AIMS Mathematics, 11(9): 30145–30161.
DOI:10.3934/math.20261194
Received: 21 June 2026
Revised: 15 August 2026
Accepted: 09 September 2026
Published: 16 September 2026

https://www.aimspress.com/journal/Math

Research article

New lower bounds for the minimum distance of a class of binary Goppa codes

Shuhua Liang[1] **and Guanghui Zhang**[2,*]

[1] School of Economics and Management, Suqian University, Suqian, Jiangsu 223800, China

[2] School of Mathematics and Physics, Suqian University, Suqian, Jiangsu 223800, China

* **Correspondence:** Email: zghui@squ.edu.cn.

Abstract: The minimum distance estimate is one of the central parameters for binary Goppa codes. Every binary Goppa code defined by a square-free polynomial of degree r has a minimum distance of at least $2r + 1$. In this paper, we develop a support-synthesis framework for binary Goppa codes that installs an independent Bose-Chaudhuri-Hocquenghem (BCH)-type distance certificate. A compression lemma encodes any s subfield parity checks as one extension-field check; choosing $\alpha_i = \beta + b_i^{-1}$ realizes this check as a degree-one Goppa condition. For BCH checks, a Frobenius reduction leaves ν representatives, yielding $\Gamma_2(L, x-\beta) = B(n, \delta, \zeta)$. For $g = (x-\beta)h$ square-free of degree r, we obtain $\Gamma_2(L, g) = B(n, \delta, \zeta) \cap \Gamma_2(L, h)$ and $d(\cdot) \geq \max\{2r+1, \delta\}$. We give positive-dimension examples for all $r \geq 1$ and $\delta > 2r + 1$, and constant-rate families with a distance of $n/\log n$ for fixed r. BCH decoding transfers to the subcode. The result is a deliberate support-design mechanism, not a universal improvement of the classical bound.

Keywords: BCH codes; binary Goppa codes; designed distance; parity-check compression; support synthesis
Mathematics Subject Classification: 94B15, 94B60

1. Introduction

1.1. Background and motivation

Goppa codes form one of the central algebraic families of linear codes. They were introduced through a rational congruence representation [1, 2] and are now standard in the coding theory [3, 4]. A binary Goppa code is defined by a support $L = (\alpha_1, \cdots, \alpha_n)$ in a finite field of characteristic two and by

a polynomial $g(x)$ that does not vanish on the support. Its codewords are the binary vectors for which

$$\sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \pmod{g(x)}.$$

Their algebraic structure, flexible parameters, and efficient decoding explain their long-standing role in both the coding theory and code-based cryptography [5–7]. The same codes can be described as alternant codes, equivalently as binary subfield subcodes of generalized Reed-Solomon codes [3, 8, 9].

For a square-free polynomial $g(x)$ of degree r, the classical characteristic-two estimate [1, 2]

$$d(\Gamma_2(L, g)) \geq 2r + 1$$

holds for every admissible support. This is an intrinsic statement: it follows from the derivative of the locator polynomial and requires no special arrangement of L. Our question is different. Can one deliberately synthesize a support so that an ordinary square-free binary Goppa code also satisfies an independently prescribed set of parity checks, and can that additional structure yield a larger certified distance and a usable decoder? We answer this question for consecutive Bose-Chaudhuri-Hocquenghem (BCH) checks.

1.2. Related work and conceptual positioning

The general theory is naturally expressed through alternant and subfield subcode constructions. Helgert developed the parity-check viewpoint for alternant codes [9], while Delsarte's trace duality gives a fundamental relation between subfield subcodes and trace codes [8]. Algebraic decoding of Goppa codes includes Patterson's algorithm and the key-equation method of Sugiyama, Kasahara, Hirasawa, and Namekawa [10, 11]. Dimension, trace, and Galois invariance questions were further studied in [12–14]; the list-decoding results include [15, 16].

A second body of work concerns special Goppa subclasses and sharper parameter information. Separable binary families with improved or exact parameter estimates, together with their q-ary separable and cumulative extensions, were studied in [17, 18]. Wild-Goppa identities were developed in [19]. A recent preprint gives criteria and constructions for exact minimum distances in selected Goppa and BCH families [20]. The mechanisms developed in these works use either special polynomial identities or the construction of minimum-weight words. To the best of our knowledge, they do not formulate the support-synthesis procedure below, which compresses a prescribed parity-check system into one extension-field check.

BCH and Goppa codes already meet in the broader alternant framework. The classical BCH designed-distance bound comes from consecutive power checks [21–23], and the generalized BCH construction of Chien and Choy contains BCH and Goppa codes in a common parity-check formalism [24]. Other early links include decoding Goppa codes with a BCH decoder and extending Goppa codes to cyclic codes [25, 26]. A recent preprint develops the generalized-BCH viewpoint and studies generalized BCH and twisted Goppa codes attaining their designed distances [27]. The present contribution is more specific and operates in the opposite direction: we start with a desired binary parity-check array, compress its rows into one extension-field check, and then realize the compressed columns as reciprocal displacements from a degree-one Goppa root. In fact, we show that every binary linear code of a distance of at least three admits such a degree-one realization. For BCH rows,

cyclotomic reduction makes the realization explicit and produces an exact intersection of an ordinary binary Goppa code with a BCH code. Thus, our result is a support-design and subcode statement, not a new universal bound for alternant or Goppa codes.

1.3. Contributions

The contributions are as follows:

(i) We prove a lossless parity-check compression lemma. If s equations have coefficients in E and $[F : E] \geq s$, then an E-independent family in F combines them into one F-valued equation. Additionally, we record the matching necessity of $[F : E] \geq s$ when the scalarization is required to be injective on all of E^s.

(ii) We realize the compressed equation as a degree-one Goppa condition. If the compressed columns b_i are distinct and nonzero, then $\alpha_i = \beta + b_i^{-1}$ gives the following:

$$\Gamma_2(L, x-\beta) = \left\{ c \in \mathbb{F}_2^n \middle| \sum_i c_i b_i = 0 \right\}.$$

For $g = (x-\beta)h$, the Chinese remainder theorem yields the exact identity

$$\Gamma_2(L, g) = \Gamma_2(L, x-\beta) \cap \Gamma_2(L, h).$$

We further characterize the scope of the construction: every binary linear code of a distance of at least three is a degree-one binary Goppa code over an extension whose binary degree equals the code's codimension, and that degree is minimal.

(iii) For binary BCH checks, Frobenius conjugacy reduces the number of rows that must be compressed. If ν is the number of binary cyclotomic cosets modulo n meeting $\{1, \ldots, \delta-1\}$, then only ν representative checks are needed, rather than $\delta - 1$. Compressing those rows gives $\Gamma_2(L, x-\beta) = B(n, \delta, \zeta)$. Consequently, if g is square-free of degree r, then

$$d(\Gamma_2(L, g)) \geq \max\{2r+1, \delta\}.$$

(iv) We establish non-vacuous parameter consequences. For every $r \geq 1$ and $\delta > 2r+1$, the construction gives examples of a positive code dimension. For a fixed r, an explicit scaling gives a rate bounded away from zero and a certified distance of order $n/\log n$. Moreover, a BCH bounded-distance decoder with a guaranteed radius of at least $\lfloor(\delta-1)/2\rfloor$ transfers to the anchored Goppa subcode with the same guarantee.

The parameter δ is purchased through a highly structured support and an extension of a degree of at least $\nu(n, \delta)$ over the BCH root field; it is not solely determined by the degree r. Therefore, we make no claim that arbitrary square-free binary Goppa codes improve on $2r+1$, or that the present structured families are immediately suitable for cryptographic deployment. Their value is a transparent synthesis principle, a rigorous distance certificate, and a direct decoding consequence.

The rest of the paper is organized as follows: Section 2 reviews the alternant and locator descriptions and proves the classical square-free bound; Section 3 develops parity-check compression, the anchor realization, the BCH intersection theorem, parameter families, and decoder transfer; and Section 4 summarizes the scope, limitations, and directions for further work.

2. Preliminaries

We fix the notations and recall the two standard Goppa estimates used later. The details are included both to define the locator numerator appearing in the anchor argument and to separate the intrinsic square-free estimate from the support-induced BCH estimate.

Let $F = \mathbb{F}_{2^M}$ be a finite field of characteristic two, let

$$L = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

be a tuple of distinct elements of F, and let $g(x) \in F[x]$ satisfy $g(\alpha_i) \neq 0$ for every i. Then, we say that L is *admissible* for $g(x)$. The binary Goppa code associated with (L, g) is as follows:

$$\Gamma_2(L, g) = \Big\{c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n \Big| \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \pmod{g(x)}\Big\}.$$

This is the standard rational representation [1–3]. Each denominator is invertible in $F[x]/(g(x))$ by admissibility. If $\deg g = r$, then the coefficient equations of this congruence form an F-valued parity-check system whose matrix is row-equivalent over F to

$$H_g = \left(\frac{\alpha_i^j}{g(\alpha_i)}\right)_{\substack{0 \le j \le r-1 \\ 1 \le i \le n}},$$

and

$$\Gamma_2(L, g) = \{c \in \mathbb{F}_2^n \big| H_g c^{\mathsf{T}} = 0\}.$$

This places the construction explicitly inside the usual alternant framework.

For $c \in \mathbb{F}_2^n$, define the following:

$$P_L(x) = \prod_{j=1}^{n}(x - \alpha_j), \qquad N_c^L(x) = \sum_{i=1}^{n} c_i \prod_{\substack{1 \le j \le n \\ j \neq i}} (x - \alpha_j).$$

Then,

$$\sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} = \frac{N_c^L(x)}{P_L(x)}.$$

Since $P_L(x)$ is coprime to every polynomial admissible for L, we obtain the following criterion.

Lemma 2.1. *If L is admissible for $g(x)$, then*

$$c \in \Gamma_2(L, g) \quad \Longleftrightarrow \quad g(x) \mid N_c^L(x).$$

Proof. The reduction modulo $g(x)$ makes $P_L(x)$ a unit. Hence, $N_c^L(x)/P_L(x)$ vanishes the modulo $g(x)$ if and only if $N_c^L(x)$ does. □

Throughout, $d(C)$ denotes the minimum Hamming distance, with $d(\{0\}) = +\infty$. The first standard estimate about the dimensiono of $\Gamma_2(L, g)$ follows from the alternant matrix or directly from the syndrome map [1]. A brief proof is included for completeness; it will only be used below to verify that the examples are not zero-code artifacts.

Lemma 2.2. *Let $F = \mathbb{F}_{2^M}$, let $g(x) \in F[x]$ have a degree of r, and assume that L is admissible for $g(x)$. Then,*

$$\dim_{\mathbb{F}_2} \Gamma_2(L, g) \geq n - rM.$$

Proof. The map

$$\Phi_g : \mathbb{F}_2^n \longrightarrow F[x]/(g(x)), \qquad c \longmapsto \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \pmod{g(x)}$$

is $\mathbb{F}_2$-linear and has a kernel of $\Gamma_2(L, g)$. Since $g \neq 0$ and $\deg g = r$, the codomain has dimension r over F, and hence dimension rM over $\mathbb{F}_2$. Therefore,

$$\dim_{\mathbb{F}_2} \Gamma_2(L, g) = n - \operatorname{rank}_{\mathbb{F}_2}(\Phi_g) \geq n - rM.$$

□

Next, we give the familiar characteristic-two argument for the square-free bound [1, 2]. Its brief proof is also included for completeness.

Corollary 2.1. *Let $g(x) \in F[x]$ be square-free of degree r and admissible for L. Then,*

$$d(\Gamma_2(L, g)) \geq 2r + 1.$$

Proof. Let $0 \neq c = (c_1, c_2, \cdots, c_n) \in \Gamma_2(L, g)$, let $I = \operatorname{supp}(c) = \{i | c_i \neq 0, 1 \leq i \leq n\}$, and put $P_I(x) = \prod_{i \in I}(x - \alpha_i)$. Based on Lemma 2.1, the binary nature of c gives $g(x) \mid P_I'(x)$. In characteristic two, every exponent occurring in $P_I'(x)$ is even; since the finite field F is perfect, there is a $Q(x) \in F[x]$ with $P_I'(x) = Q(x)^2$. Square-freeness of $g(x)$ and $g(x) \mid Q^2(x)$ imply $g(x) \mid Q(x)$, and therefore $g^2(x) \mid P_I'(x)$. The polynomial $P_I'(x)$ is nonzero because $P_I(x)$ has distinct roots. Thus,

$$2r \leq \deg(P_I'(x)) \leq |I| - 1,$$

so $\operatorname{wt}(c) = |I| \geq 2r + 1$. □

The bound above holds for every admissible support. The next section adds an independent, support-induced certificate by realizing selected BCH checks as a degree-one Goppa condition.

3. Compressed BCH anchors

We begin with a general scalarization principle. It exactly identifies what the field extension does in the anchor construction before any BCH structure is imposed.

Lemma 3.1. *Let $E \subseteq F$ be finite fields of characteristic two, let $H = (h_{j,i}) \in E^{s \times n}$, and let $\theta_1, \ldots, \theta_s \in F$ be E-linearly independent. Define the following:*

$$b_i = \sum_{j=1}^{s} \theta_j h_{j,i}, \qquad 1 \leq i \leq n.$$

Then,

$$\{c \in \mathbb{F}_2^n \big| Hc^{\mathsf{T}} = 0\} = \left\{ c \in \mathbb{F}_2^n \Big| \sum_{i=1}^{n} c_i b_i = 0 \right\}.$$

If the columns of H are nonzero and pairwise distinct, then the elements b_i are nonzero and pairwise distinct. Moreover, if scalarization by a map of the form $(u_1, \ldots, u_s) \mapsto \sum_j \theta_j u_j$ is required to be injective on all of E^s, then necessarily $[F : E] \geq s$.

Proof. The E-linear map

$$\Phi : E^s \longrightarrow F, \qquad (u_1, \ldots, u_s) \longmapsto \sum_{j=1}^{s} \theta_j u_j,$$

is injective. For every $c \in \mathbb{F}_2^n \subseteq E^n$,

$$\sum_{i=1}^{n} c_i b_i = \Phi(Hc^{\mathsf{T}}),$$

which proves the equality of kernels. Injectivity preserves nonzero and distinct columns. Finally, an E-linear injection $E^s \hookrightarrow F$ can only exist if $s \leq \dim_E F = [F : E]$. □

The following terminology isolates the role of the distinguished linear factor and either prevents confusion with BCH zeros or support coordinates.

Definition 3.1. *Let $b_0, \ldots, b_{n-1} \in F^*$ be pairwise distinct. A choice $\beta \in F$, together with the support relation*

$$\alpha_i = \beta + b_i^{-1}, \qquad 0 \leq i \leq n-1,$$

is called an anchor realization *of the scalar parity check $\sum_i c_i b_i = 0$. The element β is the* anchor*, and $x - \beta$ is the* anchor factor*. Indeed, in characteristic two, $(\beta - \alpha_i)^{-1} = b_i$, so reduction of the Goppa syndrome modulo $x - \beta$ recovers exactly the prescribed scalar check.*

If the coefficients b_i arise by losslessly compressing one representative check from each binary cyclotomic coset relevant to a BCH code, then the realization is called a BCH-anchor realization*, and β is called a* BCH anchor*. The word "anchor" does not mean that β is a BCH zero or an additional code coordinate; it is the chosen root of the linear Goppa factor from which the reciprocal support displacements are measured.*

The next proposition directly verifies the anchor realization.

Proposition 3.1. *Let F be a finite field of characteristic two. Let*

$$b_0, b_1, \ldots, b_{n-1} \in F^*$$

be distinct nonzero elements, and fix an anchor $\beta \in F$. Define the following:

$$\alpha_i = \beta + b_i^{-1}, \qquad L = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}).$$

Then, the degree-one Goppa code $\Gamma_2(L, x - \beta)$ is exactly

$$C(b_0, \ldots, b_{n-1}) := \left\{ c \in \mathbb{F}_2^n \,\middle|\, \sum_{i=0}^{n-1} c_i b_i = 0 \right\}.$$

Consequently, if $g(x) \in F[x]$ is any Goppa polynomial divisible by $x - \beta$ and satisfying $g(\alpha_i) \neq 0$ for all i, then

$$\Gamma_2(L, g) \subseteq C(b_0, b_1, \ldots, b_{n-1}).$$

In particular,

$$d(\Gamma_2(L, g)) \geq d(C(b_0, b_1, \ldots, b_{n-1})).$$

Proof. The elements α_i are distinct because the b_i are distinct, and none of them equals β. For $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$, reduction of the rational syndrome modulo $x-\beta$ is an evaluation at β, and hence

$$c \in \Gamma_2(L, x-\beta) \quad \Longleftrightarrow \quad 0 = \sum_{i=0}^{n-1} \frac{c_i}{\beta - \alpha_i}.$$

Since the characteristic is two and $\alpha_i = \beta + b_i^{-1}$,

$$\beta - \alpha_i = b_i^{-1}.$$

Therefore, the last condition is exactly

$$\sum_{i=0}^{n-1} c_i b_i = 0.$$

This proves $\Gamma_2(L, x-\beta) = C(b_0, b_1, \ldots, b_{n-1})$. If $x-\beta$ divides $g(x)$, then a syndrome that vanishes modulo $g(x)$ also vanishes modulo $x-\beta$. This proves the inclusion, and the distance inequality follows because $\Gamma_2(L, g)$ is a subcode of $C(b_0, b_1, \ldots, b_{n-1})$. □

The preceding two statements give a useful characterization of degree-one binary Goppa codes. Additionally, it makes clear that the anchor mechanism is a general parity-check realization, not an intrinsic distance phenomenon tied to the degree of the Goppa polynomial.

Theorem 3.1. *Let $n \geq 1$. A binary linear code $C \subseteq \mathbb{F}_2^n$ can be represented as $C = \Gamma_2(L, x-\beta)$ over some finite field of characteristic two with an admissible support of distinct points if and only if $d(C) \geq 3$, with the convention $d(\{0\}) = +\infty$. More precisely, if C has a codimension of s, then $F = \mathbb{F}_{2^s}$ suffices, and every such representation over $\mathbb{F}_{2^M}$ satisfies $M \geq s$. Hence, s is the minimum possible binary extension degree.*

Proof. Let $H \in \mathbb{F}_2^{s\times n}$ be a full-rank parity-check matrix for a code with $d(C) \geq 3$. This distance condition is equivalent to the columns of H being nonzero and pairwise distinct. Since $n \geq 1$, it also implies $s \geq 1$. Choose an $\mathbb{F}_2$-basis $\theta_1, \ldots, \theta_s$ of $F = \mathbb{F}_{2^s}$, compress the columns of H as in Lemma 3.1, and reindex the resulting coefficients as $b_0, \ldots, b_{n-1}$. Put $\alpha_i = \beta + b_i^{-1}$. Then, Proposition 3.1 gives $C = \Gamma_2(L, x-\beta)$.

Conversely, suppose $C = \Gamma_2(L, x-\beta)$ over $F = \mathbb{F}_{2^M}$. Its check coefficients $b_i = (\beta-\alpha_i)^{-1}$ are nonzero and pairwise distinct. Thus, no word of weight one or two can satisfy $\sum_i c_i b_i = 0$, and so $d(C) \geq 3$. Finally, the $\mathbb{F}_2$-linear map

$$T : \mathbb{F}_2^n \longrightarrow F, \qquad T(c) = \sum_i c_i b_i,$$

has a kernel C. Therefore, rank-nullity gives the following:

$$s = \operatorname{codim}_{\mathbb{F}_2} C = \dim_{\mathbb{F}_2} \operatorname{im} T \leq \dim_{\mathbb{F}_2} F = M.$$

Thus, no binary extension of degree less than s can realize C. □

The factorization of the Goppa polynomial gives an exact nesting identity.

Proposition 3.2. *Let $\beta \in F$ and $h(x) \in F[x]$ satisfy $h(\beta) \neq 0$. Assume that L is admissible for both $x-\beta$ and $h(x)$, and put $g(x) = (x-\beta)h(x)$. Then,*

$$\Gamma_2(L, g) = \Gamma_2(L, x-\beta) \cap \Gamma_2(L, h).$$

Proof. Relabel the support as $L = (\alpha_1, \ldots, \alpha_n)$ and use the same ordering for the coordinates of c. The condition $h(\beta) \neq 0$ gives the following: $\gcd(x-\beta, h) = 1$. For every $c \in \mathbb{F}_2^n$, Lemma 2.1 and coprimality give the following:

$$\begin{aligned} c \in \Gamma_2(L, g) &\iff (x-\beta)h \mid N_c^L \\ &\iff x-\beta \mid N_c^L \text{ and } h \mid N_c^L \\ &\iff c \in \Gamma_2(L, x-\beta) \cap \Gamma_2(L, h). \end{aligned}$$

□

Let n be an odd positive integer. Let E be a finite field of characteristic two containing an element ζ of multiplicative order n. Let $2 \leq \delta \leq n$. Define the binary BCH-type code as follows:

$$B(n, \delta, \zeta) = \left\{ c \in \mathbb{F}_2^n \middle| \sum_{i=0}^{n-1} c_i \zeta^{ij} = 0 \quad \text{for every } j = 1, \ldots, \delta - 1 \right\}.$$

Identifying $c = (c_0, \ldots, c_{n-1})$ with $c(x) = \sum_{i=0}^{n-1} c_i x^i$, this is the length-$n$ narrow-sense binary BCH code whose defining zeros contain $\zeta, \zeta^2, \ldots, \zeta^{\delta-1}$.

For $a \in \mathbb{Z}/n\mathbb{Z}$, let

$$C_2(a) = \{2^u a \ (\mathrm{mod} n) \big| u \geq 0\}$$

be its binary cyclotomic coset. Put $D_\delta = \{1, \ldots, \delta - 1\}$, and choose a set $J \subseteq D_\delta$ containing one representative of every binary cyclotomic coset meeting D_δ, with $1 \in J$. Write the following:

$$\nu = \nu(n, \delta) := |J|.$$

The binary nature of the code makes the checks within each coset redundant.

Lemma 3.2. *For $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$, put*

$$S_a(c) = \sum_{i=0}^{n-1} c_i \zeta^{ia}.$$

Then,

$$B(n, \delta, \zeta) = \{c \in \mathbb{F}_2^n \big| S_j(c) = 0 \text{ for every } j \in J\}.$$

Moreover,

$$\nu(n, \delta) \leq \left\lfloor \frac{\delta}{2} \right\rfloor.$$

Proof. For every $u \geq 0$, the Frobenius map gives the following:

$$S_{2^u a}(c) = \sum_{i=0}^{n-1} c_i^{2^u} \zeta^{i 2^u a} = S_a(c)^{2^u}.$$

Thus, one vanishing check per binary cyclotomic coset is equivalent to all the checks indexed by D_δ. Finally, every integer in D_δ lies in the same cyclotomic coset as its odd part. There are $\lfloor \delta/2 \rfloor$ odd integers in D_δ, which proves the stated upper bound. □

The following elementary Vandermonde argument is the only BCH fact needed for the anchor theorem. A brief proof is included for completeness [3, 4].

Lemma 3.3 (BCH bound)**.** *The code $B(n, \delta, \zeta)$ satisfies the following:*

$$d(B(n, \delta, \zeta)) \geq \delta.$$

Proof. Suppose that $0 \neq c \in B(n, \delta, \zeta)$ has a weight of $w < \delta$. Let its support be $I = \{i_1, \ldots, i_w\}$, and set $z_\ell = \zeta^{i_\ell}$. The elements $z_1, \ldots, z_w$ are distinct and nonzero. Since c is binary, the parity-check equations give

$$\sum_{\ell=1}^{w} z_\ell^j = 0 \qquad \text{for } j = 1, 2, \ldots, w,$$

because $w \leq \delta - 1$. The $w \times w$ matrix

$$M = (z_\ell^j)_{1 \leq j, \ell \leq w}$$

has the determinant

$$\det(M) = \left(\prod_{\ell=1}^{w} z_\ell \right) \prod_{1 \leq a < b \leq w} (z_b - z_a),$$

which is nonzero. Thus, the vector $(1, \ldots, 1)^T$ cannot lie in the kernel of M, which contradicts the displayed equations. Therefore, no nonzero codeword has a weight $< \delta$. □

Now, we only compress the cyclotomic representatives, rather than all $\delta - 1$ displayed BCH checks.

Theorem 3.2. *Let n be odd, let E be a finite field of characteristic two containing an element ζ of order n, and let $2 \leq \delta \leq n$. Let F/E be a field extension of degree at least $\nu = \nu(n, \delta)$, and choose E-linearly independent elements $(\theta_j)_{j \in J}$ in F. For $i = 0, \ldots, n - 1$, define the following:*

$$b_i = \sum_{j \in J} \theta_j \zeta^{ij} \in F.$$

Then, the b_i are nonzero and pairwise distinct. Fix $\beta \in F$ and define the following:

$$\alpha_i = \beta + b_i^{-1}, \qquad L = (\alpha_0, \ldots, \alpha_{n-1}).$$

Let

$$g(x) = (x - \beta)h(x) \in F[x]$$

be square-free of degree r, and assume $g(\alpha_i) \neq 0$ for all i. Then,

$$\Gamma_2(L, x - \beta) = B(n, \delta, \zeta), \qquad \Gamma_2(L, g) = B(n, \delta, \zeta) \cap \Gamma_2(L, h),$$

and

$$d(\Gamma_2(L, g)) \geq \max\{2r + 1, \delta\}.$$

In addition, with $M = [F : \mathbb{F}_2]$,

$$\dim_{\mathbb{F}_2} \Gamma_2(L, g) \geq \dim_{\mathbb{F}_2} B(n, \delta, \zeta) - (r - 1)M.$$

Proof. First, the b_i are nonzero and pairwise distinct. If $b_i = 0$, then

$$\sum_{j\in J} \theta_j \zeta^{ij} = 0.$$

Since $\zeta^{ij} \in E$ and the θ_j are E-linearly independent, all coefficients ζ^{ij} would have to be zero, impossible. If $b_i = b_k$, then

$$\sum_{j\in J} \theta_j(\zeta^{ij} - \zeta^{kj}) = 0.$$

Again, by E-linear independence, $\zeta^{ij} = \zeta^{kj}$ for every j. Taking $j = 1$ gives $\zeta^i = \zeta^k$, hence $i \equiv k \pmod{n}$. Since $0 \le i, k \le n-1$, this gives $i = k$. Thus, the support elements $\alpha_i = \beta + b_i^{-1}$ are distinct and different from β.

By Proposition 3.1,

$$\Gamma_2(L, x-\beta) = \left\{ c \in \mathbb{F}_2^n \middle| \sum_{i=0}^{n-1} c_i b_i = 0 \right\}.$$

For $c \in \mathbb{F}_2^n$,

$$\sum_{i=0}^{n-1} c_i b_i = \sum_{j\in J} \theta_j \left(\sum_{i=0}^{n-1} c_i \zeta^{ij} \right).$$

The inner sums lie in E. Since the θ_j, $j \in J$, are E-linearly independent, the last expression is zero if and only if

$$\sum_{i=0}^{n-1} c_i \zeta^{ij} = 0 \qquad \text{for every } j \in J.$$

Therefore, Lemma 3.2 gives

$$\Gamma_2(L, x-\beta) = B(n, \delta, \zeta).$$

Since $g = (x-\beta)h$ is square-free, one has $h(\beta) \neq 0$; moreover, admissibility for g implies admissibility for both factors. Therefore, Proposition 3.2 gives the exact identity

$$\Gamma_2(L, g) = B(n, \delta, \zeta) \cap \Gamma_2(L, h).$$

Therefore, Lemma 3.3 supplies the bound δ. On the other hand, $g(x)$ is square-free of degree r, so Corollary 2.1 gives the independent estimate $2r + 1$. Combining the estimates proves the distance claim. Finally, the degree- $(r-1)$ syndrome map for h, restricted to the binary space $B(n, \delta, \zeta)$, has a rank of at most $(r-1)M$. Rank-nullity proves the dimension estimate. □

Remark 3.1. *The parameter δ is inherited from the deliberately installed BCH supercode; it is not an intrinsic consequence of* $\deg g = r$. *The cyclotomic construction uses an extension of degree ν over E, with $\nu \le \lfloor \delta/2 \rfloor$. This convenient representation need not be field-minimal when some cyclotomic cosets have a size smaller than $[E : \mathbb{F}_2]$. Theorem 3.1 shows that the exact binary redundancy of the BCH code always suffices and is minimal for a degree-one realization.*

The next corollary shows that the hypotheses can be met for every fixed target above the square-free Goppa bound.

Corollary 3.1. *Fix integers $r \geq 1$ and $\delta > 2r + 1$. Then, there exist finite fields F of characteristic two, lengths n, support tuples L over F, and square-free polynomials $g(x) \in F[x]$ of degree r such that*

$$d(\Gamma_2(L, g)) \geq \delta.$$

More precisely, for all sufficiently large m, one may take $n = 2^m - 1$, let $\nu = \nu(n, \delta)$, and obtain

$$\dim_{\mathbb{F}_2} \Gamma_2(L, g) \geq n - rm\nu \geq n - rm\left\lfloor \frac{\delta}{2} \right\rfloor > 0.$$

Proof. Choose $m \geq 3$ large enough that, with $n = 2^m - 1$,

$$n \geq \delta, \qquad n > rm\left\lfloor \frac{\delta}{2} \right\rfloor, \qquad 2^{2m} - 2^m \geq r - 1.$$

Let $E = \mathbb{F}_{2^m}$, and let $\zeta \in E$ be a primitive element, so ζ has an order of n. Form the representative set J and put $\nu = \nu(n, \delta)$. Because $\delta > 2r + 1$ and $r \geq 1$, we have $\delta \geq 4$, so D_δ contains 1 and 3. The multiplicative order of 2 modulo $n = 2^m - 1$ is exactly m: certainly $2^m \equiv 1 \pmod{n}$, while, for $0 < u < m$, one has $0 < 2^u - 1 < n$. If 1 and 3 belonged to the same binary cyclotomic coset, then $3 \equiv 2^u \pmod{n}$ for some u; reducing u modulo m gives $0 \leq u < m$. Then, since both 3 and 2^u lie strictly between 0 and n, the congruence would force $3 = 2^u$, which is impossible. Hence, $\nu \geq 2$. Let $F = \mathbb{F}_{2^{m\nu}}$, choose an E-basis $(\theta_j)_{j \in J}$ of F, set

$$b_i = \sum_{j \in J} \theta_j \zeta^{ij}, \qquad \alpha_i = b_i^{-1}, \qquad L = (\alpha_0, \ldots, \alpha_{n-1}),$$

and take the anchor $\beta = 0$.

The set $L \cup \{0\}$ has $n + 1 = 2^m$ elements. By the third inequality above,

$$|F \setminus (L \cup \{0\})| = 2^{m\nu} - 2^m \geq 2^{2m} - 2^m \geq r - 1.$$

Choose $r - 1$ distinct elements of $F \setminus (L \cup \{0\})$, say $\gamma_1, \ldots, \gamma_{r-1}$. For $r = 1$, this is the empty choice. Define

$$g(x) = x \prod_{a=1}^{r-1} (x - \gamma_a),$$

with the empty product interpreted as 1. Then, g is square-free, has a degree of r, contains the anchor factor x, and satisfies $g(\alpha_i) \neq 0$ for every support point. Theorem 3.2 gives the following:

$$d(\Gamma_2(L, g)) \geq \max\{2r + 1, \delta\} = \delta.$$

Finally, Lemma 2.2 gives the following:

$$\dim_{\mathbb{F}_2} \Gamma_2(L, g) \geq n - r[F : \mathbb{F}_2] = n - rm\nu \geq n - rm\left\lfloor \frac{\delta}{2} \right\rfloor,$$

which is positive by the choice of m. □

For fixed r and δ, the displayed estimate also gives

$$\frac{\dim_{\mathbb{F}_2} \Gamma_2(L,g)}{n} \geq 1 - \frac{rm\lfloor \delta/2 \rfloor}{2^m - 1} \longrightarrow 1.$$

This is a fixed-distance high-rate statement, not a positive-relative-distance claim.

A particularly transparent specialization is obtained by asking the BCH anchor to double the usual square-free designed-distance scale.

Corollary 3.2. *For every $r \geq 1$, there exist square-free binary Goppa codes of positive dimension and degree r satisfying*

$$d(\Gamma_2(L,g)) \geq 4r + 1.$$

For these support-engineered codes, this doubles the leading term in the usual square-free distance certificate.

Proof. Apply Corollary 3.1 with $\delta = 4r + 1$. □

Allowing the target distance to grow with the length yields a quantitative rate-distance regime. It is important that the resulting relative distance still tends to zero; the statement is not a claim of asymptotic goodness.

Corollary 3.3. *Fix $r \geq 1$ and $0 < R < 1$. There is a sequence of square-free binary Goppa codes $C_m = \Gamma_2(L_m, g_m)$, with $\deg g_m = r$ and $n_m = 2^m - 1$, such that, for all sufficiently large m,*

$$\frac{\dim_{\mathbb{F}_2} C_m}{n_m} \geq R,$$

and

$$d(C_m) \geq 2\left\lfloor \frac{(1-R)n_m}{rm} \right\rfloor + 1 = \left(\frac{2(1-R)}{r} + o(1) \right) \frac{n_m}{\log_2(n_m + 1)}.$$

Proof. Put

$$q_m = \left\lfloor \frac{(1-R)n_m}{rm} \right\rfloor, \qquad \delta_m = 2q_m + 1.$$

For a sufficiently large m, we have $2r + 1 < \delta_m \leq n_m$. Construct the cyclotomic anchor with the target δ_m. Lemma 3.2 gives $\nu = \nu(n_m, \delta_m) \leq q_m$. For a large m, one also has $\delta_m \geq 4$, hence $\nu \geq 2$, and the ambient field $F_m = \mathbb{F}_{2^{m\nu}}$ contains at least $2^{2m} - 2^m \geq r - 1$ elements outside $L_m \cup \{0\}$. Thus, the required $r - 1$ distinct cofactor roots may be chosen exactly as in Corollary 3.1. Consequently,

$$\dim_{\mathbb{F}_2} C_m \geq n_m - rm\nu(n_m, \delta_m) \geq n_m - rmq_m \geq Rn_m.$$

Theorem 3.2 gives $d(C_m) \geq \delta_m$, and $m = \log_2(n_m + 1)$ gives the asymptotic form. □

The explicit supercode relation also has an immediate algorithmic consequence. This is a transfer of a standard BCH decoder, not a new decoding algorithm; related BCH-decoder connections for Goppa codes go back to [25].

Proposition 3.3. *Under the hypotheses of Theorem 3.2, put*

$$C = \Gamma_2(L, g), \qquad B = B(n, \delta, \zeta), \qquad t = \left\lfloor \frac{\delta - 1}{2} \right\rfloor.$$

Any bounded-distance decoder for B whose guaranteed decoding radius is at least t corrects every error pattern of weight at most t on a transmitted codeword of C. For an arbitrary received word, membership of the decoder output in C may be checked; failure is declared if the check does not pass.

Proof. We have $C \subseteq B$ and $d(B) \geq \delta > 2t$. If $y = c + e$ with $c \in C$ and $\mathrm{wt}(e) \leq t$, then c is the unique codeword of B within the distance t of y. Therefore, bounded-distance BCH decoding returns c. □

We finish the section with two parameter illustrations. They specify the fields and cyclotomic representatives, but do not claim computed exact minimum distances.

Example 3.1. *We illustrate Theorem 3.2 with parameters for which all field-containment hypotheses are explicit and the dimension lower bound is positive. Let*

$$E = \mathbb{F}_{32}, \qquad n = 31, \qquad \delta = 5,$$

and choose a primitive element $\zeta \in E$, so that ζ has an order of 31*. The exponents* $1, 2, 3, 4$ *meet precisely the two binary cyclotomic cosets represented by*

$$J = \{1, 3\}.$$

Thus, $\nu = 2$. Let $F = \mathbb{F}_{32^2} = \mathbb{F}_{2^{10}}$, choose an E-basis θ_1, θ_3 of F, and define

$$b_i = \theta_1 \zeta^i + \theta_3 \zeta^{3i}, \qquad i = 0, 1, \ldots, 30.$$

The proof of Theorem 3.2 shows that the b_i are nonzero and pairwise distinct. Take the anchor

$$\beta = 0, \qquad \alpha_i = b_i^{-1}, \qquad L = (\alpha_0, \ldots, \alpha_{30}).$$

Finally, choose $g(x) = x$. Then, g is square-free of degree $r = 1$, contains the anchor factor $x - \beta = x$, and is admissible because every α_i is nonzero. Theorem 3.2 gives the following:

$$d(\Gamma_2(L, x)) \geq \max\{2r + 1, \delta\} = \max\{3, 5\} = 5.$$

Therefore, the BCH anchor certifies the stronger lower bound 5*, compared with the direct square-free certificate* 3*. Moreover,*

$$\dim_{\mathbb{F}_2} \Gamma_2(L, x) \geq 31 - 1 \cdot 10 = 21,$$

and Proposition 3.3 corrects up to two errors by BCH decoding.

Example 3.2. *We give a second anchored example with an additional Goppa factor and with the BCH parameter dominating the classical square-free estimate. Let*

$$E = \mathbb{F}_{128}, \qquad n = 127, \qquad \delta = 9,$$

and let $\zeta \in E$ be primitive. The exponents $1, \dots, 8$ meet the four binary cyclotomic cosets represented by

$$J = \{1, 3, 5, 7\}.$$

Thus, $\nu = 4$. Set $F = \mathbb{F}_{128^4} = \mathbb{F}_{2^{28}}$, choose an E-basis $\theta_1, \theta_3, \theta_5, \theta_7$ of F, and put

$$b_i = \theta_1\zeta^i + \theta_3\zeta^{3i} + \theta_5\zeta^{5i} + \theta_7\zeta^{7i}, \qquad i = 0, 1, \dots, 126.$$

Again, the b_i are nonzero and pairwise distinct. With anchor $\beta = 0$, let

$$\alpha_i = b_i^{-1}, \qquad L = (\alpha_0, \dots, \alpha_{126}).$$

The set $L \cup \{0\}$ has 128 elements, whereas $|F| = 2^{28}$. Hence, we may choose the following:

$$\gamma \in F \setminus (L \cup \{0\}).$$

Define $g(x) = x(x - \gamma)$. Then, g is square-free of degree $r = 2$, contains the anchor factor x, and is admissible for L by the choice of γ. Theorem 3.2 yields the following:

$$d(\Gamma_2(L, g)) \geq \max\{2r + 1, \delta\} = \max\{5, 9\} = 9.$$

The standard square-free Goppa estimate only certifies 5. The compressed construction gives the much stronger dimension guarantee

$$\dim_{\mathbb{F}_2} \Gamma_2(L, g) \geq 127 - 2 \cdot 28 = 71.$$

The transferred BCH decoder corrects up to four errors, whereas the usual degree-two Goppa guarantee corrects two.

The construction has three immediate coding-theoretic uses. First, it provides a modular method for imposing additional Goppa constraints on a code with a known distance and decoder: the anchored code is an exact subcode of the ambient code, so the ambient unique decoder remains valid within its guaranteed radius. Second, whenever L is admissible for h, restriction of the h-syndrome map to a binary code $C \subseteq \mathbb{F}_2^n$ gives

$$\dim_{\mathbb{F}_2}(C \cap \Gamma_2(L, h)) \geq \dim_{\mathbb{F}_2} C - (\deg h)[F : \mathbb{F}_2],$$

which separates the redundancy already present in C from the redundancy added by h. Third, for any binary parity-check system whose kernel has a distance of at least three, the rank-optimal theorem identifies the smallest binary field extension in which that kernel can be represented by one linear Goppa factor.

For cryptographic applications, the construction should be interpreted with care. An explicitly known BCH supercode supplies a useful decoding structure, but it may also supply a structural distinguisher. Therefore, the present paper does not claim that BCH-anchored codes can replace the conventional random-looking binary Goppa codes used in McEliece-type systems. Any such application would require a separate analysis of code equivalence, key indistinguishability, automorphism groups, and attacks exploiting the public supercode. The current results are best viewed as an algebraic code-design and parameter-analysis framework.

4. Conclusions

This paper formulated the BCH-anchor construction as a lossless parity-check compression and support-synthesis mechanism. The degree-one realization theorem shows that this mechanism is general: a binary linear code is representable as $\Gamma_2(L, x-\beta)$ precisely when its distance is at least three. In the BCH specialization, Frobenius conjugacy reduces the required checks from $\delta-1$ to one representative from each relevant binary cyclotomic coset. If ν denotes the number of those cosets, then an extension of degree ν over the BCH root field suffices. For a square-free polynomial $g=(x-\beta)h$ of degree r, the construction gives the exact identity

$$\Gamma_2(L, g) = B(n, \delta, \zeta) \cap \Gamma_2(L, h),$$

and the independent distance certificate

$$d(\Gamma_2(L, g)) \geq \max\{2r+1, \delta\}.$$

The refined field cost materially strengthens the quantitative examples: the two illustrations have dimension guarantees 21 and 71, rather than the weaker values 11 and 15 obtained by compressing all $\delta-1$ displayed checks. More generally, every fixed pair with $r \geq 1$ and $\delta > 2r+1$ admits codes of positive dimension, and a varying-distance choice gives constant-rate families with a certified distance of order $n/\log n$. Because every constructed code is contained in the displayed BCH code, a standard bounded-distance BCH decoder corrects $\lfloor(\delta-1)/2\rfloor$ errors on its codewords.

These conclusions are deliberately limited. They do not strengthen the square-free Goppa bound for arbitrary supports, do not determine the exact minimum distance of the constructed intersections, and do not by themselves imply a cryptographic advantage. Indeed, a visible BCH supercode is an additional structure whose security effect would require a separate analysis. Natural next questions are to determine the exact distances and weight distributions, minimize the ambient field using the exact BCH redundancy, compress stronger BCH-type bounds such as Hartmann-Tzeng constraints [28], study several compatible anchors, and assess whether any resulting structured families can be hidden without exposing exploitable supercode information.

Author contributions

Shuhua Liang: conceptualization, formal analysis, investigation, writing-original draft, writing-review and editing; Guanghui Zhang: conceptualization, formal analysis, methodology, validation, writing-original draft, writing-review and editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We sincerely thank the Associate Editor and the anonymous referees for their carefully reading and helpful suggestions that led to improvements of the paper. This work was supported by the

interdisciplinary Integration and Innovation Project of Suqian university (2025XKTD02).

Conflict of interest

We declare no conflicts of interest.

References

1. V. D. Goppa, A new class of linear correcting codes, *Probl. Peredachi Inf.*, **6** (1970), 24–30.
2. V. D. Goppa, A rational representation of codes and (L, g)-codes, *Probl. Peredachi Inf.*, **7** (1971), 41–49.
3. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge: Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077
4. F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, Amsterdam: Elsevier, 1977.
5. G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, T. Dang, et al., *Status report on the fourth round of the NIST post-quantum cryptography standardization process*, Gaithersburg: National Institute of Standards and Technology, 2025. https://doi.org/10.6028/NIST.IR.8545
6. R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, *Proceedings of the Deep Space Network Progress Report 42–44*, 1978, 114–116.
7. N. Sendrier, Code-based cryptography: state of the art and perspectives, *IEEE Secur. Priv.*, **15** (2017), 44–50. https://doi.org/10.1109/MSP.2017.3151345
8. P. Delsarte, On subfield subcodes of modified Reed-Solomon codes (Corresp.), *IEEE Trans. Inform. Theory*, **21** (1975), 575–576. https://doi.org/10.1109/TIT.1975.1055435
9. H. J. Helgert, Alternant codes, *Information and Control*, **26** (1974), 369–380. https://doi.org/10.1016/S0019-9958(74)80005-7
10. N. J. Patterson, The algebraic decoding of Goppa codes, *IEEE Trans. Inform. Theory*, **21** (1975), 203–207. https://doi.org/10.1109/TIT.1975.1055350
11. Y. Sugiyama, M. Kasahara, S. Hirasawa, T. Namekawa, A method for solving key equation for decoding Goppa codes, *Information and Control*, **27** (1975), 87–99. https://doi.org/10.1016/S0019-9958(75)90090-X
12. H. Stichtenoth, On the dimension of subfield subcodes, *IEEE Trans. Inform. Theory*, **36** (1990), 90–93. https://doi.org/10.1109/18.50376
13. M. Giorgetti, A. Previtali, Galois invariance, trace codes and subfield subcodes, *Finite Fields Th. Appl.*, **16** (2010), 96–99. https://doi.org/10.1016/j.ffa.2010.01.002
14. P. Véron, Goppa codes and trace operator, *IEEE Trans. Inform. Theory*, **44** (1998), 290–294. https://doi.org/10.1109/18.651048
15. D. Augot, M. Barbier, A. Couvreur, List-decoding of binary Goppa codes up to the binary Johnson bound, *Proceedings of IEEE Information Theory Workshop*, 2011, 229–233. https://doi.org/10.1109/ITW.2011.6089384

16. D. J. Bernstein, List decoding for binary Goppa codes, In: *Coding and cryptology*, Berlin: Springer, 2011, 62–80. https://doi.org/10.1007/978-3-642-20901-7_4

17. S. Bezzateev, N. Shekhunova, Chain of separable binary Goppa codes and their minimal distance, *IEEE Trans. Inform. Theory*, **54** (2008), 5773–5778. https://doi.org/10.1109/TIT.2008.2006442

18. S. Bezzateev, N. Shekhunova, Totally decomposed cumulative Goppa codes with improved estimations, *Des. Codes Cryptogr.*, **87** (2019), 569–587. https://doi.org/10.1007/s10623-018-0566-2

19. A. Couvreur, A. Otmani, J. P. Tillich, New identities relating wild Goppa codes, *Finite Fields Th. Appl.*, **29** (2014), 178–197. https://doi.org/10.1016/j.ffa.2014.04.007

20. Y. Chen, H. Chen, C. Ding, H. Lao, On the minimum distances of some families of BCH codes, *IEEE Trans. Inform. Theory*, **72** (2026), 5736–5744. https://doi.org/10.1109/TIT.2026.3690013

21. A. Hocquenghem, Codes correcteurs d'erreurs, *Chiffres*, **2** (1959), 147–156.

22. R. C. Bose, D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, *Information and Control*, **3** (1960), 68–79. https://doi.org/10.1016/S0019-9958(60)90287-4

23. R. C. Bose, D. K. Ray-Chaudhuri, Further results on error correcting binary group codes, *Information and Control*, **3** (1960), 279–290. https://doi.org/10.1016/S0019-9958(60)90870-6

24. R. T. Chien, D. M. Choy, Algebraic generalization of BCH-Goppa-Helgert codes, *IEEE Trans. Inform. Theory*, **21** (1975), 70–79. https://doi.org/10.1109/TIT.1975.1055336

25. C. T. Retter, Decoding Goppa codes with a BCH decoder (Corresp.), *IEEE Trans. Inform. Theory*, **21** (1975), 112–112. https://doi.org/10.1109/TIT.1975.1055318

26. K. K. Tzeng, K. Zimmermann, On extending Goppa codes to cyclic codes (Corresp.), *IEEE Trans. Inform. Theory*, **21** (1975), 712–716. https://doi.org/10.1109/TIT.1975.1055449

27. Y. Chen, H. Chen, C. Ding, H. Lao, C. Liu, C. Xie, Generalized BCH codes and twisted Goppa codes attaining their designed distances, arXiv: 2607.17517. https://doi.org/10.48550/arXiv.2607.17517

28. C. R. P. Hartmann, K. K. Tzeng, Generalizations of the BCH bound, *Information and Control*, **20** (1972), 489–498. https://doi.org/10.1016/S0019-9958(72)90887-X

AIMS Press