The Covering Radius of RM(1, 9) is Precisely 242

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 RM(r, n) be the rth order Reed-Muller code of length 2^n, and let $\rho(r, n)$ denote its covering radius, so that $\rho(1, n)$ is the largest possible nonlinearity of a Boolean function in n variables. For odd n, the value of $\rho(1, n)$ was previously known only for $n \leq 7$. It is known that $242 \leq \rho(1, 9) \leq 244$, but the exact determination of $\rho(1, 9)$ has been a long-standing open question. We give a computer-assisted proof that $\rho(1, 9) = 242$. We first show that a function of nonlinearity 243 would yield one of nonlinearity 244, so it suffices to exclude 244. Divisibility properties of the Walsh spectrum then attach to any function of nonlinearity 244 a cubic p whose spectrum attains the sharp bound $\sum_a |W_p(a)| \leq 10240$, and the cases of equality take one of two forms. One form is eliminated directly. The other is eliminated by an exhaustive computation that leverages the classification of the 349 orbits in $\mathbf{RM}(3, 9)/\mathbf{RM}(2, 9)$ under $\mathbf{GL}(9, 2)$, using Langevin's catalog of representatives together with an audit of its completeness, and the enumeration is carried out twice with independent implementations. The notebook to verify the computer search portion, `Verify_RM(1,9).ipynb`, contains all data and recomputes each check, and may be found in the repository https://github.com/FreemanSlaughter/Covering-Radius.

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

MSC Classification: 94B05 , 94B65 , 06E30 , 94D10 , 94A60

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 $\deg(f) = \max\{|I| \mid a_I \neq 0\}$. 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 $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n \mid f(x) = 1\}|$. For $-1 \leq r \leq n$, the rth order *Reed-Muller code* of length 2^n is

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

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$, its *nonlinearity* is defined to be

$$\mathrm{NL}(f) = d(f, \mathrm{RM}(1, n)),$$

where $d(\cdot\,, \cdot)$ is the Hamming distance. Nonlinearity is a measure of immunity of cryptographic functions against linear attacks and fast correlation attacks [1, Section 4.1.2]. The *covering radius* of the first order Reed-Muller code $\mathrm{RM}(1, n)$, denoted by $\rho(1, n)$, is the largest possible nonlinearity of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, that is,

$$\rho(1, n) = \max_{f : \mathbb{F}_2^n \to \mathbb{F}_2} d(f, \mathrm{RM}(1, n)).$$

The study of the covering radius $\rho(1, n)$ has a long history. In 1978, Helleseth, Kløve and Mykkeltveit [2] proved that for even n,

$$\rho(1, n) = 2^{n-1} - 2^{n/2-1},$$

and for odd n,

$$2^{n-1} - 2^{(n-1)/2} \leq \rho(1, n) \leq 2^{n-1} - 2^{n/2-1}. \tag{1}$$

It is quite easy to determine that $\rho(1, 5) = 12$. In 1980, Mykkeltveit [3] proved that $\rho(1, 7) = 56$; a simpler proof of this result was later given in [4]. The value of $\rho(1, 9)$ is then the first open question. The bounds in (1) give $242 \leq \rho(1, 9) \leq 244$. It was shown in [5] that the covering radius of $\mathrm{RM}(1, 9)$ in $\mathrm{RM}(4, 9)$ is 240, that is, $\max_{f \in \mathrm{RM}(4,9)} d(f, \mathrm{RM}(1, 9)) = 240$. Two breakthroughs came in 2007 and 2010: Kavut, Maitra and Yücel [6] showed that $\rho(1, 9) \geq 241$, and Kavut and Yücel [7] improved the result to $\rho(1, 9) \geq 242$. Explicit functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with nonlinearities 241 and 242 have been found using rotational symmetry. The gap $242 \leq \rho(1, 9) \leq 244$ has remained open since then, and this was considered one of the most difficult questions about the covering radii of Reed-Muller codes.

In the present paper, with AI assistance, we adopt a new approach which enables us to determine that $\rho(1, 9) = 242$ precisely. The essence of our method is to reduce the problem of dealing with all functions $f : \mathbb{F}_2^9 \to \mathbb{F}_2$ to considering those of algebraic degree 3. Our proof can be outlined as follows: First, we show that the existence of

a function $f : \mathbb{F}_2^9 \to \mathbb{F}_2$ with nonlinearity 243 would imply the existence of another function with nonlinearity 244. If a hypothetical function with nonlinearity 244 exists, then it must satisfy stringent conditions divided into two cases. One of the two cases is directly eliminated; the other case is computationally shown to be impossible using the known classification of $\mathrm{RM}(3,9)/\mathrm{RM}(2,9)$ [8, 9].

While this paper was being prepared for submission, Wang, Lou, and Wang posted a preprint [10] which also asserts that $\rho(1,9) = 242$, using an approach closely related to ours. The two works were carried out independently. A complete draft of the present paper, together with the verification notebook and all of its data, was made publicly available in the repository https://github.com/FreemanSlaughter/Covering-Radius on October 11, 2026, two days before the preprint [10] was posted on arXiv on October 13, 2026.

2 Preliminaries

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$, put $s_f(x) = (-1)^{f(x)}$ and

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} s_f(x)(-1)^{a \cdot x}.$$

The character matrix H_n is symmetric and satisfies $H_n^2 = 2^n I$. Consequently

$$\mathrm{NL}(f) = 2^{n-1} - \tfrac{1}{2}\left\|W_f\right\|_\infty, \quad \sum_a W_f(a)^2 = 2^{2n}, \quad \sum_a W_f(a) = 2^n s_f(0). \tag{2}$$

The first identity follows from $d(f, a \cdot x + b) = 2^{n-1} - (-1)^b W_f(a)/2$. Thus $\rho(1,n) = \max_f \mathrm{NL}(f)$. At $n = 9$, Parseval and the evenness of Walsh coefficients give $\left\|W_f\right\|_\infty \geq 24$, so $\rho(1,9) \leq 244$. We will also use

$$\sum_x s_f(x) W_p(x) = \sum_a s_p(a) W_f(a), \tag{3}$$

which is just the symmetry of H_n. All polynomial degrees refer to algebraic normal form over $\mathbb{F}_2$. A "cubic" below has degree at most three. Finally, we use $\mathbb{1}_X$ to denote the indicator function of the set X.

Lemma 1 *If $W_f(a) \equiv c \pmod{2^k}$ for all a, where $1 \leq k < n$, then $(W_f - c)/2^k \pmod 2$ has degree at most $k - 1$.*

Proof Regard the bits of a as integer variables. The coefficient of a^S in the integer multilinear representation of W_f is

$$(-2)^{|S|} \sum_{\substack{x_i = 1 \\ i \in S}} s_f(x). \tag{4}$$

When $|S| = k < n$, the inner sum has an even number of odd summands, so this coefficient is divisible by 2^{k+1}. The same divisibility is immediate for $|S| > k$. Since $W_f - c$ is pointwise divisible by 2^k, integer Möbius inversion shows that all its multilinear coefficients are divisible by 2^k. After division and reduction modulo two, every term of degree at least k vanishes. □

Lemma 2 *A nonzero Boolean polynomial of degree at most $d \leq n$ has weight at least 2^{n-d}.*

Proof Choose a monomial of maximum degree $m \leq d$. After any assignment of the other $n - m$ variables, its coefficient is still one: no monomial properly containing it occurs. Each of the 2^{n-m} disjoint restrictions is therefore nonzero somewhere. □

Lemma 3 *For a cubic on m variables, every Walsh coefficient is divisible by $2^{\lceil m/3 \rceil}$. In particular, for a cubic p on nine variables,*

$$W_p(a) \equiv c + 16\ell(a) \pmod{32} \tag{5}$$

for some multiple c of eight and some linear Boolean function ℓ.

Proof Include the character in the polynomial and expand its phase as a product of factors $1 - 2x^S$, one for each nonconstant monomial. A term selecting j monomials whose union has size u contributes, after summation, a multiple of 2^{j+m-u}. Since $u \leq \min(m, 3j)$, this exponent is at least $\lceil m/3 \rceil$. A constant term only changes the overall sign.

Applying this divisibility to the restrictions in (4), the coefficient indexed by S for a nine-variable cubic is divisible by $2^{|S|+\lceil (9-|S|)/3 \rceil}$. Linear coefficients are therefore multiples of 16, and coefficients of degree at least two are multiples of 32. This gives (5). □

Lemma 4 *Let q be quadratic on m variables. Its alternating bilinear form is $B_q(u, v) = q(u + v) + q(u) + q(v) + q(0)$. If $r = \operatorname{rank}(B_q)$, then r is even, and its Walsh spectrum has 2^r nonzero coefficients, all of magnitude $2^{m-r/2}$. Hence*

$$\sum_a |W_q(a)| = 2^{m+r/2}.$$

If $\operatorname{wt}(q) = 2^{m-2}$, its support is an affine flat of codimension two.

Proof Pairing off nonzero entries of the alternating form gives coordinates in which $q = x_1x_2 + \cdots + x_{r-1}x_r + \lambda + \varepsilon$, with λ linear. Each paired character sum has magnitude two. Each unpaired coordinate contributes either zero or two, and is nonzero for exactly one choice of its frequency. This proves our claims regarding the spectrum. If $\operatorname{wt}(q) = 2^{m-2}$, then $W_q(0) = 2^{m-1}$, forcing $r = 2$. There is no nonzero linear term on the radical, and translations in the paired coordinates put q in the form x_1x_2 or $x_1x_2 + 1$. The specified weight selects the former. Its support is the intersection of two independent affine hyperplanes. □

3 Two Bounds on Cubic Spectra

For a cubic p on $\mathbb{F}_2^9$, define

$$L(p) = \sum_a |W_p(a)|, \quad C(p) = 3W_p(0) + \sum_{a \neq 0} |W_p(a)|.$$

Proposition 5 *Every such cubic satisfies* $L(p) \leq 10240$ *and* $C(p) \leq 10368$.

Proof The following elementary inequality will be used throughout, where we use w_a to denote $W_p(a)$. If $P_a(w_a) \geq |w_a|$, then

$$3w_0 + \sum_{a \neq 0} |w_a| \leq \sum_a P_a(w_a) + 3w_0 - P_0(w_0). \tag{6}$$

Indeed, the difference between the right side and the left side is $\sum_{a \neq 0} (P_a(w_a) - |w_a|) \geq 0$.

First suppose the common residue modulo 16 is eight. Write $\ell(a) = a \cdot u$ in (5) and replace $p(x)$ by $p(x+u)$. This multiplies $W_p(a)$ by $(-1)^{\ell(a)}$ and makes its residue constant modulo 32, since $-(c+16) \equiv c \pmod{32}$ for $c \equiv 8$ or 24. Neither $L(p)$ nor $W_p(0)$ changes. On the resulting lattice use

$w \bmod 32$	$P(w) \geq \lvert w \rvert$	$\max(3w - P(w))$
8	$3w^2/128 - w/8 + 15/2$	96
24	$3w^2/128 + w/8 + 15/2$	80

The maxima are over the indicated integer lattices. For the first row, $P(w) - w = 3(w-8)(w-40)/128$ when $w \geq 0$, and $P(w) + w = (w+24)(3w+40)/128$ when $w < 0$. Both are nonnegative on that lattice. Reflection proves the second row. The two concave correction quadratics attain their lattice maxima at 72 and 56, respectively. By (2),

$$\sum_a P(W_p(a)) = 9984 \mp \tfrac{1}{8} \sum_a W_p(a) \leq 10048.$$

Thus (6) gives

$$L(p) \leq 10048 < 10240, \quad C(p) \leq 10048 + 96 = 10144. \tag{7}$$

Otherwise all coefficients are divisible by 16. Set $t(a) = W_p(a)/16$ and $\epsilon(a) = t(a) \pmod 2$. Then ϵ is affine by (5), and $\sum_a t(a)^2 = 1024$. The following bounds are immediate for even and odd integers:

ϵ	$Q_a(t) \geq \lvert t \rvert$	$\sum_a Q_a(t(a))$	$3t(0) - Q_0(t(0))$ is at most
0	$t^2/2$	512	4
1	$(t^2+3)/4$	640	8
nonconstant	$(t^2+\epsilon(a))/2$	640	4

In the last row $\mathrm{wt}(\epsilon) = 256$. Multiplying the last two columns' sum by 16 in (6) bounds $C(p)$ by 8256, 10368, and 10304, respectively. The bounds on $L(p)$ are 8192, 10240, and 10240. □

4 Reduction to Two Cubic Spectra

Proposition 6 *The existence of a nine-variable function of nonlinearity* 243 *would imply the existence of one of nonlinearity* 244.

Proof Suppose $\mathrm{NL}(f) = 243$, so $\|W_f\|_\infty = 26$. For $n \geq 2$ all Walsh coefficients are congruent to $-2\,\mathrm{wt}(f)$ modulo four. Thus f has odd weight. Let $v = \bigoplus_{x:f(x)=1} x$. Comparing the character sums gives

$$W_f(a) \equiv W_f(0) + 4(a \cdot v) \pmod 8.$$

Translation by v makes this residue constant: for odd-weight spectra $c \equiv 2$ or $6 \pmod 8$, and $-(c+4) \equiv c \pmod 8$. Taking the complement if necessary then gives $W_f \equiv 2 \pmod 8$. These operations preserve nonlinearity.

Put $s = s_f(0)$ and $z = (W_f - 2)/8$. Then $-3 \leq z \leq 3$, and

$$\sum_a z(a) = 64s - 128, \quad \sum_a z(a)^2 = 4128 - 32s. \tag{8}$$

By Lemma 1, $q = z \pmod 2$ is quadratic. If $q \neq 1$, Lemma 2 applied to $q+1$ gives $\mathrm{wt}(q) \leq 384$. Since $z^2 \leq 4 + 5q$, this would imply $\sum_a z^2 \leq 4 \cdot 512 + 5 \cdot 384 = 3968$, contrary to (8). Therefore it must be that $z \in \{-3, -1, 1, 3\}$ and

$$W_f \in \{-22, -6, 10, 26\}.$$

If $s = 1$, changing $f(0)$ from zero to one subtracts two from every Walsh coefficient. The new spectrum lies in $\{-24, -8, 8, 24\}$, so the new function has nonlinearity 244 by Parseval.

If $s = -1$, then $\sum_a z^2 = 4160$, so exactly 56 values have magnitude one. Lemma 1 makes $p = (W_f - 10)/16 \pmod 2$ cubic. The product $s_p z$ is one at those 56 positions and minus three elsewhere. Equation (3) gives

$$\sum_x s_f(x) W_p(x) = \sum_a s_p(a) W_f(a) = 2W_p(0) - 10496.$$

Since $s_f(0) = -1$, it follows that

$$3W_p(0) - 10496 = \sum_{x \neq 0} s_f(x) W_p(x) \geq -\sum_{x \neq 0} |W_p(x)|.$$

Thus $10496 \leq C(p) \leq 10368$, a contradiction. □

Proposition 7 *Suppose* $\|W_f\|_\infty \leq 24$ *for a nine-variable Boolean function* f. *Then* $W_f \in \{-24, -8, 8, 24\}$, *with* 448 *coefficients of magnitude* 24 *and* 64 *of magnitude eight. There is a cubic* p *with*

$$L(p) = 10240, \quad s_f(x) = -\operatorname{sgn} W_p(x) \quad \text{when } W_p(x) \neq 0, \tag{9}$$

and its spectrum has one of the following forms:

I. *Every coefficient belongs to* $\{-48, -16, 16, 48\}$. *There are* 64 *coefficients of magnitude* 48 *and* 448 *of magnitude* 16.

II. *The parity of* $W_p/16$ *is nonconstant affine. Its* 256 *odd positions have values* ± 16. *The other positions contain* 192 *values* ± 32 *and* 64 *zeros.*

Proof Odd weight would force every magnitude to be at most 22, contradicting Parseval. Hence $4 \mid W_f$, and $W_f/4 \pmod 2$ is affine by Lemma 1. If constantly one, all magnitudes are at most 20. If nonconstant, the energy is at most $256(20^2+24^2) = 249856 < 262144$. Therefore it is zero, and $8 \mid W_f$. Now $W_f/8 \pmod 2$ is quadratic. Unless constantly one, at least 128 positions are divisible by 16, so the energy is at most $128 \cdot 16^2 + 384 \cdot 24^2 = 253952 < 262144$. Thus $W_f \in \{-24, -8, 8, 24\}$, and Parseval gives the stated counts.

Set $p = (W_f - 8)/16 \pmod 2$, which is cubic by Lemma 1. The product $s_p W_f$ equals -24 on the 448 large coefficients and eight on the others. Hence

$$-10240 = \sum_x s_f(x) W_p(x) \geq -L(p) \geq -10240.$$

Equality throughout proves (9). The strict bound (7) excludes residue eight modulo 16, and the constant-even case in Proposition 5 is also strict. In the constant-odd case, equality in $|t| \leq (t^2+3)/4$ forces $|t| \in \{1, 3\}$, giving I. In the nonconstant case, equality in $|t| \leq (t^2+\epsilon)/2$ forces $t = \pm 1$ at odd positions and $t \in \{0, \pm 2\}$ at even positions, giving II. In each case $\sum t^2 = 1024$ supplies the counts. □

5 Two Exclusions

We may change coordinates in p and add affine terms without changing the nonlinearity of its associated sign function. More explicitly, if $p'(x) = p(Mx + u) + b \cdot x + \varepsilon$, with M invertible, then

$$W_{p'}(a) = (-1)^{\varepsilon + (M^{-T}(a+b)) \cdot u} W_p(M^{-T}(a+b)). \tag{10}$$

Thus the associated f is changed by an affine input map and an affine output term. The same statement applies to (9) when zeros are present, by transforming the whole function f.

Lemma 8 *Case II of Proposition 7 is impossible.*

Proof By a linear change of variables and addition of a linear term to p, put the odd frequency sector at $\alpha = 1$. Write $p(t, y) = p_0(y) + tq(y)$, where $y \in \mathbb{F}_2^8$ and q is quadratic. Then

$$W_p(1, b) = 2H_8(s_{p_0} \mathbb{1}_{\{q=1\}})(b), \quad |W_p(1, b)| = 16.$$

Parseval gives $\mathrm{wt}(q) = 64$. Lemma 4 therefore makes $\mathrm{supp}(q) = y_0 + U$, with $\dim(U) = 6$. Choose an injective linear map $B : \mathbb{F}_2^6 \to \mathbb{F}_2^8$ with image U, and set $g(z) = p_0(y_0 + Bz)$. The displayed formula becomes

$$W_p(1, b) = 2(-1)^{b \cdot y_0} W_g(B^T b).$$

Since B^T is onto, all coefficients of W_g have magnitude eight. Write $W_g = 8s_{g^*}$. From $H_6^2 = 64I$ we obtain $H_6 s_{g^*} = 8s_g$, so g^* is bent as well.

The sign of $W_p(1, b)$ is therefore $(-1)^{b \cdot y_0} s_{g^*}(B^T b)$. A six-variable function lifted along a surjective map from eight variables has its nonzero Walsh coefficients multiplied by four. Indeed, summing over each fiber gives zero unless the character annihilates the two-dimensional kernel, and gives four otherwise. Consequently this sign function has Walsh maximum $4 \cdot 8 = 32$. By (9), so does the restriction $f(1, \cdot)$. But

$$W_{f(1,\cdot)}(b) = \frac{W_f(0, b) - W_f(1, b)}{2},$$

whose magnitude is at most 24. This is a contradiction. □

Write $D_u h(x) = h(x+u) + h(x)$. For a homogeneous cubic c, define

$$D(c) = \{(D_u c)_2 \mid u \in \mathbb{F}_2^9\},$$

where the subscript denotes the homogeneous quadratic part. This part is $\sum_i u_i (D_{e_i} c)_2$, so the map is linear. Call c nondegenerate when $\dim(D(c)) = 9$.

Lemma 9 *The cubic part of a polynomial arising in Case I of Proposition 7 is nondegenerate.*

Proof Otherwise $D_u p$ is affine for some $u \neq 0$. If this derivative is constant, half the Walsh coefficients of p vanish, contrary to I. If nonconstant, it is invariant under translation by u. Affine coordinates therefore put it at the coordinate y, with u in the t direction, and give

$$p(t, y, z) = ty + r(y, z), \quad z \in \mathbb{F}_2^7.$$

Summing first over t yields

$$W_p(\alpha, \beta, \gamma) = 2(-1)^{\alpha\beta} W_{r(\alpha,\cdot)}(\gamma).$$

These coefficients are nonzero. Let s_{h_α} be the sign of $W_{r(\alpha,\cdot)}$. Equation (9) then gives

$$s_f(\alpha, \beta, \gamma) = -(-1)^{\alpha\beta} s_{h_\alpha}(\gamma), \quad W_f(a, b, d) = -2(-1)^{ab} W_{h_b}(d).$$

Both seven-variable functions h_b would consequently have Walsh maximum at most 12.

To exclude this, suppose $\|W_h\|_\infty \leq 12$ on seven variables. Odd weight would bound all magnitudes by ten, violating Parseval. Thus $4 \mid W_h$ and $W_h/4 \pmod 2$ is affine. Constant zero would bound all magnitudes by eight. Nonconstant parity would give energy at most $64(12^2 + 8^2) = 13312 < 16384$. The parity is therefore constantly one. Parseval forces 112 values of magnitude 12 and 16 of magnitude four. Now $k = (W_h - 4)/8 \pmod 2$ is quadratic by Lemma 1, and

$$\sum_x s_h(x) W_k(x) = \sum_a s_k(a) W_h(a) = -112 \cdot 12 + 16 \cdot 4 = -1280.$$

Lemma 4 bounds $\sum |W_k|$ by $2^{7+6/2} = 1024$, a contradiction. □

6 Computation

6.1 Quadratic Portions to Enumerate

The orbit count in the literature is, by [8, 9],

$$\#\big((\mathrm{RM}(3,9)/\,\mathrm{RM}(2,9))/\,\mathrm{GL}(9,2)\big) = 349. \tag{11}$$

We use the 349 polynomials recorded in Langevin's catalog [9]. The audit below verifies that they are pairwise inequivalent, so (11) makes the list complete. After a linear change of coordinates, any cubic is $c + q + \lambda$, with c from this list, q homogeneous quadratic, and λ affine. By (10), it suffices to consider $p = c + q$. There are $\binom{9}{2} = 36$ coefficients in q.

Lemma 10 *The common residue of W_{c+q} modulo 16 depends only on c. If it is zero, the map*

$$\Phi_c(q)_i = \frac{W_{c+q}(e_i) - W_{c+q}(0)}{16} \pmod 2, \quad i = 1, \ldots, 9, \tag{12}$$

is affine in the 36 coefficients of q. Its vanishing means that W_{c+q} is constant modulo 32. If the system is consistent, write its solution space as $q_0 + K_c$. Then $D(c) \subseteq K_c$. One representative of each coset modulo $D(c)$ suffices for Case I.

Proof In the nine-variable phase expansion from Lemma 3, a term can survive modulo 16 only when $j + 9 - u \leq 3$. Since $u \leq \min(9, 3j)$, this forces $j = 3$ and $u = 9$. Thus only three disjoint cubic monomials can contribute. Quadratic and frequency-linear monomials do not affect the residue.

For (12), use

$$W_{c+q}(e_i) - W_{c+q}(0) = -2 \sum_{x_i=1} (-1)^{c(x)+q(x)}.$$

Compute the eight-variable sum modulo 16. The same expansion can retain only $j = 3$, $u = 8$. The possible degree triples are $(3, 3, 3)$ and $(3, 3, 2)$, so a surviving term involves at most one quadratic coefficient. Cubic coefficients are fixed, and quadratic coefficients in the restriction are affine in q. A possible constant sign makes no difference modulo 16, since the retained terms are multiples of eight. Dividing the displayed difference by 16 and reducing modulo two proves affinity. Equation (5) shows that Φ_c records the linear part of the affine function $W_{c+q}/16 \pmod 2$. This proves the vanishing criterion.

Translation by u changes the quadratic part of $c+q$ by $(D_u c)_2$, with the remaining change affine. In a spectrum divisible by 16, multiplication by a sign has no effect modulo 32. An affine term added to the polynomial shifts its frequency argument and possibly negates its spectrum. These operations leave the linear part of $W_{c+q}/16 \pmod 2$ unchanged. Thus $D(c)$ lies in the homogeneous kernel K_c. Equation (10) also shows that each such coset has a fixed spectral magnitude multiset and fixed sign-function nonlinearity. Choosing a complement to $D(c)$ in K_c is sufficient. □

The code obtains the affine map by evaluating it at zero and the 36 quadratic monomials. It solves the equations by Gaussian elimination, then extends a basis of $D(c)$ to a basis of K_c. The 124 residue-eight forms are excluded by (7). Of the other 225, exactly 32 are degenerate and are excluded by Lemma 9. All 193 remaining systems are consistent. For the complements B_c, the computed dimensions are

$\dim(B_c)$	18	19	20	21	22	24	27
number of classes	142	20	18	6	5	1	1

Hence $\sum_c 2^{\dim(B_c)} = 251133952$.

6.2 Completeness

The audit uses contraction and restriction invariants as in [8]. Let $T(u, v, w) = D_u D_v D_w c(0)$ be the alternating trilinear form of c. The correspondence between cubic parts and such forms is $\mathrm{GL}(9, 2)$-equivariant: $T(e_i, e_j, e_k)$ is the coefficient of $x_i x_j x_k$. Put $r(u) = \mathrm{rank}(T(u, \cdot, \cdot))$ and $\psi_j(u) = \mathbb{1}_{\{r(u)=2j\}}$ for $0 \leq j \leq 4$. Here a hat denotes

the unnormalized Fourier transform of an integer-valued function, with the natural pairing between a vector space and its dual.

For $H = a^{\perp}$, $a \neq 0$, let $r_H(u)$ be the contraction rank for $T|_H$, and $\chi_{H,j}(u) = \mathbb{1}_{\{r_H(u)=2j\}}$, $0 \le j \le 3$. These are all possible ranks: each nonzero $u \in H$ belongs to the radical of its contraction, and $\dim(H) = 8$. Define the multiset

$$\Gamma(H) = \big\{(\widehat{\chi}_{H,0}(b), \dots, \widehat{\chi}_{H,3}(b)) \mid b \in H^*\big\}.$$

An isomorphism of H merely permutes its dual, so $\Gamma(H)$ is basis-independent. Assign common labels to the distinct exact multisets occurring anywhere in the catalog. There are 32 of them. For each label j, let $\phi_j(a)$ indicate that label at $a \neq 0$, and set $\phi_j(0) = 0$. The audit compares the following two multisets jointly:

$$\big\{(\Gamma(a^{\perp}), \widehat{\psi}_0(a), \dots, \widehat{\psi}_4(a)) \mid a \neq 0\big\},$$
$$\big\{(r(u), \widehat{\phi}_0(u), \dots, \widehat{\phi}_{31}(u)) \mid u \in \mathbb{F}_2^9\big\}.$$

They are invariants. Under $T'(u,v,w) = T(Mu, Mv, Mw)$, one has $r'(u) = r(Mu)$ and $\widehat{\psi}'_j(a) = \widehat{\psi}_j(M^{-T}a)$. Also $\Gamma'(a^{\perp}) = \Gamma((M^{-T}a)^{\perp})$, so $\widehat{\phi}'_j(u) = \widehat{\phi}_j(Mu)$. Each displayed multiset is therefore only permuted.

For efficiency the code uses, for $u \in a^{\perp}$,

$$r_{a^{\perp}}(u) = \begin{cases} r(u) - 2, & a \in \operatorname{im} T(u,\cdot,\cdot), \\ r(u), & a \notin \operatorname{im} T(u,\cdot,\cdot). \end{cases}$$

To justify this, let R be the radical of the contraction. If $a \in \operatorname{im} T(u,\cdot,\cdot) = R^{\perp}$, then $a^{\perp}$ contains R and descends to a hyperplane in the symplectic quotient, reducing rank by two. Otherwise $a^{\perp}$ maps onto that quotient and retains its rank.

The code sorts and compares full integer tuples, preserving multiplicities, and obtains 349 distinct pairs. Combined with (11), this proves that each orbit is represented. The checksum checks the transcription only.

6.3 Exhaustive Check

For every $q \in q_0 + B_c$, the code computes W_{c+q}. It first checks $W_{c+q}(0) \equiv 16 \pmod{32}$, then retains precisely those spectra in $\{-48, -16, 16, 48\}^{512}$. For each retained spectrum it forms $s_f = -\operatorname{sgn} W_{c+q}$ and computes $H_9 s_f$. The completed computation gives

$$\begin{aligned} \text{quadratic representatives tested} &= 251133952, \\ \text{spectra retained} &= 90126659, \\ \max(\mathrm{NL}(f)) \text{ among retained spectra} &= 240. \end{aligned} \tag{13}$$

To prepare, we perform two independent enumerations: row elimination with full Walsh transforms, and reverse column elimination with direct character sums at $\{0, e_1, \dots, e_9\}$. They choose different offsets and complementary bases. The first enumeration stores phases in signed 16-bit arrays and uses ascending Walsh stages. The

second stores truth bits, uses 32-bit arrays and descending stages, and checks every transformed coefficient's residue. Their tested counts, retained counts, and maximum nonlinearities agree separately for all 193 classes. Every transform intermediate has magnitude at most 512, so these integer types suffice. The code also compares both transforms with direct character sums on fixed test tables.

Each complement is traversed in binary reflected Gray order $g(i) = i \,\texttt{xor}\, \lfloor i/2 \rfloor$. This is a bijection on the coefficient vectors. Between consecutive indices, only the bit at the least significant one of i changes. Parallel chunks begin at their exact Gray vector and partition the full interval $0 \le i < 2^{\dim(B_c)}$ without omissions. Thus (13) is an exhaustive integer computation. In view of Lemma 10, it excludes Case I of Proposition 7.

7 Reproduction

Kavut and Yücel [7] give the following truth table in hexadecimal [7, Section 3.1]:

```
68B7EF2DA03B0D3EA00DB6A96DD99AEAFDB9C842B6D5DC8C4526CE0DD29020DB
B75FE3314568344E73688FF0CB2482E065231869E1AA4583765CC491F8A8DB12
```

Concatenate the lines, expand each digit most significant bit first, and index the resulting bits by the integers $\{0, \ldots, 511\}$. All 512 direct character sums are checked by the notebook, giving Walsh maximum 28 and hence nonlinearity 242.

Theorem 11 $\rho(1, 9) = 242$.

Proof Equation (2) gives the upper bound 244. If nonlinearity 244 were attained, Proposition 7 would produce Case I or II. Lemma 8 excludes II. Lemma 9, Lemma 10, the catalog audit and the computation (13) exclude I. Proposition 6 then excludes 243. The witness from Kavut and Yücel attains 242. □

Run the accompanying file `Verify_RM(1,9).ipynb`, which can be found at https://github.com/FreemanSlaughter/Covering-Radius, in a Jupyter Notebook such as Google Colab to verify. This code includes the catalog of `classification.txt` from [9], and needs no additional inputs or network access. It performs both full enumerations, compares every class, and generates `rm19_verification.json`. This file is included in the repository above.

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 notebook `Verify_RM(1,9).ipynb`, which contains all data used in the computation and recomputes each check, and its output `rm19_verification.json` are available in the repository https://github.com/FreemanSlaughter/Covering-Radius.

Use of artificial intelligence. We acknowledge that discussions with AI were helpful in formulating and refining some of these proofs, as well as with editing and typesetting the document. Nonetheless, we the authors take full responsibility for the accuracy of the results contained in this manuscript, and assert that it reflects our original work.

References

[1] Carlet, C.: Boolean functions for cryptography and error-correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010). https://doi.org/10.1017/CBO9780511780448.011

[2] Helleseth, T., Kløve, T., Mykkeltveit, J.: On the covering radius of binary codes. IEEE Trans. Inform. Theory **24**, 627–628 (1978) https://doi.org/10.1109/TIT.1978.1055928

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

[4] Hou, X.-D.: Covering radius of the Reed-Muller code $R(1, 7)$ — a simpler proof. J. Combin. Theory, Ser. A **74**, 337–341 (1996) https://doi.org/10.1006/jcta.1996.0055

[5] Hou, X.-D.: The covering radius of $R(1, 9)$ in $R(4, 9)$. Des. Codes Cryptogr. **8**, 285–292 (1996) https://doi.org/10.1023/A:1027399606196

[6] Kavut, S., Maitra, S., Yücel, M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. Inform. Theory **53**, 1743–1751 (2007) https://doi.org/10.1109/TIT.2007.894696

[7] Kavut, S., Yücel, M.D.: 9-Variable Boolean Functions with Nonlinearity 242 in the Generalized Rotation Symmetric Class. Information and Computation **208**(4), 341–350 (2010) https://doi.org/10.1016/j.ic.2009.12.002

[8] Brier, E., Langevin, P.: Classification of Boolean Cubic Forms of Nine Variables. In: Proceedings 2003 IEEE Information Theory Workshop (Cat. No.03EX674), pp. 179–182 (2003). https://doi.org/10.1109/ITW.2003.1216724

[9] Langevin, P.: Cubics in Nine Variables. https://langevin.univ-tln.fr/project/cubics. Accessed: 2026-10-11 (2026)

[10] Wang, Q., Lou, Y., Wang, Z.: The Covering Radius of the Reed–Muller Code RM(1,9) is 242. https://arxiv.org/abs/2610.17871 (2026)