Mathematical proof note

The Covering-Radius Formula for Projective Reed–Solomon Codes

Yang Shifu
National Mobile Communications Research Laboratory and the Frontiers Science Center for Mobile Information Communication and Security, Southeast University, Nanjing 211189, China

Version 1.0 — October 8, 2026

Result overview

The covering radius of a projective Reed–Solomon code is governed by whether its dual normal rational curve admits one further point. We prove the radius formula for every prime power $q \geq 4$ and every dimension $2 \leq k \leq q-2$: the radius is $q-k$, except that it is $q+1-k$ for even q and $k \in \{2, q-2\}$. The proof combines a finite-field complement identity with a selected root replacement. Two degree-bounded interpolation polynomials agree on too many nodes, while their highest coefficients differ. A projective involution treats the complementary dimension range. The argument includes both exceptional endpoints and gives the complete proof of the stated radius formula.

1 Context

Reed–Solomon codes connect polynomial evaluation, maximum distance separable (MDS) coding, and finite geometry [1]. Their covering radii measure worst-case approximation of ambient words by codewords [2]. For projective Reed–Solomon (PRS) codes, a syndrome requiring the full redundancy corresponds to a point extending the normal rational curve of a parity-check matrix. This relation underlies the extension results of Seroussi and Roth [3], Dür's covering-radius formulation [4], and subsequent deep-hole classifications [5].

We prove the exact radius formula using a complete-homogeneous-polynomial identity. A selected root replacement forces two interpolants to agree on too many nodes despite different highest coefficients. A two-root projective involution covers the remaining dimensions.

2 Codes, Syndromes, and the Main Result

Let $q \geq 4$ be a prime power, and fix

$$2 \leq k \leq q-2, \qquad N = q-k, \qquad d = k-2 = q-N-2. \tag{1}$$

With an ordering of $\mathbb{F}_q$ fixed, define

$$\mathrm{PRS}_q(k) = \left\{ \left((f(t))_{t \in \mathbb{F}_q}, [X^{k-1}]f \right) : \deg f < k \right\}. \tag{2}$$

The last coordinate is indexed by ∞. Write $\rho(C) = \max_u \min_{c \in C} \mathrm{wt}(u-c)$.

Theorem 2.1. *For all parameters in* (1)*,*

$$\rho(\mathrm{PRS}_q(k)) = \begin{cases} q+1-k, & q \text{ even},\ k \in \{2, q-2\}, \\ q-k, & \text{otherwise}. \end{cases} \tag{3}$$

For $t \in \mathbb{F}_q$, put $v_N(t) = (1, t, \ldots, t^N)^{\mathsf{T}}$ and $v_N(\infty) = e_N$. Let H_N have these $q+1$ columns. Every $N+1$ columns are independent by a Vandermonde determinant, including a determinant expansion along e_N when infinity is present. The power sums

$$\sum_{t \in \mathbb{F}_q} t^j = 0 \ (0 \le j < q-1), \qquad \sum_{t \in \mathbb{F}_q} t^{q-1} = -1 \tag{4}$$

give $H_N \operatorname{ev}_k(f) = 0$: the only nonzero finite-coordinate sum is the last one, and the coefficient at infinity cancels it. Thus $\mathrm{PRS}_q(k) = \ker H_N$ and has parameters $[q+1, k, N+2]_q$.

For $s \in \mathbb{F}_q^{N+1}$ and $F \in \mathbb{F}_q[X]$ of degree at most N, set

$$L_s(F) = \sum_{j=0}^{N} s_j [X^j] F. \tag{5}$$

If $T \subseteq \mathbb{F}_q \cup \{\infty\}$ has N elements, write $F_T = \prod_{t \in T \setminus \{\infty\}} (X - t)$. Its coefficient vector annihilates the N columns indexed by T, so

$$s \in \operatorname{span}\{v_N(t) : t \in T\} \quad \Longleftrightarrow \quad L_s(F_T) = 0. \tag{6}$$

For any ambient word u, its distance to the code is the minimum number of parity-check columns spanning $H_N u$. Consequently $\rho \le N+1$. The word $((t^k)_{t \in \mathbb{F}_q}, 0)$ has at most k finite agreements with any degree-less-than-k evaluation word, and at most one further agreement at infinity. Hence $\rho \ge N$. We have therefore reduced the theorem to

$$\rho = N+1 \quad \Longleftrightarrow \quad \exists s :\ L_s(F_T) \neq 0 \text{ for every } T. \tag{7}$$

This is also the one-coordinate MDS-extension criterion for the dual code: every $N+1$ columns of $[H_N \mid s]$ must be independent.

3 A Finite-Field Complement Identity

For a list $z_1, \ldots, z_m$, including multiplicities, define the complete homogeneous polynomial

$$\mathfrak{h}_j(z_1, \ldots, z_m) = \sum_{a_1 + \cdots + a_m = j} \prod_i z_i^{a_i}, \qquad \mathfrak{h}_0 = 1. \tag{8}$$

A zero entry does not change it. Its generating series is $\prod_i (1 - z_i t)^{-1}$. In particular, $\mathfrak{h}_d$ of affine functions of X has degree at most d, with highest coefficient obtained by applying $\mathfrak{h}_d$ to their slopes.

Lemma 3.1. *Let $S \subseteq \mathbb{F}_q$, $M = \mathbb{F}_q \setminus S$, and $|M| = d < q-1$. With $Q_A(Z) = \prod_{a \in A} (Z - a)$,*

$$\mathfrak{h}_d((s)_{s \in S}, Z) = Q_M(Z). \tag{9}$$

At $z \in S$, this is $\mathfrak{h}_d((s)_{s \in S}, z) = -1/Q_S'(z)$.

Proof. The field factorization gives $\prod_{a\in\mathbb{F}_q}(1-at) = 1-t^{q-1}$. Therefore

$$\frac{1}{(1-Zt)\prod_{s\in S}(1-st)} = \frac{\prod_{m\in M}(1-mt)}{(1-t^{q-1})(1-Zt)}.$$

Since $d < q-1$, comparison of the coefficients of t^d gives (9). Differentiating $Q_S Q_M = Z^q - Z$ at $z \in S$ gives $Q_S'(z)Q_M(z) = -1$. □

Lemma 3.2. *Let $E \subseteq \mathbb{F}_q$ have size N and $w_e \neq 0$. Suppose $0, -1, ((e-a)w_e)_{e\in E}$ are distinct for each $a \notin E$. Then*

$$S_E(X) = \prod_{e\in E}(1+(e-X)w_e),$$
$$\Phi_{E,w}(X) = (-1)^N \mathfrak{h}_d(-1,-1,((e-X)w_e)_{e\in E}) \tag{10}$$

satisfy $\deg \Phi_{E,w} \le d$ *and* $\Phi_{E,w}(a) = 1/S_E(a)$ *at every* $a \notin E$.

Proof. The distinct values form a set S_a of size $N+2 = q-d$. Its derivative at -1 is $Q_{S_a}'(-1) = (-1)^{N+1}S_E(a)$. Lemma 3.1, evaluated with -1 repeated, gives the node value. The affine-entry degree bound gives $\deg \Phi \le d$. □

4 Selected Root Replacement

Proposition 4.1. *If $N > d$ and either $d \ge 1$ or q is odd, no vector in* (7) *exists.*

Proof. Suppose such a vector exists, and write $L = L_s$. Choose $D = \{d_1, \dots, d_N\} \subseteq \mathbb{F}_q^\times$, normalize $L(Q_D) = 1$, and put

$$Q_i = Q_D/(X-d_i), \quad u_i = L(Q_i),$$
$$Q_{ij} = Q_D/((X-d_i)(X-d_j)).$$

Polynomial identities give

$$L((X-a)Q_i) = 1 + (d_i-a)u_i, \tag{11}$$
$$(d_i-d_j)L((X-b)Q_{ij}) = (d_i-b)u_i - (d_j-b)u_j, \tag{12}$$
$$(d_i-d_j)L((X-a)(X-b)Q_{ij}) = d_i - d_j + (d_i-a)(d_i-b)u_i - (d_j-a)(d_j-b)u_j. \tag{13}$$

Indeed, subtracting the cofactors yields (12); adding $(d_i-d_j)Q_D$ to the corresponding quadratic remainder yields (13).

Deleting d_i and adding infinity shows $u_i \neq 0$. Set

$$\beta_i = d_i u_i, \quad v_i = 1+\beta_i, \quad f_i(X) = d_i v_i - \beta_i X.$$

The single replacement at zero and the infinity-pair replacement at zero show that the β_i are distinct and avoid $0, -1$. For $a \in B = \mathbb{F}_q \setminus (D \cup \{0\})$, the values $0, a, f_1(a), \dots, f_N(a)$ are distinct: (11)

gives $f_i(a) \neq 0$, the identity $f_i(a) - a = (d_i - a)v_i$ gives $f_i(a) \neq a$, and (13) at $b = 0$ gives $f_i(a) \neq f_j(a)$.

Let $\mathcal{M} = \mathbb{F}_q \setminus \{0, 1, -\beta_1, \ldots, -\beta_N\}$ and $g = Q_{\mathcal{M}}$. Then g is monic of degree d, and differentiation at 1 gives

$$g(1) \prod_i v_i = -1. \tag{14}$$

For $d \geq 1$, the degree-d polynomial $g(Z) + g(1)$ cannot vanish at all $N > d$ distinct values $-\beta_i$. For $d = 0$ and odd q, its value is $2 \neq 0$. Thus choose j such that

$$g(-\beta_j) + g(1) \neq 0. \tag{15}$$

Write $x = d_j$, $v = v_j$, and replace x by zero:

$$E = (D \setminus \{x\}) \cup \{0\}, \qquad \mathbb{F}_q \setminus E = B \cup \{x\}, \quad |B| = d + 1.$$

Now $L(Q_E) = v$, so $L' = L/v$ is normalized on E. Its cofactor values, from (12), are

$$w_0 = u_j/v, \qquad w_{d_i} = \frac{\beta_i - \beta_j}{(d_i - x)v} \quad (i \neq j). \tag{16}$$

For every external a, nonvanishing on root sets with one replacement, or with one replacement and infinity, makes $0, -1, ((e - a)w_e)_{e \in E}$ distinct. Lemma 3.2 gives $\Phi = \Phi_{E,w}$ with degree at most d and values $1/S_E$ on $B \cup \{x\}$.

Independently, put

$$R(X) = \mathfrak{h}_d(X, f_1(X), \ldots, f_N(X), f_j(X)). \tag{17}$$

The last entry repeats f_j. The slopes are $1, -\beta_1, \ldots, -\beta_N, -\beta_j$, so Lemma 3.1 gives

$$\deg R \leq d, \qquad [X^d]R = g(-\beta_j). \tag{18}$$

For $a \in B$, repeated-node evaluation on the distinct set $\{0, a, f_1(a), \ldots, f_N(a)\}$ gives

$$\begin{aligned} R(a) &= -\frac{1}{(f_j(a) - a) f_j(a) \Pi_j(a)}, \\ \Pi_j(a) &= \prod_{i \neq j} (f_j(a) - f_i(a)). \end{aligned} \tag{19}$$

All these factors are nonzero. Let $\eta(a) = 1 + (x - a)u_j$ and $K = v^{N+1} Q'_D(x) x \neq 0$. The transport formulas (16) give

$$\begin{aligned} 1 - a w_0 &= \eta(a)/v, \\ 1 + (d_i - a) w_{d_i} &= \frac{f_i(a) - f_j(a)}{(d_i - x)v}. \end{aligned}$$

Thus $S_E(a) = \eta(a)\Pi_j(a)/(v^N Q'_D(x))$. Since $f_j(a) - a = (x - a)v$ and $f_j(a) = x\eta(a)$, (19) implies

$$K^{-1}\Phi(a) = (a - x)R(a) \qquad (a \in B). \tag{20}$$

At x, multiplying (16) gives $S_E(x) = \prod_i v_i / v^{N+1}$. Differentiating $Q_D(X)XQ_B(X) = X^q - X$ at x gives $Q'_D(x)xQ_B(x) = -1$. Together with (14), this yields

$$K^{-1}\Phi(x) = g(1)Q_B(x). \tag{21}$$

The polynomials

$$\Psi = K^{-1}\Phi, \qquad P = (X - x)R + g(1)Q_B$$

therefore agree on $d + 2$ nodes, while $\deg(P - \Psi) \le d + 1$. Hence $P = \Psi$. Also $\deg \Psi \le d$, while

$$[X^{d+1}]P = g(-\beta_j) + g(1) \neq 0$$

by (15), a contradiction. □

5 Complementary Dimensions and Exceptions

Proposition 5.1. *If $N \ge 3$ and $2k + 3 > q$, no vector in* (7) *exists. The same holds for $N = 2$ and odd q.*

Proof. Assume all N-root values are nonzero. For a finite core C of size $N - 2$, put

$$\gamma = L(Q_C), \quad \beta = L(XQ_C), \quad \alpha = L(X^2Q_C).$$

The values for two distinct parameters outside C are

$$\begin{aligned} E(a, b) &= \alpha - (a + b)\beta + ab\gamma, \\ E(a, \infty) &= \beta - a\gamma. \end{aligned} \tag{22}$$

If $\Delta = \alpha\gamma - \beta^2 \neq 0$, the matrix

$$M = \begin{pmatrix} \beta & -\alpha \\ \gamma & -\beta \end{pmatrix}, \qquad M^2 = -\Delta I$$

defines a projective involution $\tau(a) = (\beta a - \alpha)/(\gamma a - \beta)$. When it is nonidentity, it has at most two fixed points. A subset of the projective line containing no nontrivial two-element orbit consequently has size at most $(q + 3)/2$. The allowed set has $k + 3 > (q + 3)/2$ elements, so it contains a pair $a, \tau(a)$, and (22) vanishes. For $N = 2$, the allowed set is the entire projective line and the same conclusion holds for any nonidentity involution.

We show that a core with a nondegenerate, nonidentity involution can always be obtained. If $\Delta = 0$ and $\gamma = 0$, then $\beta = 0$ and the infinity value in (22) already vanishes. Otherwise a degenerate triple has $\gamma = \lambda \neq 0$, $c = \beta/\gamma$, and

$$E(a, b) = \lambda(c - a)(c - b), \qquad E(a, \infty) = \lambda(c - a).$$

Nonvanishing forces $c \in C$. Put $D_0 = C \setminus \{c\}$ and $u = L(Q_{D_0})$. The relations

$$L(X^{j+1}Q_{D_0}) - cL(X^jQ_{D_0}) = \lambda c^j, \quad j = 0, 1, 2,$$

give, on replacing c by $y \notin C$ and writing $t = c - y$,

$$\begin{aligned} \gamma_y &= tu + \lambda, \\ \beta_y &= c\gamma_y + t\lambda, \\ \alpha_y &= c^2\gamma_y + 2ct\lambda, \quad \Delta_y = -t^2\lambda^2 \neq 0. \end{aligned} \tag{23}$$

An invertible matrix of the displayed form is projectively scalar only in characteristic two with $\alpha = \gamma = 0$. In odd characteristic, (23) is already nonidentity; in characteristic two, at most one external y makes $\gamma_y = 0$.

For an initial nondegenerate identity map, the characteristic is two and $(\alpha, \beta, \gamma) = (0, v, 0)$ with $v \neq 0$. If $N \geq 3$, choose $c \in C$ and put $u = L(Q_{C\setminus\{c\}})$. The same moment recurrence yields

$$\begin{aligned} \gamma_y &= tu, \quad \beta_y = ctu + v, \\ \alpha_y &= t(c^2u + v), \quad \Delta_y = v^2 + uvt^2. \end{aligned} \tag{24}$$

Here $\alpha_y - c^2\gamma_y = tv \neq 0$, and squaring is injective, so at most one external y makes $\Delta_y = 0$. There are $k + 2 \geq 4$ finite choices outside C; an admissible replacement exists in both cases. The resulting involution gives the contradiction above. When $N = 2$ and q is odd, C is empty, a rank-one center is itself allowed, and a nondegenerate identity map is impossible. □

Proof of Theorem 2.1. For even q and $N \in \{2, q-2\}$, take $s = e_{N-1}$. A root polynomial has coefficient $[X^{N-1}]F_T = 1$ when infinity is a root, and $-\sum_{t\in T} t$ otherwise. For $N = 2$, the latter is nonzero because two distinct elements cannot sum to zero in characteristic two. For $N = q - 2$, (4) shows that it equals the sum of the two distinct missing elements, also nonzero. Equation (7) gives $\rho = N + 1$.

For all other parameters, Proposition 4.1 applies when $N > d$, including $d = 0$ in odd characteristic. If $N \leq d$, then $k \geq N + 2$ and $N + k = q$, which imply $2k + 3 > q$. Proposition 5.1 applies for $N \geq 3$ and for the nonexceptional endpoint $N = 2$. Every syndrome therefore has a spanning set of at most N columns. The already proved lower bound $\rho \geq N$ completes the proof. The case $q = 4$, $k = N = 2$ is included in the exceptional formula. □

6 Result summary

The complement identity and root replacements determine the complete PRS covering-radius formula and its dual extension criterion. One coefficient vector witnesses both even-field exceptions.

Sources

[1] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, Jun. 1960, doi: 10.1137/0108018.

[2] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge University Press, 2003, doi: 10.1017/CBO9780511807077.

[3] G. Seroussi and R. M. Roth, "On MDS extensions of generalized Reed–Solomon codes," *IEEE Transactions on Information Theory*, vol. 32, no. 3, pp. 349–354, May 1986, doi: 10.1109/TIT.1986.1057188.

[4] A. Dür, "On the covering radius of Reed–Solomon codes," *Discrete Mathematics*, vol. 126, no. 1–3, pp. 99–105, Mar. 1994, doi: 10.1016/0012-365X(94)90256-9.

[5] J. Zhang, D. Wan, and K. Kaipa, "Deep holes of projective Reed–Solomon codes," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2392–2401, Apr. 2020, doi: 10.1109/TIT.2019.2940962.