq 1$, $\rho_3(M(4, 2)) = 7$, $\rho_t(M(4, 2)) = 8$ for all $t \geq 4$, and $\rho_3(M(5, 2)) \geq 7$ — with equality by an exhaustive computation carried out outside the formal development. The point of interest is that at both cells whose value we determine and where the trivial bound $\rho_t \leq n - k$ does not already give it, namely $(m, q, t) = (4, 2, 3)$ and $(5, 2, 3)$, that value is $2t + 1 = 7$: the upper of the two values Li and Xiong leave open for $q \in \{2, 3\}$. Two further findings are negative rather than new: $M(3, 2)$ is the repetition code $\text{Rep}_2(7)$, so its whole $t \geq 3$ column already follows from a published formula, at a cell the interval statement leaves open; and the value “the covering radius of $M(m, 2)$ is 3 if $m \geq 2$ ” printed by Shi, Helleseeth, Özbudak and Solé is false at $m = 2$, an error Li and Xiong found first and which we refute in a machine-checked form. Apart from four items labelled where they occur as computations outside the formal development, every assertion below is verified in Lean 4.

1. INTRODUCTION

The invariant. Let C be an $[n, k]_q$ linear code with parity-check matrix H whose columns are $h_1, \dots, h_n \in \mathbb{F}_q^{n-k}$. Elimelech, Firer and Schwartz [3] introduced a hierarchy of covering radii $\rho_1(C) \leq \rho_2(C) \leq \dots$ generalizing the ordinary covering radius ρ_1 . We use their definition in the form transcribed by Li and Xiong [6, Definition 2]:

Definition 1.1 ([3, Definition 1], in the form of [6, Definition 2]). The t -th generalized covering radius $\rho_t(C)$ of C is the smallest nonnegative integer r such that for any t vectors $s_1, s_2, \dots, s_t \in \mathbb{F}_q^{n-k}$ there exists a subset $I \subseteq [n]$ with $|I| \leq r$ satisfying $\{s_1, \dots, s_t\} \subseteq \langle h_i \mid i \in I \rangle$.

Thus ρ_1 is the ordinary covering radius, and ρ_t does not depend on the choice of parity-check matrix [6, Remark 1(1)], [3, Lemma 2]. The motivation is a batch version of the syndrome-decoding query: $\rho_t = r$ says that any t queries can be answered together by touching r coordinates.

Melas codes, and what Li and Xiong prove. Let α be a primitive element of $\mathbb{F}_{q^m}$ and let m_β denote the minimal polynomial of β over $\mathbb{F}_q$. The *Melas code* $M(m, q)$ is the cyclic code of length $n = q^m - 1$ over $\mathbb{F}_q$ with generator polynomial $\text{lcm}(m_\alpha, m_{\alpha^{-1}})$. Away from the degenerate pairs $(m, q) \in \{(1, 2), (1, 3), (2, 2)\}$ it has parameters $[q^m - 1, q^m - 1 - 2m]_q$, and a parity-check matrix whose i -th column is

$$(1) \quad h_i = (\varphi(\alpha^i), \varphi(\alpha^{-i})) \in \mathbb{F}_q^{2m}, \quad i = 0, 1, \dots, q^m - 2,$$

where $\varphi: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q^m$ is the coordinate map of an $\mathbb{F}_q$ -basis [6, §2.3].

Li and Xiong [6] determine ρ_1 (their Result 1, quoting [10]) and ρ_2 (their Theorem 1) for *all* pairs (m, q) . For $t \geq 3$ they prove two asymptotic bounds — $\rho_t \geq 2t$ when $1 \leq t \leq m$, $(m, q) \notin \{(1, 2), (1, 3), (2, 2)\}$ and $q^m \geq q^{t(2t-1)}/(2t-1)!$ [6, Theorem 2], and $\rho_t \leq 2t + 1$ when $1 \leq t \leq m$

and $m \geq 2(t+1)\log_q 2 + 2\log_q t$ [6, Theorem 3] — and assemble them, together with the bound $\rho_t \leq \min\{t\rho_1, 2m\}$ of [6, Remark 1(3)] and a generalized-Hamming-weight lower bound, into an interval statement [6, Theorem 4], which for $m \geq 3$ and $3 \leq t \leq m$ reads

(2)

$$\rho_t(M(m, q)) \in \begin{cases} [t + \lceil \log_2(t+1) \rceil, \min\{3t, 2m\}], & q = 2, m < 2(t+1) + 2\log_2 t, \\ [t + \lceil \log_2(t+1) \rceil, 2t+1], & q = 2, 2(t+1) + 2\log_2 t \leq m < t(2t-1), \\ [t + \lceil \log_3(2t+3) \rceil, \min\{3t, 2m\}], & q = 3, m < 2(t+1)\log_3 2 + 2\log_3 t, \\ [t + \lceil \log_3(2t+3) \rceil, 2t+1], & q = 3, 2(t+1)\log_3 2 + 2\log_3 t \leq m < t(2t-1), \\ [t + \lceil \log_q(t+1) \rceil, 2t], & q \geq 4, m < t(2t-1), \\ [2t, 2t+1], & q \in \{2, 3\}, m \geq t(2t-1), \\ \{2t\}, & q \geq 4, m \geq t(2t-1). \end{cases}$$

Their conclusion restates the last two lines. *At $q \in \{2, 3\}$ no value of ρ_t with $t \geq 3$ is determined anywhere in [6], at any cell:* every explicit assignment there at $q \in \{2, 3\}$ is a value of ρ_1 or ρ_2 . The one place where [6] does pin a ρ_t with $t \geq 3$ is the last line of (2), at $q \geq 4$ and $m \geq t(2t-1)$ — a regime that begins at $m = 15$ when $t = 3$, and which is not the regime of any cell below. The two-value ambiguity $\{2t, 2t+1\}$ for $q \in \{2, 3\}$ in the sixth line of (2) is the paper’s own open point, and the wide intervals in the first five lines leave every small cell undetermined as well.

What is settled here. We compute $\rho_t(M(m, q))$ exhaustively at the cells that fit inside a fixed computational budget. Write $D = n - k$ for the redundancy, so $D = 2m$ away from the degenerate pairs. The results are:

cell	n	k	D	interval from (2)	value
$\rho_3(M(3, 2))$	7	1	6	$[5, 6]$	6
$\rho_4(M(3, 2)), \rho_5(M(3, 2))$	7	1	6	—	6
$\rho_3(M(4, 2))$	15	7	8	$[5, 8]$	$7 = 2t + 1$
$\rho_4(M(4, 2))$	15	7	8	$[7, 8]$	$8 = D$
$\rho_5(M(4, 2))$	15	7	8	—	$8 = D$
$\rho_3(M(2, 3))$	8	4	4	—	$4 = D$
$\rho_3(M(3, 3))$	26	20	6	$[5, 6]$	$6 = D$
$\rho_3(M(5, 2))$	31	21	10	$[5, 9]$	≥ 7 (and $= 7$)
$\rho_3(M(4, 3))$	80	72	8	$[5, 8]$	≥ 6

All of these are new except the $M(3, 2)$ entries and $\rho_3(M(2, 3))$, for the reasons given below. Everything in the table is verified in Lean 4 except the equality $\rho_3(M(5, 2)) = 7$ and the bound $\rho_3(M(4, 3)) \geq 6$, which rest on exhaustive sweeps run outside the formal development and are labelled as such wherever they appear (Remarks 4.4 and 8.1). The interval for $\rho_3(M(5, 2))$ is (2)’s $[5, 9]$ narrowed to $[5, 8]$ by the subadditivity $\rho_3 \leq \rho_1 + \rho_2$ [6, Remark 1(3)], [3, Proposition 15]; $M(2, 3)$ and the rows with $t > m$ fall outside the range $m \geq 3, 3 \leq t \leq m$ of (2) and are bracketed instead by monotonicity and the trivial bound $\rho_t \leq D$.

Three things are worth separating out.

(i) *Where the redundancy does not decide, the answer is $2t + 1$.* At six of the nine rows above the answer coincides with the trivial bound D , so only a lower bound is at issue. Three rows have $2t + 1 < D$: $(m, q, t) = (4, 2, 3)$ with $D = 8$, $(5, 2, 3)$ with $D = 10$, and $(4, 3, 3)$ with $D = 8$. At the first two the answer is $2t + 1 = 7$ (Theorems 4.2 and 4.3, Remark 4.4); at the third only $\rho_3 \geq 6$ is known (Remark 8.1). The first two are therefore two independent data points on the upper side of the two-value ambiguity in the sixth line of (2). Neither cell lies in the regime $m \geq t(2t-1)$ where that ambiguity is stated; that regime is far out of computational reach (§8). What the two cells show is that where the question “ $2t$ or $2t + 1$?” can be asked at all and is not settled by the redundancy, the answer so far is $2t + 1$.

(ii) *A cell already settled in the literature.* $M(3, 2)$ has dimension $7 - 2 \cdot 3 = 1$, and its generator polynomial is $\text{lcm}(m_\alpha, m_{\alpha^{-1}}) = (x^7 - 1)/(x - 1)$: it is the binary repetition code $\text{Rep}_2(7)$. For repetition codes the generalized covering radii are known in closed form, $\rho_t(\text{Rep}_2(n)) = n - \lceil n/2^t \rceil$ (§6), which gives 3, 5, 6, 6, 6 at $n = 7$ for $t = 1, \dots, 5$. So the values in the $M(3, 2)$ entries are not new; what is new about them is only the observation that (2) leaves the interval $[5, 6]$ at a cell an already published formula determines, together with a machine-checked verification of the formula at a length not covered by the literally stated result it extends. We grade those values as consequences of published work throughout, and say so again in §6. Similarly $\rho_3(M(2, 3)) = 4$ is one line from $\rho_2(M(2, 3)) = 4 = D$ in [6, Theorem 1].

(iii) *A value in the earlier literature is wrong at one cell.* The accepted manuscript of Shi, Helleseth, Özbudak and Solé [10] states, on its first text page, that “the covering radius of $M(m, 2)$ is shown to be 3 if $m \geq 2$ ”, citing [2] and [9], and it lists only $M(1, 2)$ and $M(1, 3)$ as degenerate. At $m = 2$ that value is wrong: $M(2, 2)$ is the $[3, 1, 3]_2$ repetition code and $\rho_1(M(2, 2)) = 1$. *The observation is not ours*: Li and Xiong make it in [6, Remark 4(2)], and priority is entirely theirs. What we add is a machine-checked refutation, stated in §7.

Finally, we ran the whole of [6]’s own ρ_1 and ρ_2 tables through an independent implementation before computing anything new (§3). Eighteen values at nine cells agree, including the eight whose ρ_2 entry the source’s own text attributes to “a numeric experiment”.

Provenance of the ingredients. Definition 1.1, the basic properties of ρ_t collected in §2, the description (1) of the Melas parity-check matrix, and the interval statement (2) are all from [3] and [6]. The repetition-code formula is from [4] as extended in [1]. The observation corrected in §7 is [6, Remark 4(2)]. What is offered here is the exact values at the six cells, the supporting lower-bound witnesses and upper-bound certificates, and the calibration run.

2. PRELIMINARIES

Basic properties of ρ_t . Throughout, C is $[n, k]_q$ with parity-check columns $h_1, \dots, h_n \in \mathbb{F}_q^D$, $D = n - k$, and we assume the columns span $\mathbb{F}_q^D$ (as they do for a parity-check matrix of full rank). For $I \subseteq [n]$ write $\langle h_i \mid i \in I \rangle$ for the $\mathbb{F}_q$ -span of the corresponding columns. We use the following, all in [6, Remark 1] and [3].

Lemma 2.1. (1) $\rho_t(C)$ is independent of the choice of parity-check matrix.

(2) $\rho_1(C) \leq \rho_2(C) \leq \dots$, and $\rho_t(C) \leq D$ for every t , with $\rho_t(C) = D$ for every $t \geq D$.

(3) $\rho_{s+t}(C) \leq \rho_s(C) + \rho_t(C)$.

Proof. (1) is [3, Lemma 2]. Monotonicity in (2) is immediate from the definition, since t syndromes may be padded to $t + 1$ by repeating one of them. For $\rho_t \leq D$, choose D columns forming a basis of $\mathbb{F}_q^D$; their span is everything. For $\rho_t \geq D$ when $t \geq D$, take $s_1, \dots, s_t$ to include a basis of $\mathbb{F}_q^D$: any I with $\{s_1, \dots, s_t\} \subseteq \langle h_i \mid i \in I \rangle$ must have $\langle h_i \mid i \in I \rangle = \mathbb{F}_q^D$ and hence $|I| \geq D$. (3) is [3, Proposition 15], stated there for all $s, t \in \mathbb{N}$; [6, Remark 1(3)] records it for $s + t \leq D$, which is the only range used below. $\square$

Two reformulations are used below. The first is the one on which the sweeps of §8 run; in it and throughout, $\binom{D}{t}_q$ denotes the Gaussian binomial coefficient, that is the number of t -dimensional subspaces of $\mathbb{F}_q^D$.

Lemma 2.2. Let $t \leq D$. Then $\rho_t(C)$ is the least r such that every t -dimensional subspace of $\mathbb{F}_q^D$ is contained in $\langle h_i \mid i \in I \rangle$ for some I with $|I| \leq r$.

Proof. A set $\{s_1, \dots, s_t\}$ is contained in a subspace V if and only if its span is, and that span has dimension at most t ; conversely every subspace of dimension at most t lies inside some t -dimensional subspace, because $t \leq D$, and a t -dimensional subspace is the span of t vectors. So the two conditions on r quantify over the same collection of spans. $\square$

The second reformulation is the certificate that replaces an infeasible search at $M(4, 2)$. It is elementary, but it is what makes one of the two upper bounds of §4 computable at all, so we record it separately.

Proposition 2.3. *Let $W \subseteq (\mathbb{F}_q^D)^*$ be a subspace of linear forms with $\dim W \geq 4$, and suppose that for every nonzero $\lambda \in W$ the hyperplane $\ker \lambda$ is contained in $\langle h_i \mid i \in I_\lambda \rangle$ for some index set I_λ with $|I_\lambda| \leq r$. Then $\rho_3(C) \leq r$.*

Proof. Let $s_1, s_2, s_3 \in \mathbb{F}_q^D$. The annihilator $A = \{\lambda : \lambda(s_1) = \lambda(s_2) = \lambda(s_3) = 0\} \subseteq (\mathbb{F}_q^D)^*$ has dimension at least $D - 3$, so $\dim W + \dim A \geq 4 + D - 3 > D$ and $W \cap A \neq \{0\}$. Pick a nonzero $\lambda \in W \cap A$; then $s_1, s_2, s_3 \in \ker \lambda \subseteq \langle h_i \mid i \in I_\lambda \rangle$ and $|I_\lambda| \leq r$. $\square$

The gain is that the hypothesis of Proposition 2.3 ranges over the $q^{\dim W} - 1$ nonzero elements of W and, for each, over the q^D vectors of $\mathbb{F}_q^D$, whereas the definition ranges over the q^{3D} triples of syndromes. At $M(4, 2)$, where $D = 8$, that is about 10^4 against 2^{24} .

The computational model. All computations below — inside the formal development and outside it — use one model of the field, described here once. Fix m, q and a monic $f = x^m + f_{m-1}x^{m-1} + \dots + f_0 \in \mathbb{F}_q[x]$, and take

$$\mathbb{F}_{q^m} = \mathbb{F}_q[x]/(f), \quad \alpha = x, \quad \varphi(\text{class of } c_{m-1}x^{m-1} + \dots + c_0) = (c_0, \dots, c_{m-1}).$$

A vector of $\mathbb{F}_q^N$ is stored as the natural number whose base- q digits are its coordinates, so the column h_i of (1) is the $2m$ -digit number carrying $\varphi(\alpha^i)$ in digits $0, \dots, m-1$ and $\varphi(\alpha^{-i})$ in digits $m, \dots, 2m-1$. Under this identification $\mathbb{F}_q^{2m} = \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$, and we name syndromes by the corresponding pair whenever that is clearer than the integer.

Nothing in the development assumes that f is irreducible or primitive. Each of the cells of (3) instead *checks* that the powers $1, \alpha, \dots, \alpha^{q^m-2}$ are pairwise distinct and $\alpha^{q^m-1} = 1$, which is exactly the condition making (1) the Melas column list; it also checks that the resulting list has $q^m - 1$ pairwise distinct nonzero entries, and that D of them span $\mathbb{F}_q^D$. Without the last check the syndrome quantifier of Definition 1.1 could silently range over a proper subspace. The moduli used are

$$(3) \quad \begin{array}{lll} M(3, 2): x^3 + x + 1, & M(4, 2): x^4 + x + 1, & M(5, 2): x^5 + x^2 + 1, \\ M(2, 3): x^2 + x + 2, & M(3, 3): x^3 + 2x + 1. \end{array}$$

($M(2, 2)$ is degenerate and needs no modulus; see §7.) By Lemma 2.1(1) the answers do not depend on any of these choices; at $M(3, 2)$, $M(4, 2)$, $M(2, 3)$ and $M(3, 3)$ that was also checked directly, by rerunning the calibration values with the second primitive polynomial of the degree (Remark 3.2).

The values Li and Xiong record. For reference, at $q \in \{2, 3\}$ their tables read [6, Result 1 and Theorem 1]:

$$\rho_1(M(m, 2)) = \begin{cases} 1, & m \in \{1, 2\} \\ 3, & m \geq 3 \end{cases} \quad \rho_1(M(m, 3)) = \begin{cases} 1, & m = 1 \\ 4, & m = 2 \\ 3, & m \geq 3 \end{cases}$$

$$\rho_2(M(m, 2)) = 1, 2, 5, 6, 5 \text{ for } m = 1, 2, 3, 4, \geq 5; \quad \rho_2(M(m, 3)) = 1, 4, 5 \text{ for } m = 1, 2, \geq 3.$$

Two entries of the ρ_1 tables are worth flagging: $\rho_1(M(2, 2)) = 1$ — proved outright in [6, Remark 4(1)] from the parity-check matrix displayed there, and the subject of the correction discussed in §7 — and $\rho_1(M(2, 3)) = 4$, which exceeds 3 because $M(2, 3)$ is $[8, 4]_3$ and $4 = D$ there. Of the ρ_2 values, the generic entry $\rho_2(M(m, 2)) = 5$ is proved in [6] for $m \geq 8$ and $\rho_2(M(m, 3)) = 5$ for $m \geq 6$; apart from $m = 1$, which is [6, Remark 4(1)], every remaining entry is attributed by the source's own text to a computation, in the two sentences

“A numeric experiment indicates that $\rho_2(M(2, 2)) = 2$, $\rho_2(M(3, 2)) = 5$, $\rho_2(M(4, 2)) = 6$, and $\rho_2(M(5, 2)) = \rho_2(M(6, 2)) = \rho_2(M(7, 2)) = 5$.”

“A numeric experiment indicates that $\rho_2(M(2, 3)) = 4$ and $\rho_2(M(3, 3)) = \rho_2(M(4, 3)) = \rho_2(M(5, 3)) = 5$.”

That is one reason to recompute them, which is what §3 does.

3. CALIBRATION: THE PUBLISHED VALUES RECOMPUTED

Before computing any new value we reproduced the ρ_1 and ρ_2 entries of [6] from Definition 1.1 alone. Six of them are also verified in the formal development.

Theorem 3.1. *In the model of §2,*

$$\begin{aligned}\rho_1(M(3,2)) &= 3, & \rho_2(M(3,2)) &= 5, & \rho_1(M(4,2)) &= 3, \\ \rho_1(M(2,3)) &= 4, & \rho_2(M(2,3)) &= 4, & \rho_1(M(3,3)) &= 3.\end{aligned}$$

All six agree with [6, Result 1 and Theorem 1].

Proof. Exhaustive computation, in both directions and with nothing sampled. Each upper bound $\rho_t \leq r$ is discharged either by exhibiting D columns spanning $\mathbb{F}_q^D$ (for the two entries with $r = D$, namely $\rho_1(M(2,3))$ and $\rho_2(M(2,3))$) or by checking every t -tuple of syndromes in $\mathbb{F}_q^D$ against an explicitly enumerated list of candidate index sets of size at most r : q^D tuples for $t = 1$ and q^{2D} for $t = 2$, that is at most $2^{12} = 4096$ tuples at $M(3,2)$, $2^8 = 256$ at $M(4,2)$ and $3^6 = 729$ at $M(3,3)$. The exhaustiveness of the tuple enumeration is itself proved, by induction on the tuple, rather than assumed. Each lower bound $\rho_t > r - 1$ is an explicit t -tuple of syndromes together with a scan of *every* subset of at most $r - 1$ column indices: for instance $\rho_1(M(3,2)) > 2$ uses the single syndrome $(1,0) \in \mathbb{F}_8 \times \mathbb{F}_8$ against all $1 + 7 + 21 = 29$ subsets of size at most 2, and $\rho_2(M(3,2)) > 4$ uses $\{(1,0), (\alpha, 0)\}$ against all $\sum_{j \leq 4} \binom{7}{j} = 99$ subsets. These claims rest on exhaustive computation and on nothing else. $\square$

Remark 3.2. A computation outside the formal development. The same eighteen values — ρ_1 and ρ_2 at the nine cells $(m, q) = (1, 2), (2, 2), (3, 2), (4, 2), (5, 2), (6, 2), (2, 3), (3, 3), (4, 3)$ — were computed by an independent program written in C for this purpose, which builds $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/(f)$, forms the columns (1), re-coordinates onto the column span (so that the degenerate cells are handled correctly), and then applies Lemma 2.2 directly, marking every t -dimensional subspace contained in the span of an r -subset of columns for $r = t, t + 1, \dots$ until the number of marked subspaces reaches the Gaussian binomial $\binom{D}{t}_q$. Every value agrees with [6]:

(m, q)	(1, 2)	(2, 2)	(3, 2)	(4, 2)	(5, 2)	(6, 2)	(2, 3)	(3, 3)	(4, 3)
D	1	2	6	8	10	12	4	6	8
ρ_1	1	1	3	3	3	3	4	3	3
ρ_2	1	2	5	6	5	5	4	5	5

including the eight cells whose ρ_2 value the source attributes to a numeric experiment — every cell in the table but (1, 2) — and the corrected value $\rho_1(M(2,2)) = 1$ of §7. Every value was also recomputed with the second primitive polynomial of each degree at (3, 2), (4, 2), (2, 3) and (3, 3), giving identical answers as Lemma 2.1(1) requires. This paragraph is a measurement, not a theorem; the six entries that are also theorems are those of Theorem 3.1, and $\rho_1(M(2,2))$, $\rho_2(M(2,2))$ are Theorem 7.1.

4. THE TWO CELLS THE TRIVIAL BOUND DOES NOT DECIDE

$\rho_3(M(4,2)) = 7$. $M(4,2)$ is $[15, 7]_2$, so $D = 8$ and (2) leaves $\rho_3 \in [5, 8]$; monotonicity and $\rho_2(M(4,2)) = 6$ narrow this to $[6, 8]$ (a numeric-experiment entry of [6, Theorem 1], reproduced in Remark 3.2; nothing proved below uses it). This is the smallest cell at which $2t + 1 < D$, so the trivial bound of Lemma 2.1(2) does not decide the answer.

Remark 4.1. Neither of the two published families of formulas that touch neighbouring codes applies at this cell. $M(4,2)$ has dimension 7 and so is not a repetition code, unlike $M(3,2)$ (§6); and it is not the double-error-correcting BCH code of length 15, whose generalized covering radii have been studied [11], because the Melas zero set at length 15 is the cyclotomic union $C_1 \cup C_{14} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ while the BCH one is $C_1 \cup C_3 = \{1, 2, 3, 4, 6, 8, 9, 12\}$. Neither conclusion changes at $M(5,2)$ or at the ternary cells of §5, whose dimensions are 21, 20, 4 and 72.

Theorem 4.2. $\rho_3(M(4, 2)) = 7 = 2 \cdot 3 + 1$, that is $2t + 1$ at $t = 3$.

Proof. Upper bound. Apply Proposition 2.3 with $D = 8$, $r = 7$ and the 4-dimensional space of linear forms

$$W = \langle 19, 36, 76, 134 \rangle \subseteq \mathbb{F}_2^8,$$

the integers naming forms by their coefficient vectors in the base-2 encoding of §2, a form acting by the standard inner product. For each of the 15 nonzero $\lambda \in W$ an explicit set I_λ of seven of the fifteen column indices is supplied with $\ker \lambda \subseteq \langle h_i \mid i \in I_\lambda \rangle$; the inclusion is checked exhaustively, over all $2^8 = 256$ vectors of $\mathbb{F}_2^8$ for each of the 15 forms. The space W was found by scanning all 255 nonzero forms on $\mathbb{F}_2^8$ — of which exactly 90 have their kernel inside the span of seven columns — for a 4-dimensional subspace contained in those 90. In the formal development the dimension count of Proposition 2.3 is replaced by an equivalent finite check in the compressed coordinates $v \mapsto (\langle w_1, v \rangle, \dots, \langle w_4, v \rangle) \in \mathbb{F}_2^4$: that every compressed triple admits a common nonzero annihilator ($16^3 = 4096$ triples), and that the compression is faithful, i.e. that the form with coefficient vector c against W agrees with c read against the compressed coordinate (256×15 pairs). Total decidable work about 10^6 evaluations, against 2^{24} for the naive triple search.

Lower bound. The three syndromes

$$s_1 = (1, 0), \quad s_2 = (\alpha, 0), \quad s_3 = (\alpha^6, \alpha^6) \quad \text{in } \mathbb{F}_{16} \times \mathbb{F}_{16},$$

which in the encoding of §2 are the integers 1, 2 and 204, lie in the span of no six of the fifteen columns. This is checked against *every* subset of at most six column indices, all $\sum_{j \leq 6} \binom{15}{j} = 9949$ of them. So $\rho_3 > 6$. This half rests on exhaustive computation and on nothing else. $\square$

$\rho_3(M(5, 2)) \geq 7$. $M(5, 2)$ is $[31, 21]_2$, so $D = 10$; (2) gives $\rho_3 \in [5, 9]$, and Lemma 2.1(3) with $\rho_1 = 3$ and $\rho_2 = 5$ narrows this to $[5, 8]$ — the value $\rho_2(M(5, 2)) = 5$ being another entry of [6, Theorem 1] that the source’s own text attributes to a numeric experiment, reproduced independently in Remark 3.2. Again $2t + 1 = 7 < 10 = D$.

Theorem 4.3. $\rho_3(M(5, 2)) \geq 7 = 2 \cdot 3 + 1$: the value $2t = 6$ at $t = 3$ is excluded at this cell.

Proof. The three syndromes

$$s_1 = (1, 0), \quad s_2 = (\alpha^{30}, \alpha^{11}), \quad s_3 = (\alpha^7, \alpha^{14}) \quad \text{in } \mathbb{F}_{32} \times \mathbb{F}_{32},$$

the integers 1, 242 and 948 in the encoding of §2 with the modulus $x^5 + x^2 + 1$ of (3), lie in the span of no six of the thirty-one columns. The search is exhaustive over every subset of at most six column indices, all $\sum_{j \leq 6} \binom{31}{j} = 942\,649$ of them, with the span test a rank computation over $\mathbb{F}_2$ run off precomputed addition and scalar-multiplication tables for $\mathbb{F}_2^{10}$ (the tables are proved to agree with the digitwise operations they replace, so this is an optimisation and not a change of statement). So $\rho_3 > 6$. This claim rests on exhaustive computation and on nothing else. $\square$

With the upper bound $\rho_3 \leq \rho_1 + \rho_2 = 8$ recalled above, which borrows $\rho_2(M(5, 2)) = 5$ from [6] and is not part of the formal development, this puts $\rho_3(M(5, 2)) \in \{7, 8\}$.

Remark 4.4. A computation outside the formal development. An exhaustive sweep gives the matching upper bound $\rho_3(M(5, 2)) \leq 7$ as well, and hence the exact value

$$\rho_3(M(5, 2)) = 7 = 2 \cdot 3 + 1.$$

It was run with the C program of Remark 3.2 in the formulation of Lemma 2.2: for each of the $\binom{31}{7} = 2\,629\,575$ subsets of seven of the thirty-one columns, every one of the $\binom{7}{3}_2 = 11\,811$ three-dimensional subspaces of its span was marked, $3.1 \cdot 10^{10}$ markings in all, and at the end every one of the $\binom{10}{3}_2 = 6\,347\,715$ three-dimensional subspaces of $\mathbb{F}_2^{10}$ carried a mark. The run took 4 819 seconds of CPU time. This is an exhaustive computation, but it is *not* part of the machine-checked development: the corresponding formal statement is out of budget, for the reason given in §8. Only $\rho_3(M(5, 2)) \geq 7$ (Theorem 4.3) is verified.

The shape of the answer.

Remark 4.5. Every value of $\rho_t(M(m, q))$ with $t \geq 3$ determined in this paper satisfies

$$(4) \quad \rho_t(M(m, q)) = \min\{2t + 1, D\}, \quad D = n - k,$$

and so does the value $\rho_3(M(5, 2)) = 7$ of Remark 4.4; the lower bound $\rho_3(M(4, 3)) \geq 6$ of Remark 8.1 is consistent with it. We record (4) as a description of those nine numbers, not as a conjecture, and we note at once that the same expression is *false* at $t \leq 2$: $\rho_2(M(4, 2)) = 6$ while $\min\{5, 8\} = 5$, $\rho_1(M(2, 3)) = 4$ while $\min\{3, 4\} = 3$, and $\rho_1(M(2, 2)) = 1$ while $\min\{3, 2\} = 2$. Whether $2t + 1$ rather than $2t$ is the truth in the regime $m \geq t(2t - 1)$ where [6, Theorem 4] poses the question is exactly the open problem; nothing here bears on it beyond the two data points of Theorems 4.2 and 4.3.

5. THE CELLS THE TRIVIAL BOUND DECIDES

At the remaining cells the answer equals D , so the content is entirely in the lower bound; the upper bound is Lemma 2.1(2), discharged by exhibiting D columns that span $\mathbb{F}_q^D$. In each case the lower-bound witness is a set of t syndromes spanning a t -dimensional subspace of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ which no $D - 1$ columns cover, checked against every subset of at most $D - 1$ column indices.

Theorem 5.1. $\rho_4(M(4, 2)) = \rho_5(M(4, 2)) = 8 = D$; hence $\rho_t(M(4, 2)) = 8$ for every $t \geq 4$.

Proof. The upper bound is Lemma 2.1(2): the columns $h_0, \dots, h_7$ span $\mathbb{F}_2^8$, which is checked over all 256 vectors. For the lower bound at $t = 4$, the four syndromes $(1, 0), (\alpha, 0), (\alpha^2, 0), (\alpha^3, 0)$ — a basis of the subspace $\mathbb{F}_{16} \times \{0\}$, and the integers 1, 2, 4, 8 — lie in the span of no seven of the fifteen columns; the scan covers every subset of at most seven column indices, all $\sum_{j \leq 7} \binom{15}{j} = 16384$ of them. So $\rho_4 > 7$. The case $t = 5$ is checked separately, with the fifth syndrome $16 = (0, 1)$ adjoined, rather than being inferred; it also follows from $t = 4$ by Lemma 2.1(2), as does the value for every $t \geq 4$. The lower bounds rest on exhaustive computation and on nothing else. $\square$

At $(m, q, t) = (4, 2, 4)$ the statement (2) still applies, since $t = m = 4 < 2(t + 1) + 2 \log_2 t = 14$: its first line gives $[4 + \lceil \log_2 5 \rceil, \min\{12, 8\}] = [7, 8]$, tighter than the $[6, 8]$ that monotonicity and $\rho_2(M(4, 2)) = 6$ give. At $t = 5$ it is silent, since $t > m$.

Theorem 5.1 is not implied by Theorem 4.2: $\rho_3 = 7$ is strictly smaller than 8, so the value at $t = 4$ is an independent determination. Note also that $t = 4$ is well below the range $t \geq D = 8$ in which Lemma 2.1(2) forces the value.

Theorem 5.2. $\rho_3(M(3, 3)) = 6 = D$; hence $\rho_t(M(3, 3)) = 6$ for every $t \geq 3$.

Proof. $M(3, 3)$ is $[26, 20]_3$, and (2) leaves $\rho_3 \in [5, 6]$. The upper bound is Lemma 2.1(2), with $h_0, \dots, h_5$ checked to span $\mathbb{F}_3^6$ over all 729 vectors. For the lower bound, the three syndromes $(1, 0), (\alpha, 0), (\alpha^2, 0)$ — a basis of $\mathbb{F}_{27} \times \{0\}$, the integers 1, 3, 9 — lie in the span of no five of the twenty-six columns, checked against every subset of at most five column indices, all $\sum_{j \leq 5} \binom{26}{j} = 83682$ of them. So $\rho_3 > 5$. The extension to all $t \geq 3$ is Lemma 2.1(2). The lower bound rests on exhaustive computation and on nothing else. $\square$

Theorem 5.3. $\rho_3(M(2, 3)) = 4 = D$; hence $\rho_t(M(2, 3)) = 4$ for every $t \geq 1$.

Proof. $M(2, 3)$ is $[8, 4]_3$. This is one line from Theorem 3.1: $\rho_1 = 4 = D$ there, so Lemma 2.1(2) gives $4 = \rho_1 \leq \rho_t \leq D = 4$ for every t . The case $t = 3$ is nevertheless verified independently, the upper bound from four columns spanning $\mathbb{F}_3^4$ and the lower bound from the three syndromes $1, 3, 9$ (that is, $(1, 0), (\alpha, 0), (0, 1)$) against every subset of at most three of the eight column indices. We record the cell for completeness, not as a new determination. $\square$

6. $M(3, 2)$ IS THE REPETITION CODE

The remaining cells of the table in §1 are those of $M(3, 2)$, and they are not new. We set out why, because (2) leaves the interval $[5, 6]$ at $t = 3$ here, and a reader comparing tables should know that the cell was already determined in the literature.

$M(3, 2)$ has length 7 and dimension $7 - 2 \cdot 3 = 1$. Its zero set is the union of the cyclotomic cosets of 1 and of $-1 \equiv 6$ modulo 7, namely $\{1, 2, 4\} \cup \{3, 5, 6\} = \{1, \dots, 6\}$, so its generator polynomial is $(x^7 - 1)/(x - 1)$ and $M(3, 2) = \text{Rep}_2(7)$, the binary repetition code of length 7. (In the formal development this identification is made from the parity-check side instead: the seven columns are checked to have rank 6, so $k = 1$, and their sum is checked to be zero, so the all-ones word is a codeword.) For binary repetition codes the whole hierarchy is known. Elimelech, Wei and Schwartz [4, Proposition 9] prove the formula at length 2^m ; Belinsky and Zabokritskiy [1] record, in the proof of their proposition for the case $m = 4$, that (writing [EWS] for their own citation of [4])

“The proof of the repetition-code formula in [EWS, Proposition 9] applies verbatim to arbitrary length n and gives $R_t(\text{Rep}_2(n)) = n - \lceil n/2^t \rceil$.”

Substituting $n = 7$ gives $\rho_t(M(3, 2)) = 3, 5, 6, 6, 6$ for $t = 1, \dots, 5$.

Theorem 6.1. $\rho_3(M(3, 2)) = \rho_4(M(3, 2)) = \rho_5(M(3, 2)) = 6 = D$, hence $\rho_t(M(3, 2)) = 6$ for every $t \geq 3$. These values are a substitution into the published formula $\rho_t(\text{Rep}_2(n)) = n - \lceil n/2^t \rceil$ and are not new; what is proved here is that substitution, independently and exhaustively, at a length the literally stated result of [4] does not cover.

Proof. Upper bound: six of the seven columns span $\mathbb{F}_8^6$, checked over all 64 vectors, so $\rho_t \leq 6$ for every t by Lemma 2.1(2). Lower bound at $t = 3$: the syndromes $(1, 0), (\alpha, 0), (\alpha^2, 0)$, a basis of $\mathbb{F}_8 \times \{0\}$, lie in the span of no five of the seven columns, checked against all $\sum_{j \leq 5} \binom{7}{j} = 120$ subsets of at most five column indices. At $t = 4$ and $t = 5$ the witness is extended by $(0, 1)$ and $(0, \alpha)$ and the same exhaustive scan is rerun. The lower bounds rest on exhaustive computation and on nothing else. $\square$

The same formula, at $n = 3$, also reproduces $\rho_1(M(2, 2)) = 3 - \lceil 3/2 \rceil = 1$ and $\rho_2(M(2, 2)) = 3 - \lceil 3/4 \rceil = 2$, and at $n = 7$ it reproduces the ρ_1 and ρ_2 values of Theorem 3.1; that is four further consistency checks on the identification.

7. THE DEGENERATE CODE $M(2, 2)$, AND A VALUE IN THE EARLIER LITERATURE

At $(m, q) = (2, 2)$ the minimal polynomials of α and α^{-1} coincide, so $M(2, 2)$ is not the generic $[q^m - 1, q^m - 1 - 2m]_q$ code but the $[3, 1, 3]_2$ repetition code. Li and Xiong display its parity-check matrix outright [6, Remark 4(1)],

$$\varphi(H_{1,-1}^{2,2}) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

whose three columns are exactly the three nonzero vectors of $\mathbb{F}_2^2$. That is the column list used here.

Theorem 7.1. $\rho_1(M(2, 2)) = 1$ and $\rho_2(M(2, 2)) = 2 = D$; hence $\rho_t(M(2, 2)) = 2$ for every $t \geq 2$.

Proof. Immediate, and verified: since the columns are all the nonzero syndromes, one column covers any single syndrome, and no single column covers the pair $\{(0, 1), (1, 0)\}$. Both bounds are checked over all 4 vectors of $\mathbb{F}_2^2$ and all 16 pairs. The values agree with [6, Theorem 1 and Remark 4(1)], and with the repetition-code formula of §6 at $n = 3$. $\square$

The accepted manuscript of Shi, Helleseht, Özbudak and Solé [10] — the paper whose ρ_1 values [6] quotes as its Result 1 — prints on its first text page

“In [7, Theorem 2] (see also [16]), the covering radius of $M(m, 2)$ is shown to be 3 if $m \geq 2$,”

where its [7] is Dodunekov [2] and its [16] is Moreno [9]; and the same paper’s setup names only $M(1, 2)$ and $M(1, 3)$ as degenerate, so $m = 2$ lies inside the scope of that sentence. Theorem 7.1 contradicts it at $m = 2$.

Theorem 7.2. $\rho_1(M(2, 2)) \neq 3$. Consequently the value “3 if $m \geq 2$ ” quoted above from [10] is not correct at $m = 2$.

Proof. By Theorem 7.1, $\rho_1(M(2, 2)) \leq 1 < 3$, and the refutation of the value 3 is formally separate from the determination of the value 1: it is discharged from the upper bound alone, which is the check over the four vectors of $\mathbb{F}_2^2$. $\square$

Remark 7.3. We stress the priority. Li and Xiong noticed this first: [6, Remark 4(1)] reads $\rho_1(M(2, 2)) = 1$ and $\rho_2(M(2, 2)) = 2$ off the matrix displayed above, and [6, Remark 4(2)] observes that this makes the value recorded in the earlier literature untenable. Nothing here is a new mathematical observation; what Theorem 7.2 adds is that the refutation is now machine-checked, so that the discrepancy in the literature is settled by an object a reader can re-run rather than by a claim. Nor do we determine where the slip originates. The sentence in [10] attributes the value to [2, Theorem 2]; we were unable to obtain that paper, and so make no statement at all about what its Theorem 2 says. Whether it carries a hypothesis dropped in the quotation, or is itself in error at $m = 2$, we do not know. What is established here is only that the value printed in the sentence quoted above is wrong at $m = 2$.

8. METHOD, AND WHAT IS OUT OF REACH

Two independent instruments. Everything above was computed twice, by instruments that share no code and take different routes through the definition.

The first is a program in C, described in Remark 3.2, which works in the subspace formulation of Lemma 2.2: it enumerates the r -subsets of columns, and for each one marks every t -dimensional subspace of its span in a table indexed by a canonical form of the subspace, stopping when the number of marks reaches $\binom{D}{t}_q$. Its cost is the number of markings, at most $\binom{r}{t}_q \binom{D}{r}_q$, and its memory is one entry per t -dimensional subspace of $\mathbb{F}_q^D$.

The second is the formal development, which works from Definition 1.1 directly, over lists of syndromes rather than subspaces, and uses three instruments:

- *upper bound at the redundancy:* exhibit D column indices whose columns span $\mathbb{F}_q^D$, giving $\rho_t \leq D$ for every t at the cost of one pass over the q^D syndromes;
- *upper bound below the redundancy:* the certificate of Proposition 2.3, used once, at $M(4, 2)$;
- *lower bound:* an explicit t -tuple of syndromes together with a scan of every subset of at most r column indices, the exhaustiveness of the enumeration being itself proved rather than assumed.

The lower-bound witnesses are mostly a basis of the subspace $\mathbb{F}_{q^m} \times \{0\}$, or such a basis extended by one or two vectors of $\{0\} \times \mathbb{F}_{q^m}$: a set of columns covering $\mathbb{F}_{q^m} \times \{0\}$ would have to realise every $u \in \mathbb{F}_{q^m}$ as $\sum_{i \in I} c_i \alpha^i$ subject to $\sum_{i \in I} c_i \alpha^{-i} = 0$, and for the cells here no small I can. The exceptions are Theorems 4.2 and 4.3, whose witnesses $\{(1, 0), (\alpha, 0), (\alpha^6, \alpha^6)\}$ and $\{(1, 0), (\alpha^{30}, \alpha^{11}), (\alpha^7, \alpha^{14})\}$ span subspaces meeting both factors.

What was priced and not run. Three natural continuations are out of budget, and we give the prices so that nobody repeats the estimate.

Remark 8.1. A computation outside the formal development. For $M(4, 3)$, which is $[80, 72]_3$ with $D = 8$ and interval $[5, 8]$ from (2), the $r = 5$ sweep was run: all $\binom{80}{5} = 24\,040\,016$ five-subsets of the eighty columns, $2.9 \cdot 10^{10}$ markings, 3 632 seconds of CPU time. It leaves 46 960 of the $\binom{8}{3}_3 = 25\,095\,280$ three-dimensional subspaces of $\mathbb{F}_3^8$ uncovered, so

$$\rho_3(M(4, 3)) \geq 6,$$

improving the lower end of (2) at this cell from 5 to 6 and leaving $\rho_3(M(4, 3)) \in [6, 8]$. This is an exhaustive computation but is not part of the machine-checked development, for the reason given next. The exact value needs the $r = 6$ sweep, $\binom{80}{6} \binom{6}{3}_3 = 1.0 \cdot 10^{13}$ markings, some three hundred and fifty times the largest sweep run here.

The formal counterparts of Remarks 4.4 and 8.1 were priced and parked. For the lower bound at $M(4, 3)$ the witness scan runs over $\sum_{j \leq 5} \binom{80}{j} = 25\,706\,997$ subsets with a ternary span test, about seven hours of CPU time at the rate measured on the $M(5, 2)$ file, above the per-statement budget. For the upper bound at $M(5, 2)$ neither route is affordable: the direct one enumerates 2^{30} syndrome triples, and Proposition 2.3 does not apply, because the covering sets there have codimension 3 in $\mathbb{F}_2^{10}$ rather than codimension 1, so the dimension count $\dim W + \dim A > D$ that makes the $M(4, 2)$ certificate cheap is unavailable. Finding a codimension-3 analogue of Proposition 2.3 would close that gap and is the most useful small technical step we can identify.

Beyond that: the next binary cell, $\rho_3(M(6, 2))$, needs $\binom{63}{6} \binom{6}{3}_2 = 9.5 \cdot 10^{10}$ markings, about 1.5 hours of CPU time, together with a table for the $\binom{12}{3}_2 = 4.08 \cdot 10^8$ three-dimensional subspaces of $\mathbb{F}_2^{12}$ — 8.6 GB as the hash of 64-bit keys used here, and about 51 MB with a rank-indexed bitmap, which is the fix if it is ever run. The cheapest unexplored direction is $\rho_3(M(3, 4))$, with interval $[4, 6]$ from (2) and a price of $\binom{63}{5} \binom{5}{3}_4 = 4.1 \cdot 10^{10}$ markings; it is also the most informative, since $q \geq 4$ is where (2) predicts $2t$ outright. It needs arithmetic in a non-prime field, which the present engine does not implement. And the regime in which [6, Theorem 4] poses its question, $m \geq t(2t - 1)$, begins at $m = 15$ for $t = 3$: there $n = 32\,767$ and the lower-bound scan alone is $\binom{32767}{6} \approx 1.7 \cdot 10^{21}$ subsets. That cell will be settled by an argument or not at all.

9. VERIFICATION

Every theorem above is verified in Lean 4 [5] against *Mathlib* [8], with the four exceptions named where they occur: the equality $\rho_3(M(5, 2)) = 7$ (Remark 4.4), the bound $\rho_3(M(4, 3)) \geq 6$ (Remark 8.1), the eighteen-value calibration table (Remark 3.2), and the prices in §8. The development is one definitions module and six cell modules, one per pair (m, q) , and contains no `sorry` and no hand-written axiom. Definition 1.1 is transcribed literally — the index set I is a sublist of $[n]$, hence a genuine subset of the column indices without repetitions, and the syndromes range over all of $\mathbb{F}_q^D$ — and the statement “ $\rho_t = v$ ” is proved to mean that v is the least r that works, not merely that $r = v$ works. The columns are recomputed inside the development from the modulus rather than imported from the C program, and their values are checked against the printed list; the primitivity of each modulus, the count and distinctness and nonvanishing of the columns, and the spanning property of the chosen basis are all checked rather than assumed. Each cell also carries explicit negative controls — values adjacent to the determined one, above it or below it, refuted outright — so a quantifier slip that made the covering predicate vacuously true would be visible. Checking the seven modules takes 15, 15, 34, 169, 265, 38 and 479 seconds of wall time on a machine shared with other jobs — 1015 seconds in all, against about 670 seconds of CPU time on a quieter run — the $M(3, 3)$ cell being the most expensive; both figures are measurements on a loaded machine, quoted only as an order of magnitude. The exhaustive searches are discharged by compiled evaluation, so each theorem’s axiom set consists of the three standard axioms of the ambient library together with the native evaluation axiom that compiled evaluation introduces; no other axiom occurs. Every number reported in this paper was produced first by the C program and only then stated and checked formally, so the formal run re-checks a known answer rather than searching for one. The development lives in a repository that is private at the time of writing; repository reference to be added at submission.

10. WHAT IS OPEN

The question of [6, Theorem 4] itself. It is open. For $q \in \{2, 3\}$ and $m \geq t(2t - 1)$ the value of $\rho_t(M(m, q))$ is still only known to be $2t$ or $2t + 1$. What is added here is two cells, both below that regime, at which $2t$ is excluded outright and the answer is $2t + 1$ (at $M(5, 2)$ by the sweep of Remark 4.4). Nothing above proves anything about a single cell we did not compute.

The $q = 3$ side. Remark 8.1 gives $\rho_3(M(4, 3)) \geq 6$, which at $t = 3$ is the lower value $2t$ of the ambiguity and is therefore consistent with either answer. The cheapest cell that would say something is $\rho_3(M(4, 3))$ exactly, and it costs some three hundred and fifty times the largest sweep run here; a better search than exhaustive marking is needed, or a lower-bound witness found by hand.

The $q \geq 4$ side. There (2) asserts $\rho_t = 2t$ in the asymptotic regime, with no ambiguity, and the small cells are again undetermined. $\rho_3(M(3, 4))$, with interval $[4, 6]$, is affordable and would be the first test of that answer.

A certificate at higher codimension. Proposition 2.3 turns an upper bound at codimension 1 into a bounded amount of arithmetic, and it is what makes Theorem 4.2 possible. An analogue in which the covering sets have codimension $c > 1$ — where the counting argument $\dim W + \dim A > D$ has to be replaced by something else — would put $\rho_3(M(5, 2)) \leq 7$ inside the verified layer and, more importantly, would be the natural tool for any cell with $D \geq 10$.

The structural question behind (4). A proof that the Melas column set always misses one dimension in the sense that separates $2t + 1$ from $2t$ — not a computation — would settle [6, Theorem 4]’s ambiguity. We have not found one, and the nine numbers of Remark 4.5 are not evidence for a general statement.

REFERENCES

- [1] Z. V. Belinsky and A. L. Zabokritskiy (Yohananov), *Asymptotically tight bounds for generalized covering radii of binary primitive BCH codes at all higher orders*, arXiv:2608.23833v1 (24 August 2026). The repetition-code formula quoted in §6 appears in the proof of its proposition for the case $m = 4$.
- [2] S. M. Dodunekov, *Some quasiperfect double error correcting codes*, Problems of Control and Information Theory **15** (1986), no. 5, 367–375; Zbl 0627.94020. Not obtained; the entry is as printed in [10]’s item [7] and as recorded by zbMATH.
- [3] D. Elimelech, M. Firer and M. Schwartz, *The generalized covering radii of linear codes*, IEEE Trans. Inform. Theory **67** (2021), no. 12, 8070–8085, doi:10.1109/TIT.2021.3115433; preprint arXiv:2012.06467. Definition 1, Lemma 2 and Proposition 15 are cited above through [6]; they carry those numbers in the e-print too.
- [4] D. Elimelech, H. Wei and M. Schwartz, *On the generalized covering radii of Reed–Muller codes*, IEEE Trans. Inform. Theory **68** (2022), no. 7, 4378–4391, doi:10.1109/TIT.2022.3158762; preprint arXiv:2107.09902. Its Proposition 9 (that numbering in the e-print and in [1] alike) gives the repetition-code formula at length 2^m ; the extension to arbitrary length is quoted from [1].
- [5] 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, 625–635, doi:10.1007/978-3-030-79876-5_37.
- [6] S. Li and M. Xiong, *The generalized covering radii of Melas codes*, arXiv:2608.29906v1 (30 August 2026). All numbering cited above — Definition 2, Result 1, Theorems 1–4, Remarks 1 and 4 — is that of v1, still the only version on the arXiv listing when this paper was completed.
- [7] R. Luo, Z. Zhou, S. Mesnager, V. Sagar and H. Yan, *Determining the exact value of the second-order generalized covering radius of two classes of binary cyclic codes*, Designs, Codes and Cryptography **94** (2026), no. 4, article 71, doi:10.1007/s10623-025-01799-2. Cited in [6] for $\rho_2(M(m, 2))$ at $m \geq 8$; only its abstract and publisher record were read here.
- [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, 367–381, doi:10.1145/3372885.3373824.
- [9] O. Moreno, *Further results on quasiperfect codes related to the Goppa codes*, in: Proceedings of the Fourteenth Southeastern Conference on Combinatorics, Graph Theory and Computing (Boca Raton, 1983), Congressus Numerantium **40** (1983), 249–256; Zbl 0546.94009. Not obtained; the entry is as printed in [10]’s item [16] and as recorded by zbMATH.
- [10] M. Shi, T. Hellesest, F. Özbudak and P. Solé, *Covering radius of Melas codes*, IEEE Trans. Inform. Theory **68** (2022), no. 7, 4354–4364, doi:10.1109/TIT.2022.3152092. The sentence quoted in §7 was read on the first text page of the accepted manuscript HAL hal-03581341; the page number 4354 for it is [6]’s.
- [11] M. Xiong and C. H. Yip, *On generalized covering radii of binary primitive double-error-correcting BCH codes*, arXiv:2603.21068v1 (22 March 2026). Cited only to delimit the neighbouring literature (Remark 4.1). The related papers of Özbudak and Öztürk (Finite Fields Appl. **110** (2026), 102749; Des. Codes Cryptogr. **94** (2026), article 165) were not obtained and are not cited.