МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

VERIFYING THE COMPUTED WEIGHT DISTRIBUTION FOR THE BINARY REED–MULLER CODE R(4,9) [1]

Yuri Borissov and Miroslav Markov

Abstract

We revisit pivotal aspects of computing the weight distribution of the binary Reed–Muller code $R(4,9)$ and introduce a verification technique based on the Heninger–Rains–Sloane integrality congruences for Reed–Muller codes. The consistency checks fully confirm the correctness of the distribution obtained in our previous work: *"The weight distribution of the fourth-order Reed–Muller code of length 512"*, *Designs, Codes and Cryptography* **93**, 2487–2502 (2025).

2020 Mathematics Subject Classification: 94B70, 94B05, 68Q25.

Key words: binary Reed–Muller code, weight distribution, affine equivalence.

1 Introduction. Binary Reed–Muller codes are classical linear codes that admit efficient majority-logic decoding. However, general results on their weight structure are scarce: complete distributions are known for first- and second-order codes [15] and their duals (via the MacWilliams identities), and for arbitrary order for weights below $2d_{\min}$ [7].

The code $R(4,9)$ was historically among the smallest with unknown distribution [11]; recent work [2] determines its spectrum, renewing interest in this code, while the exact distribution requires substantial computation. In [12], we resolved this problem by applying the methodology described in D. V. Sarwate's Ph.D. thesis from 1973 [14], using newer results on the affine-equivalence classification of Boolean functions [10, 5]. Since the solution is computer-assisted, it is essential to employ rigorous verification procedures to confirm the correctness of the computed results. Here, we present a verification technique for those computations derived from specific theorems concerning the weight distribution of arbitrary Reed–Muller codes modulo certain powers of 2 [6].

We also briefly assess the goodness-of-fit of the Cusick–Cheon conjectured bounds [4] for estimating the number of balanced Boolean functions, by comparing them with the exact count of weight 256 codewords in $R(4,9)$ reported in [12].

The paper is organized as follows. In Section 2, we recall necessary background. Section 3 revisits key steps in the computation of the weight distribution of $R(4,9)$. Section 4 explains our verification technique. We conclude in Section 5.

[1] The research of the first author was partially supported by the Center of Excellence in Informatics and ICT established under the Grant No BG16RFPR002-1.014-0018, financed by the Research, Innovation and Digitalization for Smart Transformation Programme and co-financed by the European Union. The research of the second author has been partially supported by the the National Science Fund of Bulgaria under Grant KP-06-N82/5.

https://doi.org/10.55630/mem.2026.55.340-349

2 Preliminaries. For basic definitions and notations, we refer to [11]. To fix terminology, we recall the following standard notions.

Definition 2.1 (Weight distribution)**.** *Let C be a binary linear code of length n. Its weight distribution is the vector $\mathrm{W}(C) = (A_0, \ldots, A_n)$, where A_i is the number of codewords of Hamming weight i.*

Definition 2.2 (Weight enumerator)**.** *The single-variable weight enumerator of C is the polynomial in one indeterminate z*

$$\mathrm{W}[z; C] = \sum_{i=0}^{n} A_i z^i.$$

Definition 2.3 (Two-variable weight enumerator)**.** *For $\mathrm{W}(C) = (A_0, \ldots, A_n)$, the two-variable weight enumerator is*

$$\mathrm{W}_C(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i}.$$

Let $\mathcal{B}_m$ denote the set of Boolean functions in m variables; each $f \in \mathcal{B}_m$ corresponds to a binary vector of length $n = 2^m$ via its truth table.

Definition 2.4 (Reed–Muller codes)**.** *For $0 \le r \le m$, the r-th order binary Reed–Muller code $R(r, m)$ comprises those vectors of length $n = 2^m$ whose associated Boolean functions have algebraic degree at most r.*

We also use the general affine group $\mathrm{GA}(m, 2)$ acting on $\mathbb{F}_2^m$, where m is a positive integer and $\mathbb{F}_2 = \{0, 1\}$. In fact, $\mathrm{GA}(m, 2)$ is the group of automorphisms of $R(r, m)$ for $0 < r < m - 1$ [11, Ch. 13.9].

Affine equivalence. For $A \in \mathrm{GA}(m, 2)$ and $f \in \mathcal{B}_m$, let $(f \circ A)(x) = f(A(x))$. Cosets $C_1 = f_1 + R(r, m)$ and $C_2 = f_2 + R(r, m)$ are *affine equivalent* if $f_2 = f_1 \circ A$.

We list three standard facts used in this paper.

Fact 2.5. *The code $R(r, m)$ is a linear $[n, k, d]$ code with parameters*

$$n = 2^m, \qquad k = \sum_{i=0}^{r} \binom{m}{i}, \qquad d = 2^{m-r}.$$

In particular, the binary $R(4, 9)$ is a linear $[512, 256, 32]$ code.

Fact 2.6. *$R(s, 2s + 1)$ is doubly-even self-dual for $s \ge 1$. In particular, $R(4, 9)$ is a doubly-even self-dual code.*

And, finally the extensively used in this study.

Fact 2.7. *Affine-equivalent cosets of $R(r, m)$ have identical weight enumerators.*

3 Revisiting the computation for $R(4,9)$.

3.1 Theoretical basis. We employ two theorems stated in Chapter 5 of Sarwate's thesis [14, Thms. 5.12 and 5.13]. Let H_r^m denote the set of homogeneous polynomials (forms) in m binary variables of degree r, supplemented with the zero polynomial 0.

Theorem 3.1 ([14], Th. 5.12)**.** *For $0 \le r \le m$,*

$$\mathrm{W}\big[z; R(r+2,m+2)\big] = \sum_{p \in \mathsf{H}_{r+2}^{m+1}} \mathrm{W}^2\big[z;\, p + R(r+1,m+1)\big].$$

Theorem 3.2 ([14], Th. 5.13)**.** *If $p = e + f x_{m+1}$ with $e \in \mathsf{H}_{r+2}^m$ and $f \in \mathsf{H}_{r+1}^m$, then*

$$\mathrm{W}\big[z; C(p)\big] = \sum_{g \in \mathsf{H}_{r+1}^m} \mathrm{W}\big[z;\, e+g+R(r,m)\big] \cdot \mathrm{W}\big[z;\, e+f+g+R(r,m)\big],$$

where $C(p) = p + R(r+1, m+1)$.

In conjunction, we use the affine-equivalence classifications of two types of Boolean objects:

- quartic Boolean forms in eight variables due to Langevin and Leander [10];
- cosets of the quotient space $R(4,7)/R(2,7)$ due to Gillot and Langevin [5].

These classification results drastically reduce the computational burden: the former reduces the number of necessary weight-enumerator computations in Theorem 3.1 (implicitly) from $|\mathsf{H}_4^8| = 2^{\binom{8}{4}} = 2^{70}$ to a manageable 999 representatives; the latter simplifies the coset weight-enumerator computations in Theorem 3.2. Briefly, prior to implementing this machinery based on Fact 2.7, a substantial amount of pre-computation is required to create the orbits in $R(4,7)/R(2,7)$ and to compute the weight distributions of orbit representatives. Further work is also needed to resolve some incompatibilities between the two classifications; the interested reader is referred to [12, §3.2] for details.

3.2 Implementation. We employed HPC resources (dual Xeon Gold 5118, 48 cores; 256 GB RAM; NVIDIA V100 32 GB). Pre-computation took about 23 hours, and compressed storage plus in-RAM arrangement of orbit data required around 118 GB of memory in the worst case scenario; the generic computation took about 17 hours.

The voluminous table of the resulting distribution is presented in Table 3 of the Appendix for the sake of completeness.

4 Verification.

The correctness of the affine-equivalence classifications publicly available online [8, 9] is widely accepted in prior literature [5].

Since our methodology is computer-assisted, rigorous validation measures are indispensable to guarantee correctness and reliability of the computed results. But, before describing the verification tests employed here, we discuss the relationship between the self-duality of $R(4,9)$ and the weight distribution given in Table 3.

4.1 Self-duality. We start with the following well-known lemma whose proof is given for completeness.

Lemma 4.1. *A binary linear doubly-even code C of dimension equal to half the code length n is self-dual.*

Proof. Let $c_1, c_2 \in C$. Since C is doubly-even, the identity

$$\mathrm{wt}(c_1 + c_2) = \mathrm{wt}(c_1) + \mathrm{wt}(c_2) - 2\,\mathrm{wt}(c_1 * c_2)$$

reduces modulo 4 to $\mathrm{wt}(c_1 * c_2) \equiv 0 \pmod 2$. Here $c_1 * c_2$ denotes the binary vector of length n having 1s precisely where both c_1 and c_2 have 1s. Thus the inner product $c_1 \cdot c_2$ vanishes, i.e., $c_1 \perp c_2$. Hence C is self-orthogonal, and if $\dim(C) = n/2$ then C is self-dual. □

Now, we prove the following proposition.

Proposition 4.2. *Let C be a binary linear code of length 512 with the weight distribution reported in Table 3. Then C is doubly-even self-dual.*

Proof. Direct calculation gives $\sum_{i=0}^{512} A_i = 2^{256}$, implying $\dim(C) = 256$. So, the claim follows from the preceding lemma taking into account that all weights in Table 3 are divisible by 4. □

We recall a useful form of Gleason's theorem for doubly-even self-dual codes; see, e.g., [1, Th. 1, Part 2].

Theorem 4.3 (Gleason)**.** *Let C be a binary self-dual code of length n in which every weight is divisible by 4. Then n is divisible by 8, and the two-variable weight enumerator $\mathrm{W}_C(x, y)$ is a polynomial in*

$$f_1(x, y) = x^4 y^4 (x^4 - y^4)^4, \qquad f_2(x, y) = x^8 + 14x^4 y^4 + y^8,$$

that is,

$$\mathrm{W}_C(x, y) = \sum_{i,j} \omega_i \, f_1(x, y)^i \, f_2(x, y)^j, \qquad \text{where } n = 24i + 8j,$$

for suitable complex numbers ω_i.

In particular, for the intended distribution of $C = R(4, 9)$, we have:

Theorem 4.4 (Gleason for $R(4, 9)$)**.** *Let C be a binary linear code with weight distribution from Table 3 in the Appendix. Then there exist integers ω_i for $0 \le i \le 21$ such that*

$$\mathrm{W}_C(x, y) = \sum_{i=0}^{21} \omega_i \, f_1(x, y)^i \, f_2(x, y)^{64-3i}, \tag{1}$$

where $f_1(x, y), f_2(x, y)$ are defined above.

Table 1: Integer solutions ω_i (Gleason expansion) obtained from matching the smallest 22 weights $k \equiv 0 \pmod 4$.

i	ω_i
0	1
1	−896
2	366 400
3	−90 591 488
4	15 125 312 416
5	−1 804 090 983 680
6	158 633 285 104 000
7	−10 462 864 561 216 000
8	521 844 917 396 785 920
9	−19 703 740 374 727 094 272
10	560 488 125 281 758 654 464
11	−11 885 355 149 550 800 420 864
12	184 790 978 198 497 210 204 160
13	−2 057 511 108 351 137 030 602 752
14	15 886 111 690 015 316 194 099 200
15	−81 428 598 375 642 719 259 197 440
16	261 053 953 183 414 744 116 101 120
17	−481 398 485 705 822 986 116 792 320
18	451 352 262 788 439 851 856 297 984
19	−176 727 086 611 150 405 833 326 592
20	20 139 935 110 366 512 638 066 688
21	−279 475 807 551 445 268 430 848

Proof. For $n = 512$, Proposition 4.2 and Theorem 4.3 easily yield

$$\sum_{t=0}^{128} A_{4t}\, x^{4t} y^{512-4t} = \sum_{i=0}^{21} \omega_i\, f_1(x,y)^i\, f_2(x,y)^{64-3i}.$$

By comparing coefficients on both sides for the 22 smallest values of t we obtain a nonsingular linear (triangle) system in the unknowns ω_i, with free-coefficient vector $(A_0, A_4, \ldots, A_{84})$. Solving yields integer solutions (listed in Table 1); substituting back verifies the identity. □

Remark 4.5. *Note that one can get an equivalent form of (1) using instead of $f_1(x,y)$ the weight enumerator of the binary Golay code $g_1(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$ but then the coefficients obtained will be fractional [3].*

4.2 Heninger–Rains–Sloane tests. We use the following congruence due to Heninger–Rains–Sloane.

Theorem 4.6 ([6, Thm. 11]). *Let $W_{r,m}(z)$ denote the single-variable weight enumerator of the binary Reed–Muller code $R(r,m)$, with $0 \le r \le m$. Then*

$$W_{r,m}(z) \;\equiv\; \left(1 + z^{2^{m-r}}\right)^{2^r} \pmod{2^{r+1}}. \tag{2}$$

In particular, for $R(4,9)$ we obtain

$$W_{4,9}(z) \;\equiv\; f(z) \pmod{32}, \qquad f(z) \;:=\; \left(1 + z^{32}\right)^{16}. \tag{3}$$

This yields the following coefficient-level test:

- If k is not divisible by 32, then the coefficient A_k in the computed distribution must satisfy $A_k \equiv 0 \pmod{32}$.
- If $k = 32j$ with $0 \le j \le 16$, then $A_{32j} \equiv \binom{16}{j} \pmod{32}$.

Any valid weight distribution for $R(4,9)$ must satisfy these congruences. As seen from Table 2 in the Appendix, our computed distribution does meet them, providing a robust sanity check for its correctness.

Beyond congruence (2), Heninger, Rains and Sloane [6] prove the following recursive modulus relation (their Thm. 12):

$$W_{r,m+1}(z) \;\equiv\; W_{r,m}\!\left(z^2\right) \pmod{2^{m+1}}.$$

This yields a coefficient-level congruence between adjacent values of m for any fixed r.

Specializing to $r = 4$ and $m = 8$ gives the following strong consistency check for the weight distribution of $R(4,9)$:

$$W_{4,9}(z) \;\equiv\; W_{4,8}\!\left(z^2\right) \pmod{512}. \tag{4}$$

This can be applied whenever a reliable enumerator for $W_{4,8}(z)$ is available — for example, see the OEIS [13] entry A146976 for the $[256, 163, 16]$ Reed–Muller code.

A direct computation gives:

$$\begin{aligned} W_{4,8}\!\left(z^2\right) \pmod{512} = 1 &+ 304\,z^{32} + 256\,z^{48} + 248\,z^{64} + 256\,z^{80} + 400\,z^{96} + 28\,z^{128} \\ &+ 48\,z^{160} + 256\,z^{176} + 200\,z^{192} + 256\,z^{208} + 272\,z^{224} + 70\,z^{256} \\ &+ 272\,z^{288} + 256\,z^{304} + 200\,z^{320} + 256\,z^{336} + 48\,z^{352} + 28\,z^{384} \\ &+ 400\,z^{416} + 256\,z^{432} + 248\,z^{448} + 256\,z^{464} + 304\,z^{480} + z^{512}. \end{aligned}$$

Reducing modulo 512 the coefficients of the weight enumerator according to Table 3 yields exactly the same polynomial. This agreement confirms the congruence (4) and provides yet another strong consistency check for the computed distribution.

4.3 Cusick–Cheon approximation for balanced codewords in $R(4,9)$. Using the conjectured formulas provided in [4], we compute the lower and upper bounds for the number of codewords of weight 256 in the code $R(4,9)$. The actual computed value taken from Table 3 is positioned between the two bounds (both in decimal representation):

163241999092516819880381083582751276743897086608529035075014230421205629148 43,
163241999092516820004355772879343685230973976925480717778374838321083266745 02,
163321726512315142984410036687517745717705357656062517802592398845331002839 48.

It is noteworthy that the actual value coincides with the lower bound for the first 16 most significant digits, which provides yet another strong empirical support for the conjectured estimates in [4].

5 Conclusion. Recent advances in the structural classification of Boolean functions, together with modern high-performance computing, make Sarwate's recursive methodology [14] practical for computing the exact weight distribution of $R(4,9)$. To corroborate these computations, we employ a verification scheme based on the Heninger–Rains–Sloane congruences [6]. For $R(4,9)$, the resulting modulus tests provide independent consistency checks for the distribution reported in [12]. The congruence-based checks are applicable to any Reed–Muller code given a candidate weight enumerator; nevertheless, further validations always remain desirable.

Acknowledgments. We are grateful to Stefka Bouyuklieva for helpful discussion related to Lemma 1.

Appendix. Data tables: Heninger–Rains–Sloane test and complete weight distribution of $R(4,9)$.

Table 2: Heninger–Rains–Sloane congruence test according to (3). The third and fourth columns coincide.

k	$f(z)$	$f(z) \bmod 32$	$A_k \bmod 32$
0	1	1	1
32	16	16	16
64	120	24	24
96	560	16	16
128	1 820	28	28
160	4 368	16	16
192	8 008	8	8
224	11 440	16	16
256	12 870	6	6
288	11 440	16	16
320	8 008	8	8
352	4 368	16	16
384	1 820	28	28
416	560	16	16
448	120	24	24
480	16	16	16
512	1	1	1

Table 3: Weight Distribution of the [512,256,32] Reed–Muller code

Weight		Number of codewords
0	512	1
32	480	52955952
48	464	919315326720
56	456	271767121346560
60	452	860689275027456
64	448	89163020044002040
68	444	1777323352931696640
72	440	64959328938397057024
76	436	2094952122987829002240
80	432	86129855718211879936768
84	428	3718387228743293604986880
88	424	216407674400647746861465600
92	420	15958945395035022932054114304
96	416	1570964763114053055495174389136
100	412	207755244457303752035637154283520
104	408	34164336816436357675455725024378880
108	404	5992987676360073735151889707696128000
112	400	983217921810034263357552475089021004288
116	396	140881159168600922710983130625456163782656
120	392	17178463264607761296016540993629780705771520
124	388	1770270551281316280504947079180771901717872640
128	384	154198773988541804525321284585063483246993999900
132	380	113804373667128124744559508641773260684479892029 44
136	376	713793445298874211607839796879716106185715280216064
140	372	381616600344013129894862647690541247659597966711193 60
144	368	1744077996406613042017016863461234839306732612077058560
148	364	6832093649302361264113692814929677508406436591321481216 0
152	360	22997442048004658024533166375957838291089128020282067517 44
156	356	66674424868716978552789375387240003239187186349775851094016
160	352	16685597009641605873508056645831229244989283581517157330074 08
164	348	36117082274027891545154187373048131661136552390031364702863360
168	344	67748359898954710779361510124773951426962118474135604146110464 0
172	340	11032441933713096201663286389373184730113421621201515757397082112
176	336	15622509549761981330767923193778086142683556715677647652508417766 4
180	332	19266675322170971615767029917766543442504401756881968874572795084 80
184	328	20723534026876536792281002394151796205045793736436788802938336133120
188	324	19467144274183785293997555336377185623484125923840436555628706529280 0
192	320	15990449901813409988192707661615966056925120850571707914776940752826 32
196	316	11498415685246302189888474222781442491860129957714864173250891967627264
200	312	72459467570743603819378812718772497540870770484626494838959726267809792
204	308	40054993226393655422034298725822449978056412171282746567439522386149376 0
208	304	19440716119784239090594261981448498630646086750443974295489951777517324 80
212	300	82912118532783785444361572212137368354501088010426952045243530869735424 00
216	296	31095502600701130763682713427899390240950550846409105550583369693522427904
220	292	10262265243551021935495943795989790043448061584592614216685442619215865446 4
224	288	29820628130211072662300075044545013251288181062960712347847355409523781096 0
228	284	76339691963166668867675510699680388300388184743872831189110938463079759872 0
232	280	17224527761762198963574524869345731758046653437351694799190878995825516871 68
236	276	34267504602573059044705476415066421758676994653154784033541236313665086423 04
240	272	60131635994896839993127999354917771797727242479988779533784429205014179338 24
244	268	93095513202488540513326927728892454124955629888945474125328180450571164057 60
248	264	12718986044129514620716674156341900030463015021774940408815989741288144568320
252	260	15336997499945305387056357527918950456934399969250231086077675815418680311808
256		16324199909251682000435577287934368523097397692548071777837483832108326674502

REFERENCES.

[1] E. BERLEKAMP, F. J. MACWILLIAMS, and N. J. A. SLOANE. Gleason's theorem on self-dual codes. *IEEE Transactions on Information Theory*, 18:409–414, 1972.

[2] C. CARLET and P. SOLÉ. The weight spectrum of two families of Reed–Muller codes. *Discrete Mathematics*, 346(10):113568, 2023.

[3] P. CHARPIN. Open problems on cyclic codes. In V. S. PLESS and C. W. HUFFMAN, editors, *Handbook of Coding Theory*, pages 963–1063. Elsevier, 1998.

[4] T. W. CUSICK and Y. CHEON. Counting balanced boolean functions in n variables with bounded degree. *Experimental Mathematics*, 16(1):101–105, 2007.

[5] V. GILLOT and PH. LANGEVIN. Classification of some cosets of the Reed–Muller code. *Cryptography and Communications*:10.1007/s12095–023–00652–4, 2023.

[6] N. HENINGER, E. M. RAINS, and N. J. A. SLOANE. On the integrality of n-th roots of generating functions. *Journal of Combinatorial Theory, Series A*, 113:1732–1745, 2006.

[7] T. KASAMI and N. TOKURA. On the weight structure of Reed–Muller codes. *IEEE Transactions on Information Theory*, 16:752–759, 1970.

[8] PH. LANGEVIN. Classification of boolean quartic forms in eight variables, 2007. URL: `https://langevin.univ-tln.fr/project/quartics.html`.

[9] PH. LANGEVIN. Classification of $R(4,7)/R(2,7)$, 2012. URL: `https://langevin.univ-tln.fr/project/rm742/rm742.html`.

[10] PH. LANGEVIN and G. LEANDER. Classification of boolean quartic forms in eight variables. In B. PRENEEL and O. A. LOGACHEV, editors, *Boolean Functions in Cryptology and Information Security*, pages 139–147. IOS Press, 2008.

[11] F. J. MACWILLIAMS and N. J. A. SLOANE. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[12] M. MARKOV and Y. BORISSOV. The weight distribution of the fourth-order Reed–Muller code of length 512. *Designs, Codes and Cryptography*, 93:2487–2502, 2025.

[13] OEIS FOUNDATION INC. The on-line encyclopedia of integer sequences. URL: `https://oeis.org/`. Last accessed 8 Jan. 2026.

[14] D. V. SARWATE. *Weight Enumeration of Reed–Muller Codes and Cosets*. PhD thesis, Department of Electrical Engineering, Princeton University, Princeton NJ, 1973. Advisors: E. R. Berlekamp and J. D. Ullman.

[15] N. J. A. SLOANE and E. R. BERLEKAMP. Weight enumerator for second-order Reed–Muller codes. *IEEE Transactions on Information Theory*, 16:745–751, 1970.

Yuri Borissov, Miroslav Markov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: `youri@math.bas.bg, miro@math.bas.bg`

ВЕРИФИКАЦИЯ НА ИЗЧИСЛЕНОТО РАЗПРЕДЕЛЕНИЕ НА ТЕГЛАТА ЗА ДВОИЧНИЯ КОД НА РИЙД-МАЛЕР R(4,9)

Юри Борисов и Мирослав Марков

Абстракт

В първата част на настоящата работа преразглеждаме основните етапи от пресмятането на разпределението на теглата на двоичния код на Рийд-Малер $R(4,9)$, представено в нашата предходна статия "The Weight Distribution of the Fourth-Order Reed–Muller Code of Length 512", Designs, Codes and Cryptography 93, 2487-2502. Във втората част въвеждаме техника за проверка, основана на целочислени сравнения, предложени от Хенингер, Рейнс и Слоун, която е приложима към кодовете от тази фамилия. Показваме, че този тип проверки напълно потвърждават коректността на полученото разпределение на теглата.

Ключови думи: двоичен код на Рийд-Малер, разпределение на теглата, афинна еквивалентност.