The Covering Radius of RM(2, 8) is Between 88 and 91

Xiang-dong Hou[1], Evelyn Sabo[1], Freeman Slaughter[1*]

[1*]University of South Florida, Tampa, FL, USA.

*Corresponding author(s). E-mail(s): fslaughter@usf.edu;
Contributing authors: xhou@usf.edu; esabo@usf.edu;

Abstract

Let $\mathbf{RM}(r, n)$ be the rth order Reed–Muller code of length $\mathbf{2}^n$, and let $\boldsymbol{\rho}(r, n)$ denote its covering radius. The values $\boldsymbol{\rho}(2, 6) = \mathbf{18}$ and $\boldsymbol{\rho}(2, 7) = \mathbf{40}$ are known, whereas the exact value of $\boldsymbol{\rho}(2, 8)$ remains open. Starting from the current state of the art bound $\mathbf{88} \leq \boldsymbol{\rho}(2, 8) \leq \mathbf{96}$, we give a computer-assisted reduction of the upper bound $\boldsymbol{\rho}(2, 8) \leq \mathbf{91}$. We first show that every even-weight Boolean function on eight variables is within distance **90** of a quadratic function. Changing one value then gives the bound **91** for odd-weight functions. Our main lemma addresses rank-four seven-variable quintics: when their second-order distance is **36** and their maximum quadratic-shift first-order distance is **56**, they have at least **60** minimizing quadratic cosets and at most **12** cosets of cost **56**. The complete proof covers all **68443** quartic classes. For every rank-four quintic, the distance-**56** cosets are enumerated outright, and the **5199** words are examined individually. Profile counts, hyperplane contractions, and support moments then give the even-weight bound. We describe the calculations and enumerations, together with the classification upon which the proof depends. Instructions to verify the computer search portion may be found at https://github.com/EvelynSabo/RM28.

Keywords: Reed-Muller code, covering radius, Boolean function, Walsh transformation

This research was partially supported by NSF Grant DMS-2342254.

1 Introduction

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ has a unique representation

$$f(x_1, \ldots, x_n) = \sum_{I \subset \{1,\ldots,n\}} a_I \prod_{i \in I} x_i, \quad a_I \in \mathbb{F}_2.$$

The *algebraic degree* of f is $\deg f = \max\{|I| : a_I \neq 0\}$. The function f is identified with the binary vector $(f(x))_{x \in \mathbb{F}_2^n}$ of length 2^n, and its Hamming weight is $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|$. For $-1 \leq r \leq n$, the rth order *Reed-Muller code* of length 2^n is

$$\mathrm{RM}(r, n) = \{f : \mathbb{F}_2^n \to \mathbb{F}_2 : \deg f \leq r\}.$$

Set

$$d_r(f) = \min_{q \in \mathrm{RM}(r,n)} \mathrm{wt}(f + q), \quad \rho(r, n) = \max_{f : \mathbb{F}_2^n \to \mathbb{F}_2} d_r(f).$$

The covering radii $\rho(2, 6)$ and $\rho(2, 7)$ are known, with values 18 and 40, respectively [1, 2]. Thus $\rho(2, 8)$ is the smallest order-two case that has not yet been determined. It is known that $88 \leq \rho(2, 8) \leq 96$, but the precise value is a long-standing open question. We give a computer-assisted proof that $\rho(2, 8) \leq 91$, reducing the interval's width from 8 to 3.

For context, the interval recorded in [2] is $84 \leq \rho(2, 8) \leq 96$, the upper bound being $\rho(2, 7) + \rho(1, 7) = 40 + 56$. The relative covering radius of $\mathrm{RM}(2, 8)$ in $\mathrm{RM}(3, 8)$ is 88: this follows from Hou's classification of the cubic forms in eight variables [3], and is recorded as such in [4]. The witness of the lower bound below is a cubic, so that bound is a re-verification of a known value and not a new one. The new content of this manuscript is the upper bound 91.

Profile counts first bound pairs of seven-variable restrictions. A finite contraction check then supplies useful restrictions for eight-variable quintics. Finally, first and second support moments reduce degree-seven even words to either two degree-six restrictions or a two-point change of a function of degree at most five. These steps exhaust all even words. The odd bound is then a triangle inequality.

2 Preliminaries

2.1 Quadratic Profiles and Concatenation

Let $\mathcal{Q}_7$ denote the 21-dimensional vector space of homogeneous quadratics on seven variables. For $Q \in \mathcal{Q}_7$, define

$$C_f(Q) = d(f + Q, \mathrm{RM}(1, 7)), \quad M(f) = \max_Q C_f(Q), \quad N_j(f) = |\{Q : C_f(Q) = j\}|.$$

Thus $d_2(f) = \min_Q C_f(Q)$ and $\sum_j N_j(f) = 2^{21}$. The first-order covering-radius bound $\rho(1, 7) = 56$ [5, 6]gives $M(f) \leq 56$. Every affine word has even weight, so $C_f(Q)$ has the same parity as $\mathrm{wt}(f)$. In particular an odd word has $M(f) \leq 55$.

Write $g\|h$ for the function $F(x,t)$ with $F(x,0)=g(x)$ and $F(x,1)=h(x)$. Every eight-variable quadratic has the unique form $Q(x)+\ell_0(x)+t\ell_1(x)$, with Q homogeneous quadratic and ℓ_0,ℓ_1 affine. The affine functions on its two halves can therefore be chosen independently. Consequently

$$d_2(g\|h)=\min_{Q\in\mathcal{Q}_7}\big(C_g(Q)+C_h(Q)\big). \tag{1}$$

In particular

$$d_2(g\|h)\le\min\{d_2(g)+M(h),d_2(h)+M(g)\}. \tag{2}$$

Lemma 2.1. *If $|\{Q : C_g(Q)\le a\}|>|\{Q : C_h(Q)\ge b\}|$, then there is a Q with $C_g(Q)\le a$ and $C_h(Q)<b$.*

Proof The first set cannot be contained in the second. Apply (1) to an element of their difference. □

For even words the strict inequality $C_h(Q)<b$, with b even, means $C_h(Q)\le b-2$.

An invertible affine input change induces an invertible linear action on the homogeneous quadratic coefficient space; addition of a quadratic contributes a translation. Thus counts, affine-hull dimensions, and the alternating ranks of differences of quadratics are invariant under the induced affine action on $\mathcal{Q}_7$. This observation lets finite representative calculations control arbitrary relative positions of the two restrictions.

2.2 Computing Profiles

For a truth table u on m variables, put

$$W_u(a)=\sum_{x\in\mathbb{F}_2^m}(-1)^{u(x)+a\cdot x}.$$

Then $d(u,\mathrm{RM}(1,m))=2^{m-1}-\frac{1}{2}\max_a|W_u(a)|$. For seven variables write $f=f_0\|f_1$ with six-variable halves. Every homogeneous quadratic is $q(x)+t\lambda(x)$, where q has 15 coefficients and λ has six. Hence

$$C_f(q,\lambda)=64-\frac{1}{2}\max_{a\in\mathbb{F}_2^6}\big(|W_{f_0+q}(a)|+|W_{f_1+q}(a+\lambda)|\big). \tag{3}$$

The enumeration covers all $2^{15}\cdot 2^6=2^{21}$ cosets. A separate implementation avoids Walsh transforms: it computes all binary Hamming distances of each half to its 128 affine functions and takes the corresponding minima. The two kernels are compared with each other and with brute force in the `selftest` stage of the verification program `rm28_verify.py`, and again on a subset of the words in every later stage; equality of the resulting histograms is used to check the profile.

3 7-Variable Bounds

3.1 Quartics

The published catalog of $\mathrm{RM}(4,7)/\mathrm{RM}(2,7)$ under $\mathrm{AGL}(7,2)$, due to Gillot and Langevin [7, 8], contains 68443 representatives of degree at most four. The `quartic_profiles` stage computes the complete 2^{21}-coset profile of every class, together with an explicit quadratic attaining d_2; the direct-distance kernel of Section 2.2 is executed independently on all classes of distance at least 36 and on every 61st class. There are 1636 representatives at distance 36, with 33 at distance 38, and finally 4 at distance 40. The facts verified there are

$$d_2(f) = 36 \implies N_{36}(f) \geq 64, \tag{4}$$
$$d_2(f) = 38 \implies M(f) \leq 54, \quad N_{38}(f) \geq 896, \tag{5}$$
$$d_2(f) = 40 \implies M(f) \leq 52. \tag{6}$$

The inequality $M(f) \leq 54$ in (5) is not a computation. By the congruence of Section 4.1, every value of C_f for a quartic f at distance 38 is $\equiv 2 \pmod 4$, and $56 \equiv 0$. The profiles are needed for $N_{38} \geq 896$, for (4), and for (6): at distances 36 and 40 the residue is 0, so the value 56 is possible a priori and has to be excluded, or counted, by enumeration.

There is also a complete pair theorem:

Lemma 3.1 (Quartic pair theorem)**.** *For any two seven-variable quartics g, h, with arbitrary relative affine position and quadratic addition, $d_2(g\|h) \leq 90$. If their common second-order distance is* 36*,* 38*, or* 40*, the bound is* 88*.*

Section 4.1 describes the finite geometric verification; this lemma is not a consequence of the four inequalities alone. Only the bound 90 is used in Section 6. The value 88 for equal distances is a by-product of the same computation through the congruence of Section 4.1, and nothing downstream depends on it.

3.2 Degree-6 Functions

The complete degree-six restriction calculation gives $d_2(f) \leq 38$; Section 7.1 supplies its separate argument. The refinements used here are

$$d_2(f) = 38 \implies M(f) \leq 54,\ N_{38}(f) \geq 968,\ N_{54}(f) \leq 8, \tag{7}$$
$$d_2(f) = 36, M(f) = 56 \implies N_{36}(f) = 512,\ N_{56}(f) = 16. \tag{8}$$

The entire profile in the second line is

j	36	38	40	42	44	46
N_j	512	1,472	7,488	35,904	132,160	408,448
j	48	50	52	54	56	
N_j	808,896	647,296	54,928	32	16	

These numbers sum to 2^{21}.

To prove completeness of the distance-38 calculation, proceed as follows. For a degree-six seven-variable word put $v = \sum_x f(x)x \neq 0$ and $G = \sum_x f(x)xx^t$. The checked algebraic quartic-distance formula is

$$d(f, \mathrm{RM}(4,7)) = 2 + \operatorname{rank}(G|_{v^\perp}). \tag{9}$$

We justify this formula algebraically, independently of random tests of the construction. If an even correction set has size k and first moment v, evaluate a basis of $v^\perp$ on its k points. Each resulting row has even weight. The ordinary dot product on the even-weight subspace of $\mathbb{F}_2^k$ has the all-one vector in its radical, so its rank is $k-2$. Consequently $\operatorname{rank}(G|_{v^\perp}) \leq k-2$. Conversely take coordinates with $v = e_7$, and write this restricted rank as r. For $r = 0$ use the two points $0, e_7$. For positive even r use $e_7, e_1, \ldots, e_r, e_1 + \cdots + e_r$. Their first moment is e_7 and their restricted second moment has off-diagonal entries one on an r-space and rank r. Congruence of alternating forms supplies the desired restricted matrix. Translation by a vector in the first six coordinates adjusts the cross column to the desired one without changing the first moment. Thus a correction of size $r+2$ exists with the moments of f. Equal parity, first moments, and second moments mean that the difference has degree at most four. This proves the formula.

The restriction is an alternating form on a six-dimensional space, so this distance is $2, 4, 6$, or 8. If an eight-point correction set lies in $a \cdot x = c$, then $a \cdot v = 0$ and $Ga = cv$. The vector a is a nonzero radical vector of $G|_{v^\perp}$, contradicting rank six. Thus a nearest correction of size eight must be an affine basis.

The `affine8` stage enumerates every eight-point affine basis E around every quartic class u with $d_2(u) \geq 30$ and finds no word $u + \mathbf{1}_E$ of second-order distance 38 (the 4065 classes with $d_2(u) \leq 28$ cannot achieve 38 after an eight-point change). Every other degree-six word has quartic distance at most six. A two-point correction can be enlarged to six by symmetric difference with an affine three-flat containing both points. A four-point correction with nonzero support sum consists of affinely independent points; choose a three-flat containing only three of them. Its symmetric difference again has size six. Three-flat indicators in seven variables are quartics, so they can be absorbed into the quartic representative. The resulting six-point set has nonzero vector sum, since that sum is the first moment of a degree-six word.

Consequently every degree-six distance-38 function occurs in the complete six-point search (stage `support6`: six points of nonzero sum) over quartics of distance at least 32. It returns 2875 words of distance 38 and none of larger distance; all 2875 full profiles satisfy (7).

3.3 The Degree-6 First-Order-56 Classification

To verify (8), add a quadratic so that $d_1(f) = 56$. Choose a hyperplane normal a with $a \cdot v = 1$. Both six-variable restrictions g, h have odd weight, and the condition becomes

$$|W_g(b)| + |W_h(b)| \leq 16 \quad (b \in \mathbb{F}_2^6).$$

Odd six-variable Walsh coefficients are nonzero and congruent to 2 modulo 4, so each of $|W_g(b)|$, $|W_h(b)|$ is at most 14 and both restrictions have first-order distance at least 25. An odd six-variable word has first-order distance at most 27. The complete six-variable catalog (modulo affine input changes and affine output additions) therefore leaves 983 odd classes at distance 25 and four at distance 27 [9].

The `first56` stage takes g to be one of these 987 candidate classes and h to be a second candidate in an arbitrary relative position. A relative translation of one restriction can be removed by the shear $(x, t) \mapsto (x+ts, t)$. The remaining relative linear input and affine output changes act on the frequency space $\mathbb{F}_2^6$ as affine permutations π, so that $|W_h| = |W_{h'}| \circ \pi$ for the catalog representative h' of the class of h. Of the $987 \cdot 988/2 = 487578$ unordered pairs of candidate classes, 80199 are excluded by the six-variable split formula, a minimum plus a maximum profile value being at most 34. For each of the remaining 407379 pairs, a recursion enumerates all affine permutations π with $|W_g(b)| + |W_{h'}(\pi(b))| \le 16$ for every b: it assigns an affine frame, rejects dependent images, and rejects any forced image violating the inequality. Only 307331 compatible maps survive, and for each the split distance $\min_Q \big(C_g(Q) + C_h(Q)\big)$ is evaluated on the complete six-variable profiles. Only two maps give distance at least 36, and both are in fact precisely 36. The two seven-variable words are reconstructed from their maps, checked to satisfy the Walsh inequality, to have degree six and $M = 56$, and fully profiled. Their truth tables, as 128-bit integers with $f(x)$ at bit x, are

```
153364569999351074103652695127337602240
162989620139968284118969181192072596672,
```

and both have the profile of the table above.

3.4 Rank-4 Quintics

For a seven-variable quintic, complementing the indices of its degree-five monomials gives an alternating 7×7 matrix. Its rank is unchanged by invertible input substitutions. A rank-four leading part is represented by the second moment of the six-point set

$$E_0 = \{0, e_1, e_2, e_3, e_4, e_1 + e_2 + e_3 + e_4\}.$$

Its support sum is zero and its second-moment matrix has rank four. The congruence classification of alternating forms therefore shows that every rank-four quintic is a quartic plus six distinct points of vector sum zero. No enumeration of the full space of quintics is asserted.

Conversely, every six-point set E with $\sum_{x \in E} x = 0$ has second moment of rank four, so the support enumeration below loses nothing by not filtering on rank. Rank 0 would put the weight-six word $\mathbf{1}_E$ in $\mathrm{RM}(4, 7)$, whose minimum weight is 8. Rank 2 would give $\mathbf{1}_E + \mathbf{1}_P \in \mathrm{RM}(4, 7)$ for some 2-flat P, a word of weight $10 - 2|E \cap P|$, that is 10 or 8 according as $|E \cap P|$ is 0 or 1 (larger intersections give nonzero weights below 8). But $\mathrm{RM}(4, 7)$ has no words of weight 10, and its weight-8 words are 3-flats [10], which cannot meet the 2-flat P in the three points of $P \setminus E$.

The `rank4` stage enumerates every six-point support of vector sum zero around every quartic class with $d_2 \geq 30$ (a class with $d_2 \leq 28$ cannot reach 36 after a six-point change) and keeps the 2923088 supports whose word has second-order distance at least 36. It gives

$$d_2(f) \leq 38; \quad d_2(f) = 38 \implies M(f) \leq 54, \quad N_{38}(f) \geq 608, \quad N_{54}(f) \leq 576. \tag{10}$$

Exactly 23 of the supports have distance 38, all fully profiled, and none has distance 40. The additional finite lemma needed for the new global bound is

Lemma 3.2 (Rank-four profile bound)**.** *If f is a rank-four seven-variable quintic, $d_2(f) = 36$, and $M(f) = 56$, then $N_{36}(f) \geq 60$ and $N_{56}(f) \leq 12$.*

Among the 2923065 supports at distance 36, the stage counts the cost-56 cosets as described in the next subsection. Only 5199 of the words have $M = 56$; over these the minimum of N_{36} is 60 and the maximum of N_{56} is 12, which proves the lemma. Every other word has $N_{56}(f) = 0$, which is all that Corollary 4.3 needs. The next subsection shows that the count is precise.

3.5 Counting the Cost-56 Cosets

For a six-point change $f = u + \mathbf{1}_E$ of a quartic u one has $|C_f(Q) - C_u(Q)| \leq 6$ for every Q, so $C_f(Q) = 56$ forces $C_u(Q) \geq 50$. The `rank4` stage therefore counts $N_{56}(f)$ by testing only the quadratics with $C_u(Q) \geq 50$, read off the quartic profile. We specify the test explicitly.

Write such a word as $f = f_0 \| f_1$ on the last coordinate of the representative, and write a homogeneous quadratic as $Q = q + t\lambda$ with $q \in \mathcal{Q}_6$ and $\lambda \in \mathbb{F}_2^6$, as in (3). Then (3) at the value 56 reads

$$C_f(q, \lambda) = 56 \iff \max_{a \in \mathbb{F}_2^6} \big(|W_{f_0+q}(a)| + |W_{f_1+q}(a+\lambda)| \big) = 16. \tag{11}$$

The count runs over the values of q for which some λ has $C_u(q+t\lambda) \geq 50$ and computes the two spectra W_{f_0+q} and W_{f_1+q}. If either spectrum has an entry of absolute value above 16, the sum in (11) exceeds 16 for every λ at that a, and q is rejected. Otherwise every λ with $C_u(q + t\lambda) \geq 50$ is tested against (11), and the count is the number of pairs (q, λ) that attain 16.

Proposition 3.3. *The count equals $N_{56}(f)$. In particular $M(f) = 56$ when the count is positive, and otherwise $M(f) \leq 54$.*

Proof The map $(q, \lambda) \mapsto q + t\lambda$ is a bijection onto $\mathcal{Q}_7$, (11) is the equivalence $C_f(Q) = 56$ coset by coset, and the early rejection discards only pairs whose maximum is already above 16. A pair with $C_u(q + t\lambda) < 50$ has $C_f(q + t\lambda) < 56$ by the triangle inequality, so omitting it loses nothing. Since $C_f(Q) \leq 56$ for every Q, a positive count means $M(f) = 56$ and a zero count means $M(f) < 56$. The words have even weight, so C_f takes even values and $M(f) < 56$ is $M(f) \leq 54$. □

The value $N_{36}(f)$ of a support may be read off the bank of Section 3.6. The whole `rank4` enumeration took about ten CPU-hours. On every sixteenth class, the bank statistics and the cost-56 count of one support are checked against an independent complete profile computed by direct Hamming distances (3518 classes in the recorded run).

Corollary 4.3 below: every word of the relevant family at distance 36 has more minimizing cosets than cost-56 cosets. For a word with $N_{56}(f) = 0$ this is $N_{36}(f) > 0 = N_{56}(f)$; for the 5199 words with $M(f) = 56$ it is $60 > 12$.

3.6 Support Enumeration and Symmetry Reduction

Suppose a quartic u is changed on a k-point set E. For an explicit quadratic q, let $B_q = \operatorname{supp}(u + q)$ and $w_q = |B_q|$. Then

$$\operatorname{wt}(u + \mathbf{1}_E + q) = w_q + k - 2|E \cap B_q|. \tag{12}$$

Thus a putative distance at least D requires $|E \cap B_q| \le \lfloor (w_q + k - D)/2 \rfloor$ for every supplied q. The depth-first search traverses all distinct-point supports satisfying these necessary inequalities and the required degree or moment conditions (vector sum nonzero for `support6`, affine independence for `affine8`, vector sum zero for `rank4`). A quadratic with $w_q \ge D + k - 1$ never constrains E, so the bank of all pairs (Q, ℓ) with $w_q \le D + k - 2$ provides a test: the search enforces the strongest inequalities while choosing points, every survivor is then tested against the whole bank, and the final list is exactly $\{E : d_2(u + \mathbf{1}_E) \ge D\}$.

The stabilizer generators listed in the catalog reduce equivalent support prefixes. Every generator used is re-verified by truth-table substitution: $u(Ax + c) + u(x)$ must have degree at most two. Any set of verified elements generates a subgroup G of the stabilizer, and reducing modulo a subgroup is sound: G permutes the bank and preserves the three predicates, so the surviving supports form a G-invariant set, and one representative per G-orbit of prefixes (to depth three, using the G-orbits of ordered pairs and triples) suffices. The three enumerations share one profile, one bank, and one set of normalization cases per class. The stage is sharded and resumable; a missing class leaves its certificate `INCOMPLETE`, in which case the `final` stage does not conclude.

4 Pair Bounds

4.1 Quartic Pairs

For quartic u and quadratic q, $\operatorname{wt}(uq)$ is even, since $\deg(uq) \le 6$ in seven variables. Also $\operatorname{wt}(q)$ is divisible by four. Hence $\operatorname{wt}(u+q) \equiv \operatorname{wt}(u) \pmod 4$, including affine terms in q. Every value of C_u has that residue. For equal-distance quartic pairs at distances $36, 38, 40$, excluding a split distance of at least 92 therefore gives the stronger bound 88.

Let $L_u = \{Q : C_u(Q) = d_2(u)\}$ and $H_u = \{Q : C_u(Q) \ge 92 - d_2(u)\}$. A hypothetical split distance at least 92 requires an affine quadratic-coefficient map ϕ satisfying

$$\phi(L_g) \subseteq H_h, \quad \phi^{-1}(L_h) \subseteq H_g.$$

First compare the two cardinalities. Next, in the space of linear forms V, consider the six-dimensional star $W_\ell = \{\ell \wedge m : m \in V\}$ for each nonzero ℓ. Set $m_S(\ell) = \max_t |S \cap (t + W_\ell)|$. An embedding induced by an invertible map A requires $m_S(\ell) \le m_T(A\ell)$; the reverse embedding must use the same A. Sorted star maxima give necessary inequalities.

At distance 38, cardinality excludes 362 of the 561 unordered pairs, and star maxima exclude the other 199. At distance 36, the 1339066 unordered pairs split into 1337840 cardinality exclusions, 1221 star exclusions, and 5 residual pairs. Catalog indices here and in the certificates are zero-based.

Residual pair	Final obstruction
$(4, 4)$	Exhaustive relative-position search
$(67986, 67986)$	Affine-hull dimensions 15 and 12
$(67986, 68382)$	Reverse dimensions 13 and 12
$(68382, 68382)$	Ranks in annihilators of affine hulls
$(68385, 68385)$	Exhaustive relative-position search

For $(68382, 68382)$, the annihilator of the affine hull of the high set is a three-space whose seven nonzero alternating forms have rank two, and the annihilator of the low set contains no such three-space; the `quartic_pairs` stage checks this over all three-spaces of rank-two forms. The two remaining pairs go to an exhaustive relative-position search. A relative position is a pair (B, t) with $B \in \mathrm{GL}(7, 2)$ acting on the coefficient space and t a translation by a quadratic. The search assigns the images of the linear forms one at a time, subject to the star conditions above and normalized by the verified linear symmetries of the second class; for each complete B it enumerates the translations t compatible with the set inclusions and checks every candidate on the full 2^{21} profiles. For $(4, 4)$ the star conditions admit 1344 maps B, and none of the 2359296 candidate pairs (B, t) passing the inclusions yields a split distance 92; for $(68385, 68385)$ the star conditions admit no map at all.

For distance 40, cardinality excludes four of the ten unordered pairs and star maxima five. The remaining self-pair, class 68380, is excluded by the same exhaustive search: the star conditions admit 55296 maps B, and no translation satisfies the inclusions for any of them.

Finally, unequal quartic distances require no orbit search. A minimum at most 34 gives $34 + 56 = 90$; the remaining pairs 36/38, 36/40, and 38/40 give respectively 90, 88, and 90 by (5)–(6). This proves Lemma 3.1.

4.2 Quartics Changed at One Point

Lemma 4.1. *If u, v are arbitrary seven-variable quartics and p, q are arbitrary points, then $d_2((u + \delta_p) \| (v + \delta_q)) \le 90$.*

Proof The `point_changes` stage gives the following exhaustive alternatives:

- If $d_2(u) \le 34$, then $d_2(u + \delta_p) \le 35$.

- If $d_2(u) = 36$, nearest-quadratic error sets cover every point, so again $d_2(u + \delta_p) = 35$. For each of the 1636 classes a greedy cover by nearest error sets is recorded, 11578 explicit quadratics in all, each checked for degree, distance, and coverage.
- If $d_2(u) = 38$, every point change has distance 37 and $N_{37}(u + \delta_p) > N_{55}(u + \delta_p)$. All $33 \cdot 128$ point changes are fully profiled, every 37th by both kernels of Section 2.2.
- If $d_2(u) = 40$, every point change has distance 39, maximum at most 53, and $N_{39} > N_{53}$. Again all $4 \cdot 128$ point changes are profiled.

Write the changed words as g, h. If either minimum is at most 35, use $35 + 55 = 90$. Minima 37/39 give $37 + 53 = 90$. For two minima 37, a split distance at least 92 would require $N_{37}(g) \le N_{55}(h)$ and $N_{37}(h) \le N_{55}(g)$, contradicting the two strict inequalities. The same argument with 39/53 handles two minima 39. The split has even weight, so a value below 92 is at most 90. This proves the claim for independent quartics; no common global quartic is required. □

Remark 4.2. The residue-4 congruence of Section 4.1 does not survive a point change. For a quadratic q one has $\mathrm{wt}(\delta_p q) = q(p)$, which is odd for half of the quadratics, so $C_{u+\delta_p}$ is constrained only modulo 2. The values 37 and 55 (or 39 and 53) are both of the right parity, no congruence excludes 55, and the point-change profiles above have to be computed.

4.3 Degree-6 and Rank-4 Pairs

Let $\mathcal{A}$ be the union of seven-variable degree-six functions and rank-four quintics.

Corollary 4.3. *Every $f \in \mathcal{A}$ with $d_2(f) = 36$ satisfies $N_{36}(f) > N_{56}(f)$.*

Proof If $M(f) \le 54$ then $N_{56}(f) = 0 < N_{36}(f)$. If $M(f) = 56$, then for a degree-six word (8) gives $512 > 16$, and for a rank-four quintic Lemma 3.2 gives $60 > 12$. By Proposition 3.3 the `rank4` stage decides which case applies to every support, and records N_{36} and N_{56} in the second. □

Lemma 4.4. *If $g, h \in \mathcal{A}$, then $d_2(g\|h) \le 90$.*

Proof All words in $\mathcal{A}$ have even weight and minimum at most 38. If one minimum is at most 34, use $34 + 56 = 90$. Otherwise the minima are 36 or 38. A 36/38 pair gives $36 + 54 = 90$ by the maximum-54 bound on the distance-38 side, from (7) or (10). For 38/38, at least 608 minimizing cosets cannot fit among at most 576 opposing cost-54 cosets, giving $38 + 52 = 90$. For 36/36, apply Corollary 4.3 to both words. If $N_{36}(g) \le N_{56}(h)$ and $N_{36}(h) \le N_{56}(g)$ held together, then

$$N_{36}(g) \le N_{56}(h) < N_{36}(h) \le N_{56}(g) < N_{36}(g),$$

which is absurd. So one of the two inequalities fails, and Lemma 2.1 with $a = 36$, $b = 56$ gives a Q of cost 36 on one side and cost below 56, hence at most 54, on the other: $36 + 54 = 90$. □

Remark 4.5. Lemma 3.2 is needed at full strength only when both words are rank-four quintics. Against a degree-six word with $M = 56$, whose profile is fixed by (8), the obstruction needs only $N_{56} \le 511$ or $N_{36} \ge 17$ on the rank-four side.

Lemma 4.6. *If g has degree six and h is quartic, then $d_2(g\|h) \le 90$.*

Proof A minimum at most 34 suffices. If the quartic minimum is 40, its maximum is at most 52, giving $d_2(g) + 52 \le 90$. For minima 36/38 or 38/36, use the maximum-54 bound on the distance-38 side. For 36/36, only $M(g) = 56$ can cause difficulty; then the quartic's at least 64 minimizers cannot fit in the degree-six word's 16 cost-56 positions. For 38/38, use the quartic's at least 896 minimizers and the degree-six word's at most eight cost-54 positions. □

5 Hyperplane Reductions

Let $V = \mathbb{F}_2^8$. Complementing monomial indices identifies $\mathrm{RM}(5,8)/\mathrm{RM}(4,8)$ with the trivectors $\Lambda^3 V$, so the leading part of an eight-variable quintic is a trivector T. A hyperplane normal a is a linear form on V, and the two restrictions to $a = 0$ and $a = 1$ share the same leading part, the restriction of the quintic form to $\ker a$; a translation into the affine hyperplane only adds terms of lower degree. The contraction $\iota_a T \in \Lambda^2 V$ satisfies $\iota_a \iota_a T = 0$, so it lies in $\Lambda^2(\ker a)$ and has rank at most six. In coordinates with $a = e_8^*$ the dual 7×7 alternating matrix of the common leading part is the matrix of $\iota_a T$ with its eighth row and column deleted, and since a is in the radical of the 8×8 contraction matrix $(\sum_k a_k T_{ijk})_{ij}$, the two ranks agree. The identity is independently checked on all 56 basis trivectors and all 255 normals, a total of 14280 checks (stage `directions`). Linearity in T then proves it for every quintic leading part, and equivariance under $\mathrm{GL}(V)$ removes the choice of coordinates. Throughout, $a \in v^\perp$ means $a(v) = 0$ for a vector $v \in V$.

The complete list of 32 three-form types, that is, of the $\mathrm{GL}(8,2)$-orbits of cubic forms in eight variables [3], extracted by the `directions` stage from the nine-variable catalog [11] as the forms with nonzero radical, gives:

1. Every type has a nonzero normal with contraction rank 0 or 4.
2. For every type and every nonzero vector v, either there is a normal $a \in v^\perp$ of contraction rank 0 or 4, or there is a normal $a \notin v^\perp$ of contraction rank 0.

The second enumeration covers $32 \cdot 255 = 8160$ type/vector pairs: 8032 use the first alternative and 128 use the second. For every type the ranks are computed both by contraction and from the actual hyperplane restrictions of the dual quintic, and the two agree.

Rank zero means both restrictions have degree at most four; rank four means both are rank-four quintics. The lower-degree terms of the original function do not change these leading ranks.

6 The Covering-Radius Bounds

For any Boolean word on m variables, its parity is the coefficient of the full degree-m monomial. Thus an even eight-variable word F has degree at most seven. We consider all possible degrees.

6.1 Degree at Most 5

If $\deg F \le 4$, any hyperplane split gives two quartics, and Lemma 3.1 applies. If $\deg F = 5$, the first direction statement in Section 5 supplies either two quartic restrictions or two rank-four quintic restrictions. Apply Lemma 3.1 or Lemma 4.4, respectively.

6.2 Degree 6

A nonzero sextic monomial omits two coordinates. Split on either omitted coordinate. The selected sextic term survives in both restrictions, so both have degree six. Lemma 4.4 applies.

6.3 Degree 7 and the 2-Point Moment Reduction

Define

$$v = \sum_x F(x)x, \quad G = \sum_x F(x)xx^t.$$

Since F is even, v is the complementary encoding of its septic part. In degree seven $v \neq 0$. The matrix G is symmetric and $\operatorname{diag} G = v$. For a normal $a \in v^\perp$, both restrictions have even weight. Their ambient first moments are Ga and $v + Ga$. If $Ga \notin \{0, v\}$, both are nonzero and both restrictions have degree six. Lemma 4.4 settles this case.

It remains that $G(v^\perp) \subseteq \langle v \rangle$. Make an invertible linear coordinate change taking v to e_8. Symmetry and $\operatorname{diag} G = e_8$ force

$$G = \begin{pmatrix} 0 & u \\ u^t & 1 \end{pmatrix}, \quad u \in \mathbb{F}_2^7.$$

Choose p whose first seven coordinates are u, and set $q = p + v$. The two-point word $\delta_p + \delta_q$ has first moment v and second moment G: indeed $pp^t + (p+v)(p+v)^t = pv^t + vp^t + vv^t$. Therefore

$$H = F + \delta_p + \delta_q$$

is even and has zero first and second moments. The coefficients of degrees eight, seven, and six consequently vanish, so $\deg H \le 5$. (The `algebra` stage checks the moment identities and this two-point reduction exhaustively over all 32640 unordered point pairs.)

If $\deg H \le 4$, choose a hyperplane separating p, q and apply Lemma 4.1. If H is quintic, apply the second direction statement of Section 5 to its leading three-form and $v = q - p$. In the nonseparating alternative, the points lie in one restriction. That restriction of F is a quartic or rank-four quintic plus two points whose difference is nonzero; it has even weight and nonzero first moment, hence degree six. The unchanged restriction is quartic or rank-four quintic. Lemma 4.6 or Lemma 4.4 applies. In the separating alternative, both restrictions of H are quartics and each is changed at one point. Lemma 4.1 applies. This exhausts degree seven and proves the even-weight bound 90. The `final` stage re-reads every certificate, re-checks from the recorded values the inequalities combined in Lemmas 4.4 and 4.6, and writes the certificate `MASTER`.

7 Computation

All finite computations are performed by the program `rm28_verify.py` in the repository named in the abstract (also wrapped as the Colab notebook `RM28_colab.ipynb`). It uses only the four public catalogs of Section 3.1, Section 3.3, Section 5 and Section 7.1, downloaded from their authors' sites with SHA-256 digests recorded, and it runs in stages, each of which writes a JSON certificate:

Stage	Certificate	Supports
`catalogs`	`catalogs`	the four catalogs and their class counts
`selftest`	`selftest`	Section 2.2
`witness`	`witness`	Section 8
`directions`	`directions`	Section 5
`algebra`	`algebra`	formula (9), Section 6
`quartic_profiles`	`quartic_profiles`	(4)–(6)
`point_changes`	`point_changes`	Lemma 4.1
`quartic_pairs`	`quartic_pairs`	Lemma 3.1
`degree6_bound`	`degree6_bound`	Section 7.1
`first56`	`first56`	(8)
`supports`	`support6`, `affine8`, `rank4`	(7), (10), Lemma 3.2
`final`	`MASTER`	Lemmas 4.4 and 4.6, Theorem 8.1

Every certificate records the inputs, their digests, the program version and its digest, and the quantities quoted in the text. A complete run on a 20-thread laptop took about 3.5 hours of wall time, of which the three support enumerations account for about 29 CPU-hours.

7.1 The Degree-6 Restriction Bound

We now give the finite argument behind the bound $d_2(f) \le 38$ for degree-six seven-variable words (stage `degree6_bound`).

Split a degree-six word on a coordinate omitted by one nonzero sextic monomial. Both six-variable restrictions have odd weight. The published classification modulo quadratics [9, 12] has 205 classes, of which 85 are odd. Compute their complete 2^{15}-entry quadratic profiles. As in Section 4.1, the relative position of the two restrictions is encoded by an affine bijection ϕ of the 15-dimensional coefficient space, and a putative split distance at least 40 requires

$$\phi\big(\{Q : C_g(Q) \le a\}\big) \subseteq \{Q : C_h(Q) \ge 40 - a\},$$
$$\phi^{-1}\big(\{Q : C_h(Q) \le a\}\big) \subseteq \{Q : C_g(Q) \ge 40 - a\}.$$

for every threshold a, with one and the same ϕ for all a. Of the $85 \cdot 86/2 = 3655$ unordered odd/odd class pairs, 3607 are excluded by the split formula alone, a minimum plus a maximum profile value being at most 38. Cardinality and affine dimension of these sets are invariants of ϕ and reject 8 and 15 further pairs, and the star-maxima

matching of Section 4.1 rejects 22 more. The last three pairs,

$$\begin{aligned} U &= ace + bce + bde + bcf + adf + abcdef \quad \text{with itself,} \\ A &= abcd + bce + ade + abf + abcdef \quad \text{with itself,} \\ & \quad bcd + ace + abf + abcdef \\ & \qquad \text{with} \quad abd + acd + ace + bcde + bcf + acdf + abef + abcdef, \end{aligned}$$

are excluded by the exhaustive relative-position search of Section 4.1, now over $\mathrm{GL}(6,2)$ and the 2^{15} quadratic translations: for (U,U) the star conditions admit 774144 maps and no translation satisfies the inclusions for any of them, for (A,A) they admit no map at all, for the third pair 602112 maps are examined and none admits a translation.

Every odd/odd split therefore has distance below 40. Its weight is even, so its quadratic distance is at most 38, as required. The completeness of the 205-class six-variable catalog is an additional external input; the `catalogs` stage downloads it, together with the other three catalogs, and records their digests.

8 The Lower Bound and the Main Theorem

For the lower bound, consider the eight-variable cubic

$$w(a,b,c,d,e,f,g,h) = abc + adg + afh + agh + bdh + beg + ceh + def,$$

taken from the cubic-forms catalog of Brier and Langevin [11, 13]; the classification of cubic forms in eight variables is due to Hou [3]. Its truth table is represented in hexadecimal by

```
01010101010101fe0154326701543298
01320e3d54675b975432680e01673da4
```

Concatenate the lines, expand each hexadecimal digit most significant bit first, and index the resulting bits by the integers $\{0,\dots,255\}$, with a the least significant bit of the input index. An exhaustive computation over all quadratic forms and affine functions (stage `witness`, by a Walsh decoder split on h and by an independent direct decoder) gives

$$\max_{\substack{Q \text{ homogeneous quadratic} \\ \ell \text{ affine}}} \left| \sum_{x \in \mathbb{F}_2^8} (-1)^{w(x)+Q(x)+\ell(x)} \right| = 80.$$

Consequently,

$$d_2(w) = 128 - \frac{80}{2} = 88,$$

attained by 28672 quadratics, for instance by $h(1{+}a{+}c{+}f{+}g)$, so $\rho(2,8) \geq \rho_{2,3}(8) \geq 88$, where $\rho_{2,3}(8)$ denotes the relative covering radius of $\mathrm{RM}(2,8)$ in $\mathrm{RM}(3,8)$.

Theorem 8.1. $88 \leq \rho(2, 8) \leq 91$.

More specifically, every even-weight eight-variable word has second-order distance at most 90*, and every odd-weight word has distance at most* 91*.*

Proof We have shown the upper bound for even words is 90. If F is odd, choose any point p. The word $F + \delta_p$ is even, so

$$d_2(F) \leq d_2(F + \delta_p) + 1 \leq 91.$$

Combined with the established lower bound of 88 this concludes the proof. □

9 Conclusion

In this manuscript, we set out to narrow the interval for $\rho(2, 8)$, and reduced the upper bound from 96 to 91. The lower bound of 88 was already implicit in the classification of cubic forms; we have re-verified it with an explicit cubic and two exhaustive decoders. The upper bound is the novelty of this work. It derives from splitting an eight-variable function into its two seven-variable halves, asking how well a single quadratic can interact with both at once, and answering using the seven-variable catalogs instead of any eight variable classification. Even-weight functions come within 90 of a quadratic; odd-weight functions follow by changing a single bit.

What we have shown is conditional on the completeness of the four catalogs we drew from – everything else is a computer enumeration performed by `rm28_verify.py`, which can be re-run by anyone.

A further reduction of these bounds would be welcome. Our techniques stop at the even bound, and the odd bound is a triangle inequality we could not improve on. Whether some odd-weight function sits at distance 91, or whether a quartic or quintic beats the cubic's 88, we leave for future work.

Statements and Declarations

Funding. This research was partially supported by National Science Foundation (NSF) Grant DMS-2342254.

Competing interests. The authors have no relevant financial or non-financial interests to disclose.

Author contributions. All authors contributed substantially to this work. Author name ordering is alphabetical.

Data availability. The verification program `rm28_verify.py`, the Colab notebook `RM28_colab.ipynb`, and the certificates of a complete run are available in the repository https://github.com/EvelynSabo/RM28

Use of artificial intelligence. Large language models (ChatGPT and Fable) were used as a sounding board during the work, to assist in refining the computer search code, and for editing and typesetting the manuscript. All mathematics, code, and verification were written and checked by the authors, who take full responsibility for the content of this document.

References

[1] Schatz, J.R.: The second order Reed-Muller code of length 64 has covering radius 18. IEEE Transactions on Information Theory **27**(4), 529–530 (1981) https://doi.org/10.1109/TIT.1981.1056364

[2] Wang, Q.: The covering radius of the Reed-Muller code $RM(2,7)$ is 40. Discrete Mathematics **342**(12), 111625 (2019) https://doi.org/10.1016/j.disc.2019.111625 1809.04864

[3] Hou, X.-d.: $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$. Discrete Mathematics **149**(1–3), 99–122 (1996) https://doi.org/10.1016/0012-365X(94)00342-G

[4] Khoruzhii, K., Gelß, P., Pokutta, S.: The weight distribution of the third-order Reed-Muller code of length 2048 (2026). https://arxiv.org/abs/2607.02365

[5] Mykkeltveit, J.: The covering radius of the $(128,8)$ Reed-Muller code is 56. IEEE Transactions on Information Theory **26**(3), 359–362 (1980) https://doi.org/10.1109/TIT.1980.1056187

[6] Hou, X.-d.: Covering radius of the Reed-Muller code $R(1,7)$ – a simpler proof. Journal of Combinatorial Theory, Series A **74**(2), 337–341 (1996) https://doi.org/10.1006/jcta.1996.0055

[7] Gillot, V., Langevin, P.: Classification of some cosets of the Reed-Muller code. Cryptography and Communications **15**(6), 1129–1137 (2023) https://doi.org/10.1007/s12095-023-00652-4

[8] Gillot, V., Langevin, P.: Classification of $B(s,t,7)$ (2022). https://langevin.univ-tln.fr/project/agl7/aglclass.html Accessed 2026-10-18

[9] Langevin, P.: Classification of Boolean functions under the affine group: six variables. https://langevin.univ-tln.fr/project/agl/agl.html Accessed 2026-10-18

[10] Kasami, T., Tokura, N.: On the weight structure of Reed-Muller codes. IEEE Transactions on Information Theory **16**(6), 752–759 (1970) https://doi.org/10.1109/TIT.1970.1054545

[11] Langevin, P.: Classification of Boolean cubic forms: project page and 349-representative data file. https://langevin.univ-tln.fr/project/cubics/ Accessed 2026-10-18

[12] Langevin, P.: Six-variable Boolean functions modulo quadratics: 205 representatives. https://github.com/drmichko/radii/blob/main/class-3-6.txt Accessed 2026-10-18

[13] Brier, E., Langevin, P.: Classification of Boolean cubic forms of nine variables. In: Proceedings of the 2003 IEEE Information Theory Workshop (ITW 2003), pp.

179–182. IEEE, Paris, France (2003). https://doi.org/10.1109/ITW.2003.1216724