Optimized Goppa Coded Cooperation: Recursive Relay Selection Design and Subcode Construction with Improved Joint Decoder

Lawrence Muthama PAUL [1], Fengfan YANG [1], Viola Amondi OCHIENG [1], Daniel Kariuki WAWERU [2]

[1] Dept. of Communication and Information Engineering, Nanjing University of Aeronautics and Astronautics, 29, 210016, Nanjing, China
[2] Dept. of Mathematics, Egerton University, 536, 20115, Njoro, Kenya

lawrence.muthama12@gmail.com, yfee@nuaa.edu.cn, violahamondi@gmail.com, daniel.kariuki@egerton.ac.ke

Submitted June 22, 2026 / Accepted October 24, 2026 / Online first November 20, 2026

Abstract. *Coded cooperative communication using short-to-medium algebraic codes has emerged as a promising solution for short-packet wireless applications such as Internet-of-Things (IoT) and vehicular networks. While distributed binary Goppa codes have recently been investigated for this purpose, the minimum distance of the resulting cooperative destination code admits no general bound, and existing destination decoders do not exploit any algebraic structure of the joint code. In this paper we propose a joint Goppa coded cooperative (GCC) communication scheme in which the source and relay employ binary Goppa codes sharing a common Goppa polynomial and using disjoint supports. Under this construction, we prove that the cooperative destination code is a sub-code of an ambient binary Goppa code, yielding a guaranteed distance floor* $d_{\min} \geq 2t + 1$ *where* t *is the degree of the shared Goppa polynomial. To decode efficiently on the ambient code, we develop the extended euclidean algorithm–localized maximum likelihood (EEA-LML) decoder, which extends standard EEA–based decoding through a localized maximum-likelihood search. Furthermore, we propose a recursive bisection target search algorithm for optimising the relay message-selection pattern, scaling systematically to large code dimensions, and a three-stage joint destination decoder combining EEA-LML decoding, a sub-code membership test, and a maximum likelihood decoding (MLD) with few search candidates on the destination joint code. Monte-Carlo simulations over the additive white Gaussian noise (AWGN) and Rayleigh fading channels demonstrate that the proposed scheme outperforms existing distributed BCH-coded and Reed-Muller-coded cooperative schemes of comparable parameters, while employing the three-stage joint destination decoder.*

Keywords

Binary Goppa codes, coded cooperative communication, joint decoding, sub-code construction, extended Euclidean algorithm, information selection, Rayleigh fading channel

1. Introduction

Multiple-input multiple-output (MIMO) technology has become a fundamental component of modern wireless communications, ensuring substantial gains in data rate, spectral efficiency, and link reliability [1], [2]. Since its standardization in 4G LTE and its pivotal role in 5G, MIMO has continued to evolve toward sixth-generation (6G) systems through advancements such as massive MIMO, cell-free MIMO, and extremely-large-scale MIMO (XL-MIMO) [2–4]. By exploiting spatial diversity through multiple antennas, wireless systems achieve remarkable improvements in both network capacity and coverage. However, deploying multiple antennas on a single device imposes practical constraints on size, hardware complexity, and power consumption, making on-device MIMO impractical for many emerging applications such as Internet-of-Things (IoT) terminals, wireless sensor nodes, and vehicular ad-hoc network (VANET) units [5–7]. To address these limitations, cooperative communication allows geographically separated single-antenna terminals to share their antennas, forming a *virtual* MIMO array that achieves spatial diversity gains comparable to physical MIMO without requiring multiple antennas at any individual node [8–10].

In a cooperative communication network, a message is transmitted from a source node to a destination node with the assistance of one or more relay nodes, exploiting the broadcast nature of the wireless medium to provide independent fading paths and spatial diversity [11], [12]. Three main relaying strategies have been studied: amplify-and-forward (AF), in which the relay scales and retransmits the received signal [13]; compress-and-forward (CF), where the relay forwards a compressed version of its observation [14]; and decode-and-forward (DF), where the relay fully decodes the source message, then re-encodes and transmits it to the destination [11], [15]. Among these, DF is the natural choice for channel-coded systems: it avoids the noise amplification inherent in AF and the rate penalty of CF, and it allows the relay

DOI: 10.13164/re.2026.0522

to participate actively in the construction of the destination code [9], [16]. Due to its implementation simplicity, time-division-based half-duplex DF relaying is widely adopted in practice, where the source broadcasts in the first time slot and the relay forwards in the second, avoiding the hardware complexity of full-duplex operation [10], [17]. Most recent works on coded cooperative diversity adopt this two-time-slot half-duplex DF model as the standard framework [18–21].

Coded cooperation (CC) has been shown to achieve substantial performance gains over both non-cooperative coded transmission and uncoded cooperation [9], [22]. Various CC schemes have been investigated, each offering different trade-offs in encoding/decoding complexity, achievable rate, and suitability for specific block lengths, including LDPC CC [23], [24], turbo CC [25], polar CC [26], [27], Reed-Muller CC [28], and Reed-Solomon CC [29]. While probabilistic codes such as LDPC and turbo codes perform excellently at long block lengths approaching capacity, most emerging applications, including IoT terminals, wireless sensor nodes, and short-packet machine-type communication, operate with short-to-medium information blocks, where short algebraic codes offer superior performance [18], [27]. Binary Goppa codes [30], [31] are among the most compelling algebraic codes for this regime. As subfield subcodes of Generalized Reed-Solomon (GRS) codes, they satisfy the Goppa bound $d_{\min} \geq 2t + 1$, where t is the degree of the Goppa polynomial [31], [32]. Unlike BCH codes, binary Goppa codes offer flexible parameter design through independent choice of the locator set $\mathcal{L}$ and Goppa polynomial $G(x)$ [33]. They also exhibit excellent weight spectra at short block lengths, with families known to meet the Gilbert-Varshamov bound [34], and admit efficient hard-decision decoding via the Extended Euclidean Algorithm (EEA) [35]. These properties make binary Goppa codes a natural fit for short-packet coded-cooperative diversity.

Waweru et al. [18] introduced the Goppa coded-cooperative (GCC) framework, the first systematic application of binary Goppa codes to a single-relay cooperative system. In their construction, two Goppa codes are deployed independently at the source and relay, with the relay selecting a subset of the decoded source bits to generate its codeword via exhaustive or partial heuristic search. The resulting joint destination code is decoded using naive and smart algorithms that treat it as a generic linear code. Feng et al. [36] subsequently extended the GCC framework to higher-order modulations while retaining the same relay selection and decoding philosophy.

The main features and limitations of these prior Goppa-coded cooperative schemes are summarized in Tab. 1. Despite these contributions, three fundamental limitations persist across both works. First, since general Goppa codes are deployed at the source and relay without algebraic coupling, the minimum distance of the joint destination code $C_{\mathrm{D_e}}$ has no analytical bound and must be determined numerically for each code pair, offering no structural guarantee on error-correction capability. Second, the relay selection algorithms in both works fix an ad hoc division of the message block with no principled stopping criterion, making the search unreliable as the code dimension grows. Third, the naive and smart destination decoders make no use of the Goppa algebraic structure of the joint code, even when that structure is present and could be exploited for more reliable decoding. Motivated by these limitations, this paper proposes the following contibutions:

- Algebraically coupled distributed Goppa code design with a guaranteed minimum distance bound. We propose a distributed binary Goppa code design in which the source code $C_{\mathrm{S_o}} = \Gamma(\mathcal{L}_S, G)$ and relay code $C_{\mathrm{R_e}} = \Gamma(\mathcal{L}_R, G)$ share a common Goppa polynomial $G(x)$ while operating over disjoint locator sets $\mathcal{L}_S$ and $\mathcal{L}_R$ drawn from the same field. This algebraic coupling ensures that the joint destination code $C_{\mathrm{D_e}}$ is a subcode of the well-defined ambient Goppa code $\Gamma(\mathcal{L}_D, G(x))$, where $\mathcal{L}_D = \mathcal{L}_S \cup \mathcal{L}_R$. Consequently, $C_{\mathrm{D_e}}$ inherits the Goppa bound $d_{\min} \geq 2t + 1$; a structural guarantee on the error-correction capability of the destination code that is absent from all prior GCC constructions [18], [36], where the minimum distance is determined only numerically. Furthermore, this subcode relationship directly enables the algebraic decoding strategy of contribution 2 below.

- Extended Euclidean Algorithm–localized maximum likelihood (EEA-LML) decoder exploiting the Goppa structure of the joint code. Building on the proposed code design, we develop an EEA-LML decoder for binary Goppa codes that operates in two stages: it first applies an EEA-based decoder to the received vector, then invokes a localized maximum likelihood (LML) search only at positions where the EEA output contains non-binary coordinates, reducing decoding complexity while retaining reliability. This decoder is employed independently at the source and relay nodes. At the destination, the subcode structure of $C_{\mathrm{D_e}} \subset \Gamma(\mathcal{L}_D, G(x))$ established in contribution 1 means that every codeword of $C_{\mathrm{D_e}}$ is also a codeword of the ambient Goppa code. The received joint vector $\mathbf{r} = [\mathbf{r}_1, \mathbf{r}_2]$ is therefore first decoded as a codeword of $\Gamma(\mathcal{L}_D, G(x))$ via the EEA-LML decoder, yielding $\tilde{\mathbf{c}} = [\tilde{\mathbf{c}}_1, \tilde{\mathbf{c}}_2]$, which is then verified to lie in $C_{\mathrm{D_e}}$. This two-level decoding strategy is formalized in Algorithm 3 and achieves a lower bit error rate than both the smart and naive decoders of [18], [36], which make no use of the Goppa structure.

- Recursive bisection target search for systematic relay selection. To identify the optimal relay bit selection pattern and hence the best possible joint destination code $C_{\mathrm{D_e}}^{(i)}$, we propose a recursive bisection target search algorithm (Algorithm 2). Here $k_2 \leq k_1$ denotes the number of bits selected by the relay from the k_1 decoded source bits, and $p \in \mathbb{N}$ is the bisection depth satisfying $2^p \leq \lfloor k_2/2 \rfloor < 2^{p+1}$. In Phase 1, the de-

Work	Code design	$\mathbf{d}_{\min}$ guarantee	Relay selection	Destination decoder
Waweru et al. [18]	Independent distributed Goppa codes at the source and relay; no common ambient destination Goppa code is imposed.	No structural lower bound for the joint destination block; $d_{\min}$ is obtained numerically for each selection pattern.	Full search and target-search-based selection.	Naive and Smart decoders; the destination decoder treats the joint block as a generic linear code.
Feng et al. [36]	Distributed Goppa-coded cooperation extended to higher-order modulation settings.	No structural lower bound for the joint destination block; follows the same numerical-distance approach.	Selection-pattern search based on the joint destination code distance.	Naive and Smart decoders; no explicit use of an ambient Goppa decoder at the destination.
Proposed scheme	Algebraically coupled binary Goppa codes with common Goppa polynomial $G(x)$ and disjoint locator sets, so that $C_{\mathrm{D_e}} \subsetneq \Gamma_{\mathrm{D_e}}$.	Guaranteed by the ambient Goppa code: $d_{\min}(C_{\mathrm{D_e}}) \geq d_{\min}(\Gamma_{\mathrm{D_e}}) \geq 2t+1$.	Recursive bisection target search with reduced candidate selection patterns.	Proposed improved joint decoder based on EEA–LML decoding, membership testing, and localized joint ML refinement.

Tab. 1. Comparison with prior Goppa-coded cooperative communication schemes.

coded message block $\hat{\mathbf{m}}_1$ is bisected p times to produce 2^p disjoint intervals, pre-selecting $2^p - 1$ bit positions and distributing the remaining $k_2 - 2^p + 1$ positions systematically across intervals. In Phase 2, the selection pattern set $\bar{\Psi}_i$ is refined iteratively by retaining only the patterns that minimise the number of low-weight joint codewords at each iteration, until a unique optimal pattern is identified. Unlike the heuristic partial search of [18], [36], which fixes an ad hoc message block division with no principled stopping criterion, the proposed algorithm is governed by a well-defined termination condition, making it reliable and scalable for large code dimensions.

The remainder of this paper is organized as follows: Section 2 presents the definition, parity check matrix and code parameters of binary Goppa codes. Section 3 describes the system model and the joint Goppa sub-code construction. Section 4 describes the proposed full search and target search algorithms for optimized destination code and illustrative examples of the two search methods. In Sec. 5, the EEA-LML decoder for binary Goppa codes and the three-stage joint destination decoder is presented. Section 6 presents Monte-Carlo simulation results over the Rayleigh fading channel for five parameter cases. Finally, a conclusion of the manuscript is presented in Sec. 7.

2. Preliminaries

This section reviews the fundamental theory of Goppa codes, its properties [31], [32] and fixes the notations used throughout the paper.

2.1 Definition and Parity Check Matrix of Goppa Codes

Let $q = 2^m$ for some $m \in \mathbb{N}$, and let $\mathbb{F}_q$ denote the binary extension field of q elements with primitive element ξ. Let $G(x) \in \mathbb{F}_q[x]$ with $\deg G(x) = t$, called the *Goppa polynomial*, and let $\mathcal{L} = \{\xi_i : 0 \leq i \leq n-1\} \subset \mathbb{F}_q$ be a set of n distinct elements, called the *locator set*, such that $G(\xi_i) \neq 0$ for all $\xi_i \in \mathcal{L}$. The binary Goppa code $\Gamma(\mathcal{L}, G)$ is defined as the set of all vectors $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$ satisfying

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

When $\mathcal{L} = \mathbb{F}_q$, the code $\Gamma(\mathcal{L}, G)$ is called *maximal*. From (1), $c\mathbf{H}^{\mathrm{T}} = \mathbf{0}$, where the parity check matrix $\mathbf{H} \in \mathbb{F}_q^{t \times n}$ is given by

$$\mathbf{H} = \begin{pmatrix} \frac{1}{G(\xi_0)} & \frac{1}{G(\xi_1)} & \cdots & \frac{1}{G(\xi_{n-1})} \\ \frac{\xi_0}{G(\xi_0)} & \frac{\xi_1}{G(\xi_1)} & \cdots & \frac{\xi_{n-1}}{G(\xi_{n-1})} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\xi_0^{t-1}}{G(\xi_0)} & \frac{\xi_1^{t-1}}{G(\xi_1)} & \cdots & \frac{\xi_{n-1}^{t-1}}{G(\xi_{n-1})} \end{pmatrix}. \tag{2}$$

When each $\mathbb{F}_q$-entry of $\mathbf{H}$ is expanded as an m-dimensional column vector over $\mathbb{F}_2$, a binary parity check matrix of size $mt \times n$ is obtained. Consequently, $\Gamma(\mathcal{L}, G)$ is a binary linear code with dimension $k \geq n - mt$ and minimum distance $d_{\min} \geq 2t + 1$.

2.2 Example of a Goppa Code

Consider the Goppa polynomial $G(x) = x^2 + x + \alpha^3$ and the locator set $\mathcal{L} = \mathbb{F}_{16} \setminus \{0\} = \{1, \xi, \xi^2, \ldots, \xi^{14}\}$, where ξ is a primitive element of $\mathbb{F}_{16}$ satisfying $\xi^4 + \xi + 1 = 0$. Since $G(\xi^i) \neq 0$ for all $\xi^i \in \mathcal{L}$, the code $\Gamma(\mathcal{L}, G)$ is well defined. The code has length $n = |\mathcal{L}| = 15$, dimension $k \geq 15 - 4 \cdot 2 = 7$, and minimum distance $d_{\min} \geq 2(2) + 1 = 5$. Thus $\Gamma(\mathcal{L}, G)$ is a binary $[15, 7, 5]$ Goppa code capable of correcting up to $t = 2$ errors. Its parity check matrix over $\mathbb{F}_{16}$ takes the form

$$\mathbf{H} = \begin{pmatrix} \frac{1}{G(1)} & \frac{1}{G(\xi)} & \cdots & \frac{1}{G(\xi^{14})} \\ \frac{1}{G(1)} & \frac{\xi}{G(\xi)} & \cdots & \frac{\xi^{14}}{G(\xi^{14})} \end{pmatrix}, \tag{3}$$

where each entry $\frac{\xi_i^j}{G(\xi_i)} \in \mathbb{F}_{16}$ is expanded into its 4-dimensional binary column vector over $\mathbb{F}_2$, yielding the binary parity check matrix $\widetilde{\mathbf{H}} \in \mathbb{F}_2^{8 \times 15}$. From $\widetilde{\mathbf{H}}$, standard row reduction gives the systematic generator matrix $\widetilde{\mathbf{G}} \in \mathbb{F}_2^{7 \times 15}$, whose rows span the $[15, 7, 5]$ Goppa code. This code corrects any combination of up to $t = 2$ bit errors, consistent with the Goppa bound $d_{\min} \geq 2t + 1 = 5$.

3. System Model for Coded Cooperative Communication

In this section, we describe how coded cooperation works with a single relay communicating over two time slots. The system comprises of three nodes: a source node, a relay node and a destination node. Figure 1 illustrates how the three nodes interacts across a noisy wireless channel.

The cooperative system operates over a Rayleigh fading channel in a two-time-slot half-duplex mode involving three nodes: a source S, a relay R, and a destination D. Unlike prior GCC schemes [18], [36] which deploy arbitrary Goppa codes at the source and relay, the proposed scheme employs two binary Goppa codes $C_{\mathrm{S_o}}$ and $C_{\mathrm{R_e}}$ that are algebraically coupled by design. Specifically, both codes share a common Goppa polynomial $G(x)$ and operate over disjoint locator sets drawn from the same field, a construction that, as shown in Sec. 3.1.2, guarantees a minimum distance bound on the joint destination code $C_{\mathrm{D_e}}$.

In the broadcast phase (time slot 1), the source encodes the message block $\mathbf{m}_1 \in \mathbb{F}_2^{k_1}$ using the generator matrix $\boldsymbol{\mathcal{G}}_S$ of $C_{\mathrm{S_o}}[n_1, k_1, d_1]$ to produce a codeword $\mathbf{c}_1 \in C_{\mathrm{S_o}} \subset \mathbb{F}_2^{n_1}$. The modulated signal is broadcast simultaneously to both the relay and destination nodes over independent fading links. In the cooperation phase (time slot 2), the relay decodes its received observation $\hat{\mathbf{r}}$ to recover an estimated codeword $\hat{\mathbf{c}}_1 \in C_{\mathrm{S_o}}$ and the corresponding information vector $\hat{\mathbf{m}}_1 \in \mathbb{F}_2^{k_1}$. The relay then selects $k_2 \leq k_1$ bits from $\hat{\mathbf{m}}_1$ according to an optimized selection pattern, determined by the recursive bisection target search proposed in Sec. 4 to form its own message $\mathbf{m}_2 \in \mathbb{F}_2^{k_2}$. This message is encoded by the relay code $C_{\mathrm{R_e}}[n_2, k_2, d_2]$ with generator matrix $\boldsymbol{\mathcal{G}}_R$, satisfying $k_2 \leq k_1$ and $d_1 < d_2$, to produce the relay codeword $\mathbf{c}_2 = \mathbf{m}_2\boldsymbol{\mathcal{G}}_R \in C_{\mathrm{R_e}}$, which is then modulated and forwarded to the destination.

At the destination, the joint received signal $[\hat{\mathbf{r}}_1, \hat{\mathbf{r}}_2]$ from the source and relay links is passed to the proposed EEA-LML joint decoder (Algorithm 3). Because the joint destination code $C_{\mathrm{D_e}}$ is a subcode of the ambient Goppa code $\Gamma(\mathcal{L}_D, G(x))$ by construction, the decoder can exploit the full Goppa algebraic structure of the ambient code, an avenue unavailable to the generic smart and naive decoders of prior works.

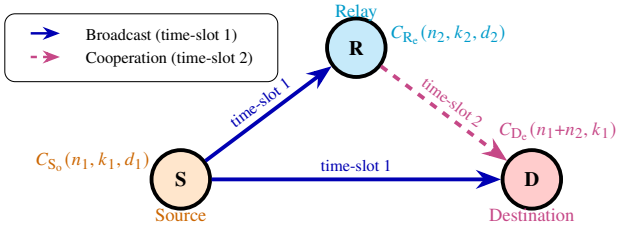


Fig. 1. Single-relay coded-cooperative system. The source S broadcasts $\mathbf{c}_1 \in C_{\mathrm{S_o}}$ in time-slot 1 over fading links. The relay R decodes, selects k_2 bits, re-encodes as $\mathbf{c}_2 \in C_{\mathrm{R_e}}$, and forwards to the destination in time-slot 2. The destination jointly decodes the received signal $\mathbf{r}_D$ using the ambient Goppa code $\Gamma(\mathcal{L}_D, G(x))$.

3.1 The Channel

A single-relay channel model is considered, where distributed channel coding is enabled through the use of Goppa codes.

3.1.1 General Linear Block Code at the Destination Node

Figure 2 illustrates the proposed distributed Goppa coded-cooperative system for a single-relay operating over a Rayleigh fading channel. As described in Sec. 3.1.2, the source and relay codes $C_{\mathrm{S_o}}$ and $C_{\mathrm{R_e}}$ share a common Goppa polynomial $G(x)$ and operate over disjoint locator sets, a design that guarantees a minimum distance bound on the joint destination code $C_{\mathrm{D_e}}$.

Broadcast Phase (Time-slot 1)

The source encodes the message block $\mathbf{m}_1 \in \mathbb{F}_2^{k_1}$ into a codeword $\mathbf{c}_1 \in C_{\mathrm{S_o}}$ using the generator matrix $\boldsymbol{\mathcal{G}}_S$. The codeword $\mathbf{c}_1$ is modulated (BPSK or M-QAM, depending on the target spectral efficiency/SNR regime) to produce the transmitted signal sequence

$$\mathbf{t}_S = \left[t_S^0, t_S^1, \ldots, t_S^{n_1-1}\right] \tag{4}$$

which is broadcasted simultaneously to both the relay and destination nodes over independent Rayleigh fading links. The received signals at time instant i are

$$t_{S,R}^i = \alpha_{S,R}^i t_S^i + \eta_{S,R}^i, \qquad t_{S,D}^i = \alpha_{S,D}^i t_S^i + \eta_{S,D}^i \tag{5}$$

where $\alpha_{S,R}^i$ and $\alpha_{S,D}^i$ are independent complex Gaussian channel fading coefficients with zero mean and variance $\sigma^2/2$ per dimension, and $\eta_{S,R}^i$, $\eta_{S,D}^i$ are additive white Gaussian noise terms with the same statistics. After all n_1 modulated bits are transmitted, the received sequences at the relay and destination are

$$\mathbf{r}_{S,R} = \left[r_{S,R}^0, \ldots, r_{S,R}^{n_1-1}\right], \qquad \mathbf{r}_{S,D} = \left[r_{S,D}^0, \ldots, r_{S,D}^{n_1-1}\right]. \tag{6}$$

Cooperation Phase (Time-slot 2)

The relay demodulates $\mathbf{r}_{S,R}$ and decodes it using the EEA-LML decoder (Algorithm 3) to recover the estimated codeword $\hat{\mathbf{c}}_1 \in C_{\mathrm{S_o}}$ and the corresponding message $\hat{\mathbf{m}}_1 \in \mathbb{F}_2^{k_1}$. Under an ideal source-relay channel, $\hat{\mathbf{m}}_1 = \mathbf{m}_1$. The relay then applies the recursive bisection target search (Algorithm 2) to select $k_2 \leq k_1$ bits from $\hat{\mathbf{m}}_1$, forming the relay message $\mathbf{m}_2 \in \mathbb{F}_2^{k_2}$. This is encoded by $C_{\mathrm{R_e}}$ with generator matrix $\boldsymbol{\mathcal{G}}_R$ to yield $\mathbf{c}_2 = \mathbf{m}_2\boldsymbol{\mathcal{G}}_R \in C_{\mathrm{R_e}}$, which is BPSK or M-QAM-modulated and forwarded to the destination. The received signal at time instant i is y

$$t_{R,D}^i = \alpha_{R,D}^i t_R^i + \eta_{R,D}^i \tag{7}$$

where $\alpha_{R,D}^i$ and $\eta_{R,D}^i$ are defined analogously to those in the broadcast phase. After all n_2 modulated bits are transmitted, the received sequence at the destination is

$$\mathbf{r}_{R,D} = \left[r_{R,D}^0, r_{R,D}^1, \ldots, r_{R,D}^{n_2-1}\right]. \tag{8}$$

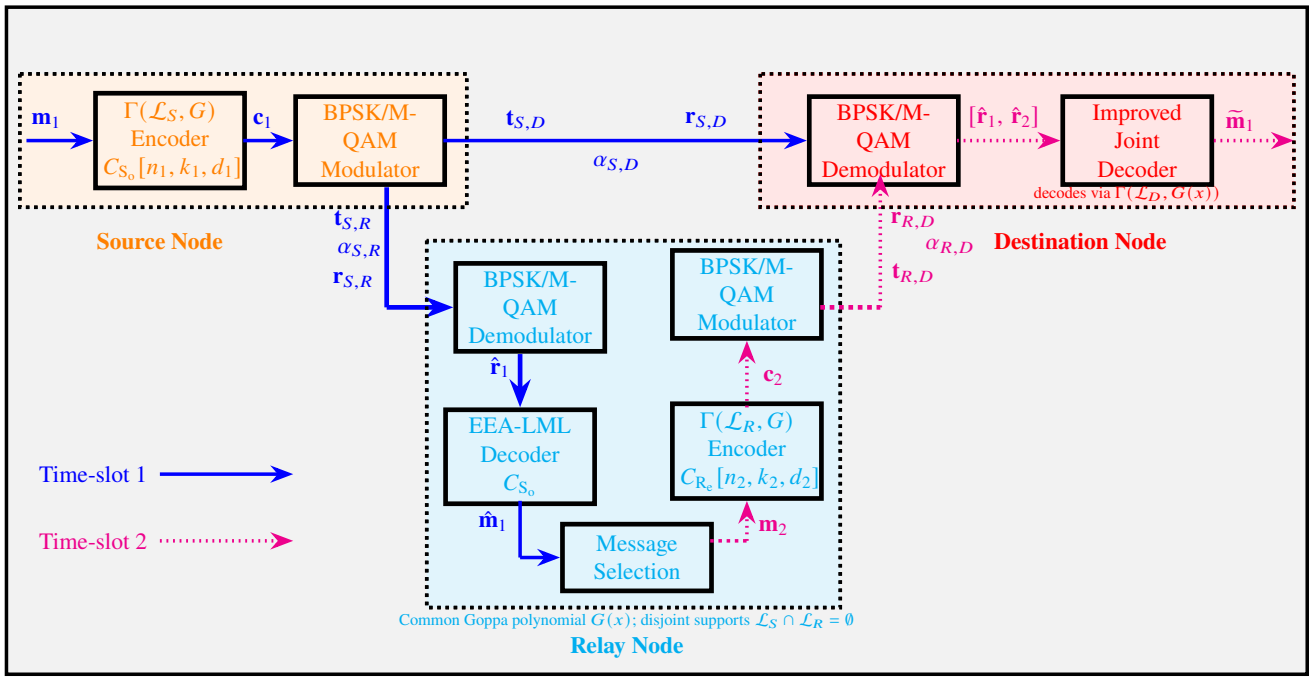


Fig. 2. System model of the proposed single-relay distributed Goppa coded-cooperative scheme. The source encodes $\mathbf{m}_1$ using $C_{S_o} = \Gamma(\mathcal{L}_S, G)$ and broadcasts in time-slot 1 over fading links $\alpha_{S,D}$ and $\alpha_{S,R}$. The relay decodes via the EEA-LML decoder, applies the recursive bisection target search to select k_2 bits, and re-encodes using $C_{R_e} = \Gamma(\mathcal{L}_R, G)$, where $\mathcal{L}_S$ and $\mathcal{L}_R$ are disjoint subsets of the same field sharing the common Goppa polynomial $G(x)$. The destination jointly decodes $[\hat{\mathbf{r}}_1, \hat{\mathbf{r}}_2]$ by decoding the ambient code $\Gamma(\mathcal{L}_D, G(x))$ via EEA-LML and verifying the result against C_{D_e}.

Finally, the destination concatenates the two received sequences into the joint signal

$$\mathbf{r}_D = \left[\mathbf{r}_{S,D}, \mathbf{r}_{R,D}\right]. \tag{9}$$

The joint signal $\mathbf{r}_D$ is demodulated to yield $[\hat{\mathbf{r}}_1, \hat{\mathbf{r}}_2]$, which is passed to the proposed EEA-LML joint destination decoder (Algorithm 3).

3.1.2 Joint Goppa Subcode at the Destination Node

Generally, any two distinct Goppa codes at the source and relay nodes, respectively, will yield a general linear block code $C_{D_e}(n_1+n_2, k_1, d_{\min})$ at the destination as discussed in Sec. 3.1.1. In this scenario, the joint code will be decoded using the smart algorithm [18] and the naive algorithm [20]. However, if the joint code has a Goppa structure, the three stage decoding technique (Algorithm 3) proposed in Sec. 5 becomes more effective, since it exploits the algebraic structure of the joint code directly.

In this section, we explore the conditions under which the joint code C_{D_e} at the destination is a subcode of a Goppa code. A Goppa code $\Gamma(\mathcal{L}, G)$ is fully specified by its support set $\mathcal{L} \subseteq \mathbb{F}_q$ and its Goppa polynomial $G(x) \in \mathbb{F}_q[x]$ of degree t, with the parity-check condition

$$\sum_{\xi \in \mathcal{L}} \frac{c_\xi}{x - \xi} \equiv 0 \pmod{G(x)}. \tag{10}$$

Consider the source code $C_{S_o} = \Gamma(\mathcal{L}_S, G_S)$ and the relay code $C_{R_e} = \Gamma(\mathcal{L}_R, G_R)$, with parity-check matrices $\mathbf{H}_S$ and $\mathbf{H}_R$ respectively. The support sets $\mathcal{L}_S$ and $\mathcal{L}_R$ are indexed as; $\mathcal{L}_S = \{\xi_i : 0 \le i \le n_1 - 1\} \subset \mathbb{F}_q$, $\mathcal{L}_R = \{\xi_i : n_1 \le i \le n_1 + n_2 - 1\} \subset \mathbb{F}_q$ with $\xi_i \neq \xi_j$ and $G(\xi_i) \neq 0\ \forall\, i$. The joint destination support is

$$\mathcal{L}_D = \mathcal{L}_S \cup \mathcal{L}_R = \{\xi_0, \xi_1, \ldots, \xi_{n_1+n_2-1}\}, \tag{11}$$

of cardinality $n_D = n_1 + n_2 \le q$. If $G_S(x) = G_R(x) = G(x)$, the Goppa code at the destination is

$$\Gamma_D \triangleq \Gamma(\mathcal{L}_D, G) \tag{12}$$

with dimension $k_{\Gamma_D} \ge n_D - mt$ and minimum distance $d_{\min}(\Gamma_D) \ge 2t+1$. Under these conditions, Equation (10) for the destination codeword $\mathbf{c}_D$ decomposes as

$$\sum_{i=0}^{n_D-1} \frac{c_{D,i}}{x - \xi_i} = \underbrace{\sum_{i=0}^{n_1-1} \frac{c_{1,i}}{x - \xi_i}}_{\equiv 0 \pmod{G(x)}} + \underbrace{\sum_{i=n_1}^{n_D-1} \frac{c_{2,i}}{x - \xi_i}}_{\equiv 0 \pmod{G(x)}}$$
$$\equiv 0 \pmod{G(x)} \tag{13}$$

where the first sum vanishes because $\mathbf{c}_1 \in \Gamma(\mathcal{L}_S, G)$ and the second sum vanishes because $\mathbf{c}_2 \in \Gamma(\mathcal{L}_R, G)$. Therefore, the destination codeword $\mathbf{c}_D$ satisfies the Goppa parity-check condition over the joint support $\mathcal{L}_D$ with respect to the common polynomial $G(x)$. Consequently,

$$C_{D_e} \subsetneq \Gamma_D, \tag{14}$$

with parity-check matrix

$$\mathbf{H}_D = \left[\mathbf{H}_S \,\middle|\, \mathbf{H}_R\right]. \tag{15}$$

From (14), it follows that

$$d_{\min}(C_{\mathrm{D_e}}) \geq 2t+1. \tag{16}$$

Equation (16) establishes a lower bound on the free distance of the joint linear code that is guaranteed by the Goppa structure alone, independent of the specific selection pattern Φ chosen at the relay. The target search method of Sec. 4 operates within a family of codes that all share this distance floor, and the optimisation reduces to selecting the pattern that minimises the higher-order terms of the weight spectrum.

4. Proposed Bit Selection Algorithm at the Relay

At the relay node, different message selection patterns leads to different joint codes at the destination. The joint code with the largest minimum Hamming distance at the destination yields the best performance. Therefore, finding an optimized message selection at the relay is essential.

Let k_1 and $k_2 \leq k_1$ denote the information lengths of the source and relay codes, respectively. The relay constructs its message by selecting k_2 positions from the k_1 decoded source bits. Formally, a *selection pattern* is an ordered k_2-subset of position indices drawn from $\{0,1,\ldots,k_1-1\}$, and is represented as a mapping

$$\Phi : \{0,1,\ldots,k_2-1\} \longrightarrow \{0,1,\ldots,k_1-1\} \tag{17}$$

where Φ is strictly order-preserving, i.e., $\Phi(0) < \Phi(1) < \cdots < \Phi(k_2-1)$. The collection of all such mappings forms the *selection pattern space*

$$\Psi = \left\{ \Phi_i \;\middle|\; i \in \mathcal{I} = \left\{1,2,\ldots,\binom{k_1}{k_2}\right\}\right\} \tag{18}$$

where $|\Psi| = \binom{k_1}{k_2}$ is the total number of admissible patterns. Given the decoded source message $\hat{\mathbf{m}}_1 = [\hat{m}_0, \hat{m}_1, \ldots, \hat{m}_{k_1-1}] \in \mathbb{F}_2^{k_1}$, the relay message induced by the i-th pattern $\Phi_i \in \Psi$ is

$$\mathbf{m}_2^{(i)} = \left[\hat{m}_{\Phi_i(0)}, \hat{m}_{\Phi_i(1)}, \ldots, \hat{m}_{\Phi_i(k_2-1)}\right] \in \mathbb{F}_2^{k_2}. \tag{19}$$

For each $\Phi_i \in \Psi$, the relay encodes $\mathbf{m}_2^{(i)}$ using $C_{\mathrm{R_e}} = \Gamma(\mathcal{L}_R, G)$ to produce the relay codeword $\mathbf{c}_2^{(i)} = \mathbf{m}_2^{(i)}\boldsymbol{\mathcal{G}}_R \in C_{\mathrm{R_e}}$, and the corresponding joint destination code is

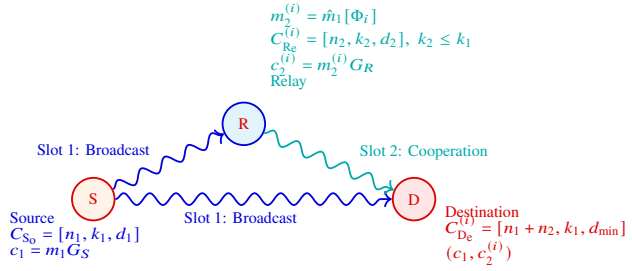


Fig. 3. Two-phase Goppa-coded cooperation with-division half-duplex.

$$C_{\mathrm{D_e}}^{(i)} = \left\{ [\mathbf{c}_1, \mathbf{c}_2^{(i)}] \;\middle|\; \begin{array}{c} \mathbf{c}_1 = \mathbf{m}_1\boldsymbol{\mathcal{G}}_S \in \Gamma(\mathcal{L}_S, G),\ \mathbf{m}_1 \in \mathbb{F}_2^{k_1} \\ \mathbf{m}_2^{(i)} = \hat{m}_1[\Phi_i] \in \mathbb{F}_2^{k_2},\ k_2 \leq k_1 \\ \mathbf{c}_2^{(i)} = \mathbf{m}_2^{(i)}\boldsymbol{\mathcal{G}}_R \in \Gamma(\mathcal{L}_R, G) \end{array} \right\} \tag{20}$$

where each $C_{\mathrm{D_e}}^{(i)}$ is a subcode corresponding to index $\Phi_i \in \Psi$. The full search and the targeted search algorithms are employed to determine the optimal subcode $C_{\mathrm{D_e}}^{(i^{\mathrm{opt}})}$ and its corresponding vector $\Phi_{i^{\mathrm{opt}}} \in \Psi$, which is chosen to maximize the minimum distance $d(C_{\mathrm{D_e}}^{(i)})$. Each $C_{\mathrm{D_e}}^{(i)}$ has a weight distribution polynomial $B^{(i)}(x)$ defined as

$$B^{(i)}(x) = \sum_{j=d_1}^{n_1+n_2} B_j^{(i)} x^j \tag{21}$$

where, the coefficient $B_d^{(i)}$ denotes the number of joint codewords $(\mathbf{c}_1, \mathbf{c}_2^{(i)})$ with Hamming weight $d^{(i)}$ for $d_1 \leq d^{(i)} \leq n_1+n_2$. Each code has a minimum Hamming distance, denoted $d_{\min}^{(i)}$, defined by

$$d_{\min}^{(i)} = \min_j \{\, j \mid B_j^{(i)} > 0,\ i \in \mathcal{I} \,\}. \tag{22}$$

The maximum minimum distance among all the subcodes is called the free distance of the ensemble and is given by $d_{\min} = d(C_{\mathrm{D_e}}^{(i^{\mathrm{opt}})}) = \max_{i\in\mathcal{I}}\{d(C_{\mathrm{D_e}}^{(i)})\}$. Once the optimization process is over, we denote the resulting code as $C_{\mathrm{D_e}}$ with free distance $d_{\min}$, omitting the index i^{opt}. Therefore, $C_{\mathrm{D_e}}$ is an $[n_1+n_2, k_1, d_{\min}]$ code.

4.1 The Full Search Method

When the binomial coefficient $\binom{k_1}{k_2}$ is small, a full search over all the candidate codes $C_{\mathrm{D_e}}^{(i)}$, $i \in \mathcal{I}$, becomes computationally feasible and directly yields the optimum code $C_{\mathrm{D_e}}^{(i^{\mathrm{opt}})}$. The detailed steps of this procedure are outlined in Algorithm 1.

4.1.1 A Design Example of the Full Search Method

Consider a Goppa coded cooperative (GCC) scheme which employs the binary Goppa codes $C_{\mathrm{S_o}}(14,6,5)$ and $C_{\mathrm{R_e}}(12,4,5)$ at the source and relay nodes respectively. Both codes are constructed over GF(16) with primitive polynomial $p(x) = x^4 + x + 1$. Specifically, $C_{\mathrm{S_o}}$ is defined by the Goppa polynomial $G_S(x) = x^2 + x + \xi^3$ over the support $\mathcal{L}_S = \{\xi^0, \xi^1, \ldots, \xi^{13}\}$, while C_R is defined by $G_R(x) = x^2 + x + \xi^6$ over the support $\mathcal{L}_R = \{\xi^0, \xi^1, \ldots, \xi^{11}\}$, where ξ is a primitive element of GF(16). The generator matrices $\boldsymbol{\mathcal{G}}_S$ and $\boldsymbol{\mathcal{G}}_R$ are obtained from the corresponding parity-check matrices via standard row reduction over GF(2). The resulting destination code $C_{\mathrm{D_e}}$ has length $n_1+n_2 = 26$ and contains $2^{k_1} = 64$ codewords. Since $k_1 = 6$ and $k_2 = 4$, there are $\binom{k_1}{k_2} = \binom{6}{4} = 15$ information selection patterns as follows;

$$\begin{aligned}\Psi &= \{\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6, \Phi_7, \Phi_8, \Phi_9, \Phi_{10}, \Phi_{11}, \\ &\quad \Phi_{12}, \Phi_{13}, \Phi_{14}, \Phi_{15}\} \\ &= \big\{[1,2,3,4], [1,2,3,5], [1,2,3,6], [1,2,4,5], \\ &\quad [1,2,4,6], [1,2,5,6], [1,3,4,5], [1,3,4,6], \\ &\quad [1,3,5,6], [1,4,5,6], [2,3,4,5], [2,3,4,6], \\ &\quad [2,3,5,6], [2,4,5,6], [3,4,5,6]\big\}.\end{aligned}$$

The weight distribution polynomial $B^{(i)}(x)$ and minimum distance $d_{\min}$ of the resulting destination code $C_{\mathrm{D_e}}^{(i)}(26,6)$ are computed and listed in Tab. 2. From Tab. 2, the selection patterns Φ_6, Φ_9 and Φ_{10} results to a destination code with a minimum distance $d_{\min} = 6 > d_1 = 5$. This asserts that the subcode construction can strictly improve the minimum distance of the source code. The rest of the patterns retain $d_{\min} = d_1 = 5$, confirming that not all selection patterns yield an improvement. Among the patterns Φ_6, Φ_9 and Φ_{10}, a further comparison via the weight spectrum reveals that pattern Φ_9 has fewer low weight codewords as compared to Φ_6 and Φ_{10} as shown in Tab. 3. This leads to a better BER performance [37]. Thus, Φ_9 is the unique optimum pattern, yielding the destination code $C_{\mathrm{D_e}}(26,6,6)$. While the full search method guarantees an optimally designed relay code, its practicality diminishes as the binomial coefficient $\binom{k_1}{k_2}$ grows exponentially with k_1 and peaks at $\lfloor k_1/2 \rfloor$. This exponential growth renders the full search method computationally infeasible for large k_1 and thus the need for a practical strategy that restricts the search to a strategically chosen subset of the $\binom{k_1}{k_2}$ candidates. By exploiting the recursive binary partitioning of the k_1 decoded message bits, the target search identifies selection patterns that are most likely to preserve or improve the minimum distance of the destination code, achieving a favourable trade-off between search complexity and code performance.

4.2 The Targeted Search Method

A large binomial coefficient $\binom{k_1}{k_2}$ renders a full search computationally prohibitive. We therefore propose a target search over the promising candidates $C_{\mathrm{D_e}}^{(i)}$, $i \in \mathcal{I}$, based on a recursive binary partitioning strategy. Specifically, the k_1 decoded message bits at the relay are first split into two nearly equal halves with the midpoint bit preselected, and this partitioning is applied recursively to each resulting half, progressively refining the search until 2^p disjoint intervals and $2^p - 1$ preselected bits are obtained, as shown in Figs. 4 and 5. The specific steps of the targeted search method are shown in Algorithm 2. A clear performance advantage emerges when $d_{\min} > d_1$, as the increased minimum distance and redundancy of $C_{\mathrm{D_e}}$ translate directly into superior BER performance relative to $C_{\mathrm{S_o}}$. It is equally important to recognise, however, that even when the minimum Hamming distance of $C_{\mathrm{D_e}}$ does not exceed d_1, the sub-code construction still delivers a measurable benefit by substantially reducing the number of low-weight codewords in $C_{\mathrm{D_e}}^{(i)}$ across all i. In this sense, the weight spectrum is always improved, regardless of whether the minimum distance is. The combined effect of these two optimisation criteria; minimum distance and weight spectrum, solidifies the BER superiority of $C_{\mathrm{D_e}}$ over $C_{\mathrm{S_o}}$, complemented further by the cooperative diversity gain.

i	Φ_j	$C_{\mathrm{D_e}}^{(i)}(26,6)$	$d_{\min}^{(i)}$	The weight polynomial: $\mathrm{B}^{(i)}(x)$
1	Φ_1	$C_D^{(1)}(26,6)$	5	$1{+}x^5\ {+}2x^6{+}0x^7{+}0x^8{+}0x^9{+}5x^{10}{+}7x^{11}\ {+}7x^{12}\ {+}13x^{13}{+}8x^{14}\ {+}7x^{15}\ {+}8x^{16}\ {+}x^{17}\ {+}2x^{18}{+}2x^{19}$
2	Φ_2	$C_D^{(2)}(26,6)$	5	$1{+}x^5\ {+}x^6\ {+}x^7\ {+}0x^8{+}0x^9{+}3x^{10}{+}9x^{11}\ {+}11x^{12}{+}10x^{13}{+}6x^{14}\ {+}8x^{15}\ {+}8x^{16}\ {+}x^{17}\ {+}2x^{18}{+}2x^{19}$
3	Φ_3	$C_D^{(3)}(26,6)$	5	$1{+}2x^5{+}x^6\ {+}0x^7{+}0x^8{+}0x^9{+}4x^{10}{+}9x^{11}\ {+}9x^{12}\ {+}9x^{13}\ {+}6x^{14}\ {+}9x^{15}\ {+}10x^{16}{+}x^{17}\ {+}x^{18}\ {+}2x^{19}$
4	Φ_4	$C_D^{(4)}(26,6)$	5	$1{+}x^5\ {+}x^6\ {+}x^7\ {+}0x^8{+}0x^9{+}x^{10}\ {+}10x^{11}{+}11x^{12}{+}10x^{13}{+}12x^{14}{+}4x^{15}\ {+}4x^{16}\ {+}5x^{17}{+}2x^{18}{+}x^{19}$
5	Φ_5	$C_D^{(5)}(26,6)$	5	$1{+}2x^5{+}x^6\ {+}0x^7{+}0x^8{+}0x^9{+}2x^{10}{+}10x^{11}{+}9x^{12}\ {+}9x^{13}\ {+}12x^{14}{+}5x^{15}\ {+}6x^{16}\ {+}5x^{17}{+}x^{18}\ {+}x^{19}$
6	Φ_6	$C_D^{(6)}(26,6)$	**6**	$1{+}0x^5{+}3x^6{+}0x^7{+}0x^8{+}0x^9{+}6x^{10}{+}6x^{11}\ {+}8x^{12}\ {+}12x^{13}{+}7x^{14}\ {+}8x^{15}\ {+}7x^{16}\ {+}4x^{17}{+}0x^{18}{+}2x^{19}$
7	Φ_7	$C_D^{(7)}(26,6)$	5	$1{+}2x^5{+}x^6\ {+}0x^7{+}0x^8{+}0x^9{+}2x^{10}{+}8x^{11}\ {+}11x^{12}{+}11x^{13}{+}10x^{14}{+}7x^{15}\ {+}4x^{16}\ {+}3x^{17}{+}3x^{18}{+}x^{19}$
8	Φ_8	$C_D^{(8)}(26,6)$	5	$1{+}x^5\ {+}x^6\ {+}x^7\ {+}0x^8{+}0x^9{+}3x^{10}{+}8x^{11}\ {+}9x^{12}\ {+}12x^{13}{+}10x^{14}{+}6x^{15}\ {+}6x^{16}\ {+}3x^{17}{+}2x^{18}{+}x^{19}$
9	Φ_9	$C_D^{(9)}(26,6)$	**6**	$1{+}0x^5{+}2x^6{+}0x^7{+}x^8\ {+}0x^9{+}7x^{10}{+}5x^{11}\ {+}6x^{12}\ {+}13x^{13}{+}10x^{14}{+}9x^{15}\ {+}4x^{16}\ {+}3x^{17}{+}x^{18}\ {+}2x^{19}$
10	Φ_{10}	$C_D^{(10)}(26,6)$	**6**	$1{+}0x^5{+}3x^6{+}0x^7{+}0x^8{+}0x^9{+}6x^{10}{+}5x^{11}\ {+}7x^{12}\ {+}12x^{13}{+}10x^{14}{+}10x^{15}{+}4x^{16}\ {+}4x^{17}{+}x^{18}\ {+}x^{19}$
11	Φ_{11}	$C_D^{(11)}(26,6)$	5	$1{+}2x^5{+}x^6\ {+}0x^7{+}0x^8{+}0x^9{+}3x^{10}{+}7x^{11}\ {+}13x^{12}{+}9x^{13}\ {+}10x^{14}{+}7x^{15}\ {+}2x^{16}\ {+}5x^{17}{+}2x^{18}{+}2x^{19}$
12	Φ_{12}	$C_D^{(12)}(26,6)$	5	$1{+}2x^5{+}0x^6{+}0x^7{+}x^8\ {+}0x^9{+}4x^{10}{+}6x^{11}\ {+}12x^{12}{+}10x^{13}{+}10x^{14}{+}8x^{15}\ {+}2x^{16}\ {+}4x^{17}{+}2x^{18}{+}2x^{19}$
13	Φ_{13}	$C_D^{(13)}(26,6)$	5	$1{+}2x^5{+}x^6\ {+}0x^7{+}0x^8{+}0x^9{+}5x^{10}{+}4x^{11}\ {+}10x^{12}{+}15x^{13}{+}9x^{14}\ {+}5x^{15}\ {+}5x^{16}\ {+}3x^{17}{+}x^{18}\ {+}3x^{19}$
14	Φ_{14}	$C_D^{(14)}(26,6)$	5	$1{+}x^5\ {+}x^6\ {+}0x^7{+}0x^8{+}x^9\ {+}6x^{10}{+}6x^{11}\ {+}7x^{12}\ {+}11x^{13}{+}12x^{14}{+}8x^{15}\ {+}4x^{16}\ {+}3x^{17}{+}x^{18}\ {+}2x^{19}$
15	Φ_{15}	$C_D^{(15)}(26,6)$	5	$1{+}2x^5{+}x^6\ {+}0x^7{+}0x^8{+}0x^9{+}3x^{10}{+}9x^{11}\ {+}9x^{12}\ {+}11x^{13}{+}10x^{14}{+}5x^{15}\ {+}6x^{16}\ {+}3x^{17}{+}2x^{18}{+}2x^{19}$

Tab. 2. Minimum distance & weight spectra of destination codes $C_D^{(i)}(26,6)$ for all selection patterns.

i	Φ_j	$C_D^{(i)}(26,6)$	$d_{min}^{(i)}$	The weight polynomial: $\mathrm{B}^{(i)}(x)$
6	Φ_6	$C_D^{(6)}(26,6)$	6	$1{+}0x^5{+}3x^6{+}0x^7{+}0x^8{+}0x^9{+}6x^{10}{+}6x^{11}{+}8x^{12}{+}12x^{13}{+}7x^{14}\ {+}8x^{15}\ {+}7x^{16}{+}4x^{17}{+}0x^{18}{+}2x^{19}$
9	Φ_9	$C_D^{(9)}(26,6)$	**6**	$1{+}0x^5{+}\mathbf{2}x^6{+}0x^7{+}x^8\ {+}0x^9{+}7x^{10}{+}5x^{11}{+}6x^{12}{+}13x^{13}{+}10x^{14}{+}9x^{15}\ {+}4x^{16}{+}3x^{17}{+}x^{18}\ {+}2x^{19}$
10	Φ_{10}	$C_D^{(10)}(26,6)$	6	$1{+}0x^5{+}3x^6{+}0x^7{+}0x^8{+}0x^9{+}6x^{10}{+}5x^{11}{+}7x^{12}{+}12x^{13}{+}10x^{14}{+}10x^{15}{+}4x^{16}{+}4x^{17}{+}x^{18}\ {+}x^{19}$

Tab. 3. Destination codes $C_{\mathrm{D_e}}^{(i)}(26,6)$ with improved $d_{\min}$.

Algorithm 1. Full search for the optimum code.

Require: Index set $\mathcal{I}$, parameter set Ψ
Ensure: Optimum code $C_{\mathrm{D_e}}(n_1+n_2, k_1, d_{\min})$
for all $i \in \mathcal{I}$ **do**
  for all $\Phi_i \in \Psi$ **do**
    Determine all candidate codes $C_{\mathrm{D_e}}^{(i)}(n_1+n_2, k_1)$
    Compute the weight-distribution polynomial $B^{(i)}(X)$
  end for
end for
Compute

$$d_{\min}^{(\max)} = \max\left\{d_{\min}^{(i)} \mid i \in \mathcal{I}\right\}$$

Define

$$\mathcal{I}_0 = \left\{i \in \mathcal{I} \mid d_{\min}^{(i)} = d_{\min}^{(\max)}\right\}$$
$$\Psi_0 = \{\Phi_i \in \Psi \mid i \in \mathcal{I}_0\}$$

if $|\Psi_0| = 1$ **then**

  return optimum code $C_{\mathrm{D_e}}(n_1+n_2, k_1, d_{\min})$
end if
Set $j \leftarrow 0$
while $|\Psi_j| > 1$ **and** $d_1 \le d_{\min}^{(\max)} + j \le n_1$ **do**
  Compute

$$B^{(\min)}_{d_{\min}^{(\max)}+j} = \arg\min_{i\in\mathcal{I}_j}\left\{B^{(i)}_{d_{\min}^{(\max)}+j} \mid i \in \mathcal{I}_j\right\}$$

  Update

$$\mathcal{I}_{j+1} = \left\{i \in \mathcal{I}_j \mid B^{(i)}_{d_{\min}^{(\max)}+j} = B^{(\min)}_{d_{\min}^{(\max)}+j}\right\}$$
$$\Psi_{j+1} = \left\{\Phi_i \in \Psi_j \mid i \in \mathcal{I}_{j+1}\right\}$$

  if $|\Omega_{i+1}| = 1$ **then**

    return optimum code $C_{\mathrm{D_e}}(n_1+n_2, k_1, d_{\min})$
  end if
  $j \leftarrow j+1$
end while

Algorithm 2. Targeted search method.

Require: $\hat{\mathbf{m}}_1 \in \mathbb{F}_2^{k_1}$, k_2, $p \in \mathbb{N}$ such that $2^p \le \lfloor k_2/2 \rfloor < 2^{p+1}$, $\mathcal{G}_S$, d_1, d_2, n_1+n_2
Ensure: Optimal selection-pattern set $\bar{\Psi}_i$
Split $\hat{\mathbf{m}}_1$ into two nearly equal halves and pre-select the symbol at position $\lfloor (k_1+1)/2 \rfloor$.
Repeat the bisection process p times to obtain 2^p disjoint intervals and $2^p - 1$ pre-selected bits.
for $\ell = 1$ **to** $k_2 - 2^p + 1$ **do**
  Assign the ℓ-th remaining bit to the next interval and store the resulting pattern in $\bar{\Psi}$.
end for
$\bar{\Psi}_{-1} \leftarrow \bar{\Psi}$
$i \leftarrow 0$
repeat
  Construct the candidate set

$$\Lambda_i = \left\{m_j \in \mathbb{F}_2^{k_1} \;\middle|\; \begin{array}{l} m_j\hat{\mathcal{G}}_S = c_j, \\ \mathrm{wt}(c_j) = d_1 + i,\ j = 1, \ldots, 2^{k_1} - 1 \end{array}\right\}$$

  Apply each pattern in $\bar{\Psi}_{i-1}$ to Δ_i.
  Update $\bar{\Psi}_i$ by retaining the patterns that minimise the number of codewords satisfying

$$\mathrm{wt}([c_1, c_2]) = d_1 + d_2 + i.$$

  $i \leftarrow i+1$
until $|\bar{\Psi}_{i-1}| = 1$ **or** $d_1 + i > n_1$
return $\bar{\Psi}_{i-1}$

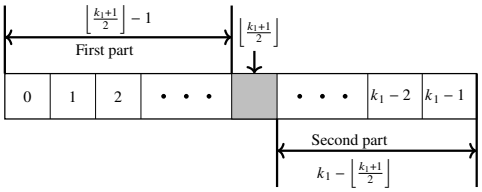


Fig. 4. First-level binary partitioning.

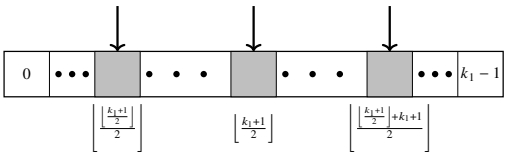


Fig. 5. Second-level binary partitioning.

4.2.1 Illustrative Example of the Target Search Method

Consider the Goppa coded cooperative (GCC) scheme employing the binary Goppa codes $C_{\mathrm{S_o}}(36, 24, 5)$ and $C_{\mathrm{R_e}}(22, 10, 5)$ at the source and relay nodes respectively. The codes are defined over $GF(2^6)$ with primitive polynomial $p(x) = x^6 + x + 1$, defined by $G_S(x) = x^2 + x + \xi^5$ over $\mathcal{L}_S = \{\xi^0, \ldots, \xi^{35}\}$ and $G_R(x) = x^2 + x + \xi^{10}$ over $\mathcal{L}_R = \{\xi^0, \ldots, \xi^{21}\}$.

Phase 1 – Recursive division of $\hat{m}_1$:

Since $2^2 \le \lfloor 10/2 \rfloor < 2^3$, $p = 2$

1. Preselect $\lfloor 25/2 \rfloor = 12 - th$ bit, giving $\mathcal{H}_L = \{1, \ldots, 11\}$ and $\mathcal{H}_R = \{13, \ldots, 24\}$.
2. Preselect $\lfloor 12/2 \rfloor = 6 - th$ and $\lfloor 38/2 \rfloor = 19 - th$ bits, yielding four intervals $\mathcal{I}_1 = \{1, \ldots, 5\}$, $\mathcal{I}_2 = \{7, \ldots, 11\}$, $\mathcal{I}_3 = \{13, \ldots, 18\}$, $\mathcal{I}_4 = \{20, \ldots, 24\}$.

The remaining $k_2 - 2^p + 1 = 7$ bits are distributed as follows: **2** bits from each of $\mathcal{I}_1$, $\mathcal{I}_2$, $\mathcal{I}_3$, and **1** bit from $\mathcal{I}_4$, giving

$$|\bar{\Psi}| = \binom{5}{2}\binom{5}{2}\binom{6}{2}\binom{5}{1} = 10 \times 10 \times 15 \times 5 = 7{,}500$$

selection patterns denoted as $\bar{\Psi} = \{\Phi_1,\ \Phi_2,\ \cdots,\ \Phi_{7500}\}$.

Phase 2 – search for the optimal selection pattern:

1. $\Delta_0 = \{m_j \mid \mathrm{wt}(m_j G_S) = d_1 = 5\}$; $|\Delta_0| = 103$ information vectors.
2. Applying all $\bar{\Psi}$ selection patterns to Δ_0 and check for minimum $A_{d_1+d_2} = B_{10}$. The minimum is $A_{10} = 2$, achieved by $|\bar{\Psi}_0| = 6$ patterns; $\bar{\Psi}_0 = \{\Phi_{65},\ \Phi_{70},\ \Phi_{515},\ \Phi_{520},\ \Phi_{3065},\ \Phi_{3515}\}$.
3. Since $|\bar{\Psi}_0| = 6 > 1$, proceed to $i = 1$: construct $\Delta_1 = \{m_j \mid \mathrm{wt}(m_j G_S) = 6\}$ with $|\Delta_1| = 529$ and apply the patterns $\bar{\Psi}_0$ to Δ_1. Check for minimum B_{11} and record the corresponding pattern. Update $\bar{\Psi}_0$ to $\bar{\Psi}_1$. In this case $\bar{\Psi}_1 = \{\Phi_{3515}\}$.
4. Since $|\bar{\Psi}_1| = 1$, the search is complete.

The unique optimum selection pattern is

$$\Phi_{i^{\text{sub-opt}}} = \Phi_{3515} = [2, 3, 6, 8, 11, 12, 16, 17, 19, 24].$$

The target search evaluated only 7,500 patterns compared to $\binom{24}{10}$ = 1,961,256 for the full search. This is a decrease of over 99.6% of the number of selection patterns confirming the reduced search complexity of the proposed target search method.

4.3 Complexity Analysis of the Two Relay Information Search Algorithms

For the full search, every $\Phi_i \in \Psi$, $i \in \mathcal{I}$, requires encoding every candidate source message $m_1 \in \mathbb{F}_2^{k_1}$ and its corresponding relay message $m_2 = m_1[\Phi_i]$ to obtain the weight distribution polynomial $B^{(i)}(x)$. This leads to an overall complexity of

$$O_{\text{full}} = O\left(\binom{k_1}{k_2} 2^{k_1}\, k_2 n_2\right), \tag{23}$$

which grows exponentially in k_1 and becomes computationally infeasible for large values of k_1, since $\binom{k_1}{k_2}$ itself peaks combinatorially at $k_2 = \lfloor k_1/2 \rfloor$ and is compounded by the 2^{k_1} enumeration of the full message space. On the other hand, the target search avoids both sources of growth. In the recursive bisection phase, only

$$|\bar{\Psi}| = \prod_{j=1}^{2^p} \binom{|I_j|}{\ell_j} \tag{24}$$

candidate patterns are generated, where I_j are the 2^p disjoint bisected intervals and ℓ_j is the number of remaining bits assigned to interval I_j. Since each $|I_j| \ll k_1$, the product $|\bar{\Psi}|$ is combinatorially far smaller than $\binom{k_1}{k_2}$. In Phase 2, each surviving pattern set $\bar{\Psi}_{i-1}$ is tested only against the near-minimum-weight subset

$$\Delta_i = \left\{ m_j \in \mathbb{F}_2^{k_1} \;\middle|\; \text{wt}(m_j G_S) = d_1 + i \right\}, \tag{25}$$

rather than the full 2^{k_1} message space, since $|\Delta_i| \ll 2^{k_1}$ for the low-order terms i at which the search typically terminates. The resulting overall complexity of the target search is therefore

$$O_{\text{target}} = O\left(|\bar{\Psi}| \left(\sum_i |\Delta_i|\right) k_2 n_2\right) \tag{26}$$

where the summation runs only over the iterations $i = 0, 1, \ldots$ executed before the termination condition $|\bar{\Psi}_{i-1}| = 1$ (or $d_1 + i > n_1$) in Algorithm 2 is met.

5. Joint Decoding

This section describes the decoding procedures for both a general joint linear block code and a joint sub-code of a Goppa code at the destination node. The decoders used at the source and relay nodes are denoted by $C_{\text{So}}-$decoder and $C_{\text{Re}}-$decoder, respectively.

5.1 Decoding of the General Joint Linear Block Code

For the general case, two joint decoding algorithms are employed: the smart decoding algorithm [18] and the naive decoding algorithm [20].

5.2 Decoding of the Joint Subcode of the Goppa Code

From Sec. 3.1.2, the source and relay component codes can be selected so as to induce a joint subcode C_{D_e} contained in a Goppa code $\Gamma_{\text{D}_\text{e}}$ at the destination node. Since binary Goppa codes may be viewed as subfield subcodes of suitable Generalized Reed–Solomon (GRS) codes, it is natural to exploit a GRS-based algebraic decoding framework for their recovery [30], [38]. In the proposed approach, the transmitted codeword is binary, but the decoding stage is carried out in the extension field $\mathbb{F}_{2^m}$. Specifically, after demodulation, the received binary sequence is regrouped according to the chosen basis representation of $\mathbb{F}_{2^m}$ to form a received vector $\mathbf{r} \in \mathbb{F}_{2^m}^n$. Owing to channel errors, the coordinates of $\mathbf{r}$ are not necessarily restricted to the binary subfield $\mathbb{F}_2$. The EEA–based GRS decoder then computes the syndrome polynomial $S(x)$, the error-locator polynomial $\Lambda(x)$, and the error-evaluator polynomial $\Omega(x)$, all over $\mathbb{F}_{2^m}$. These polynomials satisfy the key equation

$$\Omega(x) \equiv \Lambda(x) S(x) \pmod{G(x)}.$$

The corresponding error values are obtained as

$$e_i = \frac{\Omega(\gamma_i)}{\Lambda'(\gamma_i)}. \tag{27}$$

Since the decoding process is performed over $\mathbb{F}_{2^m}$, the estimated decoded codeword $\hat{\mathbf{c}}$ may contain coordinates that are valid extension-field symbols but do not belong to the binary subfield $\mathbb{F}_2$. As a result, $\hat{\mathbf{c}}$ need not be a valid binary Goppa codeword. To address this issue, we propose a post-processing heuristic that replaces such non-binary coordinates in $\hat{\mathbf{c}}$ with binary candidates in a parity-consistent manner, thereby producing a corrected binary estimate $\bar{\mathbf{c}}$. By combining EEA-based GRS decoding with this localized binary projection step, we obtain a decoder that is almost identical to maximum-likelihood decoding (MLD), but with a significantly reduced candidate search space. We refer to this decoder as the Extended Euclidean Algorithm–Localized Maximum Likelihood (EEA-LML) decoder. Suppose that the decoded codeword after the euclidean based decoding is

$$\hat{c}_t = (\hat{c}_0,\ \hat{c}_1,\ \ldots,\ \hat{c}_{j_1},\ \ldots, \hat{c}_{j_2}, \ldots, \hat{c}_{j_t}, \ldots,\ \hat{c}_{n-1})$$

where $\hat{c}_i \notin \mathbb{F}_2 \Leftrightarrow i \in \left\{ j_1,\ j_2,\ \ldots,\ j_t \right\}$ with

$$0 \le j_1 < j_2 < \ldots < j_t \le n-1, \quad 1 \le t \le n.$$

More specifically,

$$\hat{c}_{j_\ell} = (\hat{c}_{j_{\ell,0}}, \hat{c}_{j_{\ell,1}}, \ldots, \hat{c}_{j_{\ell,m-1}}) \in \mathbb{F}_2^m \setminus \{0,1\}$$

for $\ell = 1, 2, \ldots, t$. Denote $\hat{b}_t$ as the vector

$$\hat{b}_t = (\hat{c}_{j_{1,0}}, \hat{c}_{j_{2,0}}, \ldots, \hat{c}_{j_{t,0}}).$$

Evidently, $\hat{b}_t \in \mathbb{F}_2^t$. Let $\widetilde{c}_t$ be the vectors

$$\widetilde{c}_t = (\hat{c}_0,\ \hat{c}_1,\ \ldots,\ \widetilde{c}_{j_1},\ \ldots, \widetilde{c}_{j_2}, \ldots, \widetilde{c}_{j_t}, \ldots,\ \hat{c}_{n-1})$$

where

$$(\widetilde{c}_{j_1},\ \widetilde{c}_{j_2}, \ldots, \widetilde{c}_{j_t}) \in \mathbb{F}_2^t,$$

is denoted as $\widetilde{d}_t$. Let Λ be the set as

$$\Lambda = \{\widetilde{c}_t | \mathbf{H}_{\mathbf{\Gamma}(\mathbf{L},\mathbf{G})} \widetilde{c}_t^{\mathrm{T}} = 0\}.$$

Clearly, $0 \le |\Lambda| \le 2^t$. The following cases are considered:

1. If $|\Lambda| = 0$, then Λ is an empty set and we have

$$(s_{j_1}, s_{j_2}, \ldots, s_{j_t}) = \arg \min_{\widetilde{d}_t \in \mathbb{F}_2^t} \{d_H(\widetilde{d}_t, \hat{b}_t)\}.$$

2. If $|\Lambda| = 1$, then Λ is a set of single element and $(s_{j_1}, s_{j_2}, \ldots, s_{j_t})$ is obtained directly, i.e.,

$$(s_{j_1}, s_{j_2}, \ldots, s_{j_t}) = (\widetilde{c}_{j_1}, \widetilde{c}_{j_2}, \ldots, \widetilde{c}_{j_t}).$$

3. If $2 \le |\Lambda| \le 2^t$, then

$$(s_{j_1}, s_{j_2}, \ldots, s_{j_t}) = \arg \min_{\widetilde{c}_t \in \Lambda} \{d_H(\widetilde{d}_t, \hat{b}_t)\}.$$

Finally, the modified decoded codeword is

$$\overline{c} = (\hat{c}_0, \hat{c}_1, \ldots, s_{j_1}, \ldots, s_{j_1}, \ldots, s_{j_t}, \ldots, \hat{c}_{n-1}).$$

Tables 4, 5 and 6 shows different syndrome patterns for $t = 1$ non-binary symbol, $t = 2$ non-binary symbols and $3 \le t \le \lfloor \frac{d-1}{2} \rfloor$ non-binary symbols respectively. The symbol Σ is used to represent a non zero syndrome.i.e., $\mathbf{H}\widetilde{c}_t^{\mathrm{T}} \triangleq \Sigma$ if $\mathbf{H}\widetilde{c}_t^{\mathrm{T}} \neq 0$.

$\widetilde{c}_{j_1}$	Syndromes			
0	0	Σ	0	Σ
1	0	0	Σ	Σ

Tab. 4. Syndrome patterns for $t = 1$ symbol.

$\widetilde{c}_{j_1}$	$\widetilde{c}_{j_2}$	Syndromes									
0	0	0	Σ	0	Σ	0	Σ	0	...	0	Σ
1	0	0	0	Σ	Σ	0	0	Σ	...	Σ	Σ
0	1	0	0	0	0	Σ	Σ	Σ	...	Σ	Σ
1	1	0	0	0	0	0	0	0	...	Σ	Σ

Tab. 5. Syndrome patterns for $t = 2$ symbols.

The specific steps of the proposed EEA-LML decoding procedure are summarized below.

Step 1. Apply the Extended Euclidean Algorithm (EEA)-based decoding to the received vector $\mathbf{r} \in \mathbb{F}_2^n$ to obtain the estimated codeword $\hat{\mathbf{c}}$. Identify the set of non-binary positions

$$\mathcal{J} = \{j_1 < j_2 < \cdots < j_t\} \subseteq \{0, 1, \ldots, n-1\} \quad (28)$$

such that $\hat{c}_{j_\ell} \in \mathbb{F}_2^m \setminus \{0,1\}$ for each $\ell = 1, \ldots, t$, where each non-binary entry is an m-bit vector that does not correspond to a valid binary symbol.

Step 2. Construct a binary reference vector $\hat{\mathbf{b}}_t \in \mathbb{F}_2^t$ by extracting the first bit entry from each non-binary position in $\mathcal{J}$:

$$\hat{\mathbf{b}} = \left(\hat{c}_{j_1,0},\ \hat{c}_{j_2,0},\ \ldots,\ \hat{c}_{j_t,0}\right) \in \mathbb{F}_2^t \quad (29)$$

where $\hat{c}_{j_\ell,0}$ denotes the first binary entry of the m-bit vector $\hat{c}_{j_\ell}$.

Step 3. Form the corrected estimate $\widetilde{\mathbf{c}}_t$ by replacing each non-binary entry $\hat{c}_{j_\ell}$ with a binary value $\widetilde{c}_{j_\ell} \in \mathbb{F}_2$, and let $\widetilde{\mathbf{d}}_t = (\widetilde{c}_{j_1}, \widetilde{c}_{j_2}, \ldots, \widetilde{c}_{j_t}) \in \mathbb{F}_2^t$ denote the vector of substituted values. Construct the syndrome-valid candidate set

$$\Lambda = \left\{\widetilde{\mathbf{c}}_t \;\middle|\; \mathbf{H}\widetilde{\mathbf{c}}_t^{\top} = \mathbf{0}\right\}, \quad (30)$$

comprising all binary completions of $\hat{\mathbf{c}}$ that satisfy the parity-check constraint.

Step 4. Select the optimal binary substitution $\widetilde{\mathbf{d}}_t^* \in \mathbb{F}_2^t$ according to the cardinality of Λ:

- **Case 1** ($|\Lambda| = 0$): No syndrome-valid candidate exists. Select $\widetilde{\mathbf{d}}^*$ as the binary vector minimising the Hamming distance to the reference:

$$\widetilde{\mathbf{d}}^* = \arg\min_{\widetilde{\mathbf{d}}_t \in \mathbb{F}_2^t} d_H\left(\widetilde{\mathbf{d}}_t,\ \hat{\mathbf{b}}_t\right). \quad (31)$$

- **Case 2** ($|\Lambda| = 1$): A unique syndrome-valid candidate exists. Set $\widetilde{\mathbf{d}}^*$ to be the unique element of Λ restricted to the positions in $\mathcal{J}$.
- **Case 3** ($2 \le |\Lambda| \le 2^t$): Multiple syndrome-valid candidates exist. Select the one closest to the binary reference in Hamming distance:

$$\widetilde{\mathbf{d}}^* = \arg\min_{\widetilde{\mathbf{c}}_t \in \Lambda} d_H\left(\widetilde{\mathbf{d}}_t,\ \hat{\mathbf{b}}_t\right). \quad (32)$$

Step 5. Reconstruct the final binary codeword estimate $\bar{\mathbf{c}} \in \mathbb{F}_2^n$ by substituting the selected values $\widetilde{\mathbf{d}}^* = (s_{j_1}, s_{j_2}, \ldots, s_{j_t})$ into the non-binary positions of $\hat{\mathbf{c}}$:

$$\bar{\mathbf{c}} = \left(\hat{c}_0, \ldots, s_{j_1}, \ldots, s_{j_2}, \ldots, s_{j_t}, \ldots, \hat{c}_{n-1}\right), \quad (33)$$

$\widetilde{c}_{j_1}$	$\widetilde{c}_{j_2}$	$\widetilde{c}_{j_3}$	$\cdots$	$\widetilde{c}_{j_t}$	Syndromes									
0	0	0	$\cdots$	0	0	Σ	0	0	0	$\cdots$	0	0	0	Σ
1	0	0	$\cdots$	0	0	0	Σ	Σ	0	$\cdots$	0	0	Σ	Σ
0	1	0	$\cdots$	0	0	0	0	Σ	Σ	$\cdots$	0	Σ	Σ	Σ
0	0	1	$\cdots$	0	0	0	0	0	Σ	$\cdots$	Σ	Σ	Σ	Σ
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	1	$\cdots$	1	0	0	0	0	0	$\cdots$	Σ	Σ	Σ	Σ

Tab. 6. Syndrome patterns for $3 \le t \le \lfloor \frac{d-1}{2} \rfloor$ symbols.

where all binary positions in $\hat{\mathbf{c}}$ are retained unchanged and the non-binary positions $\mathcal{J}$ are replaced by the corrections $(s_{j_1}, \ldots, s_{j_t})$ obtained from Step 4.

However since $C_{\mathrm{De}} \subsetneq \Gamma_{\mathrm{De}}$, the EEA-LML decoder may return a valid Goppa codeword $\bar{\mathbf{c}} \in \Gamma_{\mathrm{De}} \setminus C_{\mathrm{De}}$. In this case, we invoke a localized joint search over C_{De}. Let $\mathbf{m}_1^{(0)}$ denote the message estimate obtained from the decoded source component, and let $\mathcal{I}_\ell$ contain the ℓ least reliable message positions, selected using the soft values $|z_i|$. We then form the candidate set

$$\mathcal{M}_\ell = \left\{ \mathbf{m}_1^{(0)} + \mathbf{e} : \mathrm{supp}(\mathbf{e}) \subseteq \mathcal{I}_\ell \right\}, \qquad |\mathcal{M}_\ell| = 2^\ell, \tag{34}$$

encode each $\mathbf{m}_1 \in \mathcal{M}_\ell$ into C_{De}, and choose the candidate with the largest binary phase shift keying (BPSK) correlation metric. The pseudocode for the three stage joint decoder are outlined in Algorithm 3.

Algorithm 3. EEA-LML decoder for $C_{\mathrm{De}} \subsetneq \Gamma_{\mathrm{De}}$.

Require: Goppa code $\Gamma_{\mathrm{De}} = \Gamma(\mathcal{L}_{\mathrm{De}}, G)$; joint subcode $C_{\mathrm{De}} \subsetneq \Gamma_{\mathrm{De}}$; selection pattern Φ; generator matrices $\mathcal{G}_S, \mathcal{G}_R$; parity- check matrix $\mathbf{H}_{\mathrm{De}}$; received vector $\mathbf{r} \in \mathbb{F}_{2^m}^{n_1+n_2}$; reliability vector $\mathbf{z} \in \mathbb{R}^{n_1+n_2}$; localized search size ℓ.
Ensure: Decoded message sequence $\hat{\mathbf{m}}_1 \in \mathbb{F}_2^{k_1}$
Stage 1: EEA-based GRS decoding and binary projection
$\bar{\mathbf{c}} \leftarrow \text{EEA-LML}(\Gamma_{\mathrm{De}}, \mathbf{r}, \mathbf{H}_{\mathrm{De}})$ $\{\bar{\mathbf{c}} \in \mathbb{F}_2^{n_1+n_2}\}$
$\bar{\mathbf{c}}_1 \leftarrow \bar{\mathbf{c}}_{[1:n_1]}$
$\bar{\mathbf{c}}_2 \leftarrow \bar{\mathbf{c}}_{[n_1+1:n_1+n_2]}$
$\bar{\mathbf{m}}_1 \leftarrow \bar{\mathbf{c}}_{1,\mathcal{I}_S}$ {$\mathcal{I}_S$ denotes the source information set}
Stage 2: Validity test of $\bar{\mathbf{c}}$ *in* C_{De}
$\bar{\mathbf{m}}_2 \leftarrow \Phi[\bar{\mathbf{m}}_1]$
if $\bar{\mathbf{c}}_2 = \bar{\mathbf{m}}_2 \mathcal{G}_R$ **then**
  return $\bar{\mathbf{m}}_1$ {$\bar{\mathbf{c}} \in C_{\mathrm{De}}$, accept}
end if
Stage 3: Localized joint ML search in C_{De}
$\mathbf{m}_1^{(0)} \leftarrow \bar{\mathbf{m}}_1$ {Initial estimate from Stage 1}
$\mathcal{I}_\ell \leftarrow$ indices of the ℓ least reliable positions in $\mathbf{z}_{1,\mathcal{I}_S}$
$\mathcal{M}_\ell \leftarrow \{\mathbf{m}_1^{(0)} + \mathbf{e} \mid \mathbf{e} \in \mathbb{F}_2^{k_1},\ \mathrm{supp}(\mathbf{e}) \subseteq \mathcal{I}_\ell\}$ $\{|\mathcal{M}_\ell| = 2^\ell\}$
for all $\mathbf{m}_1 \in \mathcal{M}_\ell$ **do**
  $\mathbf{m}_2 \leftarrow \Phi[\mathbf{m}_1]$
  $\mathbf{c}(\mathbf{m}_1) \leftarrow (\mathbf{m}_1 \mathcal{G}_S, \mathbf{m}_2 \mathcal{G}_R)$
  $\Lambda(\mathbf{m}_1) \leftarrow \sum_{j=1}^{n_1+n_2} z_j (1 - 2c_j(\mathbf{m}_1))$
end for
$\hat{\mathbf{m}}_1 \leftarrow \arg\max_{\mathbf{m}_1 \in \mathcal{M}_\ell} \Lambda(\mathbf{m}_1)$
return $\hat{\mathbf{m}}_1$

5.3 Complexity Analysis of the Proposed Joint Decoder

We now analyze the computational complexity of the proposed EEA-LML decoder and the three-stage joint destination decoder (Algorithm 3), and compare them with the smart [18] and naive [20] decoding algorithms. First we note that since the three-stage joint decoder (Algorithm 3) uses the EEA-LML decoder as its first stage, we derive a single cost expression for Algorithm 3 and treat the EEA-LML decoder as its special case (Stage 1 alone). In stage 1, for a length-n Goppa code with a polynomial of degree t, the Extended Euclidean Algorithm computes $S(x)$, $\Lambda(x)$, and $\Omega(x)$ in $O(nt)$ field operations. The localized binary-projection step then enumerates the syndrome-valid completions of the $|\mathcal{J}| \le t$ non-binary positions, costing $O(2^t)$. Hence

$$O_{\text{EEA-LML}}(n, t) = O\left(nt + 2^t\right). \tag{35}$$

Stage 2 verifies if $\bar{c}_2 = \bar{m}_2 G_R$ in $O(k_2 n_2)$ while stage 3 executes only if Stage 2 fails, searching $|\mathcal{M}_\ell| = 2^\ell$ candidates at cost $O\left(2^\ell (k_1 n_1 + k_2 n_2)\right)$. Applying (35) with $n = n_1 + n_2$ for stage 1 of Algorithm 3 and adding stages 2–3 gives

$$O_{\text{Alg.3}} = O\left(\underbrace{(n_1+n_2)t + 2^t}_{\text{Stage 1: EEA-LML}} + \underbrace{k_2 n_2}_{\text{Stage 2}} + \underbrace{2^\ell (k_1 n_1 + k_2 n_2)}_{\text{Stage 3 (if triggered)}} \right). \tag{36}$$

For small t and ℓ, 2^t and 2^ℓ remain modest, so (36) stays far below a brute-force joint ML search, $O(2^{k_1}(n_1 + n_2))$. Both the naive [20] and smart [18] decoders perform two independent single-code EEA decodes plus an $O(k_2)$ substitution, with no joint search over C_{De}:

$$O_{\text{Naive}} = O_{\text{Smart}} = O(n_1 t_1 + n_2 t_2 + k_2). \tag{37}$$

Comparing (36) and (37), the proposed decoder's overhead is the additive terms 2^t and (only when Stage 2 fails) $2^\ell (k_1 n_1 + k_2 n_2)$ (only when Stage 2 fails). Thia is a bounded, modest cost traded for exploiting the Goppa subcode structure of $C_{\mathrm{De}} \subsetneq \Gamma_{\mathrm{De}}$, which naive and smart cannot access. This trade-off underlies the BER gains reported in Sec. 6. Decoding latency scales with (36), and reduces to stage 1 alone whenever stage 2 succeeds; memory is dominated by G_S, G_R, H_D ($O(k_1 n_1 + k_2 n_2 + t(n_1 + n_2))$ symbols) plus the stage-3 candidate buffer, with no precomputed syndrome table required.

6. Numerical Analysis and Simulation Results

In this section, the system performance is analyzed under both flat Rayleigh fading and additive white Gaussian noise (AWGN) channels using binary phase shift keying (BPSK) and higher-order quadrature amplitude modulation (QAM) signaling. The simulations were implemented in MATLAB R2019A. A fixed-trial Monte Carlo design is used, in which a fixed number of frames, numFrames, is transmitted at every E_b/N_0 point for a given curve, giving a sample size of $N = \text{numFrames} \times k_1$ information bits, where k_1 is the source information length as shown in Tabs. 8 and 9. For an observed BER $\hat{p} = k/N$, the 95% confidence interval is

$$\hat{p} \pm 1.96\sqrt{\hat{p}(1-\hat{p})/N} \approx \hat{p}\left(1 \pm \frac{1.96}{\sqrt{k}}\right), \qquad (38)$$

which is considered statistically reliable when $k \geq 30$. Since curves that reach lower BER floors require a proportionally larger N to maintain $k \geq 30$ observed errors, numFrames is increased accordingly for such simulations rather than held fixed across all cases and channels. For example, in Fig. 19 (numFrames $= 3 \times 10^5$, $k_1 = 8$, $N = 2.4 \times 10^6$), the lowest plotted BER (proposed decoder, 20 dB) is 3.2917×10^{-5}, corresponding to $k = 79$ observed errors and a 95% CI of $[2.57 \times 10^{-5}, 4.02 \times 10^{-5}]$ (±22.1%); the corresponding worst-case points on the BCH, RS, and RM comparison curves in the same figure range from $k = 152$ to $k = 2473$ (95% CI half-width ≤ 16%), all above the reliability criterion. We have verified this criterion curve-by-curve for every figure in this paper, and confirmed that all plotted BER values satisfy $k \geq 30$. Coherent detection with perfect channel state information (CSI) at the receiver is assumed in Sec. 6.2–6.4; Section 6.5 relaxes this assumption and evaluates the proposed scheme under imperfect CSI. Gray mapping is used for the M-QAM constellations throughout. The different selection patterns used in the simulations are shown in Tab. 7. In addition, Tables 8 and 9 list the parameters $\mathcal{L}$ and $G(x)$ used for constructing the different binary Goppa codes. The parameters were selected to satisfy both algebraic and cooperative-design requirements. For a binary Goppa code over GF(2^m), the locator set must satisfy $|\mathcal{L}| \leq 2^m$ and the Goppa polynomial $G(x)$ must have no roots in $\mathcal{L}$. In the proposed construction, $\mathcal{L}_S$ and $\mathcal{L}_R$ are chosen disjointly with $\mathcal{L}_D = \mathcal{L}_S \cup \mathcal{L}_R$, and the same Goppa polynomial is used at the source and relay. This ensures that the destination block code is embedded in the ambient Goppa code $\Gamma_{\mathrm{D_e}}$, enabling the proposed joint decoder. The degree $t = \deg(G)$ determines the designed correction capability and guarantees $d_{\min} \geq 2t + 1$ for the ambient binary Goppa code. The EEA-LML decoder is employed for the source and relay component codes to recover the information, while the destination uses the corresponding cooperative decoding strategies under the considered scenarios. Unless otherwise stated, the R-D link is assumed to have a signal-to-noise ratio (SNR) gain relative to the S-D link, that is, $\gamma_{R,D} = \gamma_{S,D} + 3$ dB, reflecting the practical assumption that the relay is deployed closer to the destination. The quantities $\gamma_{S,D}$, $\gamma_{S,R}$, and $\gamma_{R,D}$ denote the SNRs of the source-to-destination, source-to-relay, and relay-to-destination links, respectively. The AWGN-BPSK results serve as a baseline for evaluating the coding and decoding

Case	Type	Selection pattern
1	Full search	[1, 5, 6, 7]
	Target search	[3, 4, 5, 6]
	Random	[1, 2, 3, 4]
2	Full search	[1, 2, 3, 4, 5, 8, 9, 10, 12, 13, 15, 17]
	Target search	[2, 4, 5, 7, 8, 9, 11, 12, 13, 14, 16, 17]
	Random	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
3	Target search	[1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, 28, 29, 31, 32, 33, 34, 36, 37, 38, 39]
	Random	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39]
4	Target search	[2, 4, 5, 8]
	Random	[1, 2, 3, 4]
5	Target search	[3, 4, 5, 7, 9, 10, 13, 14, 15, 18]
	Random	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Tab. 7. Selection patterns for the different cases.

Case	Mod	Galois field	Source Goppa coding	Relay Goppa coding	Destination code	R_{CC}	$\binom{k_1}{k_2}$
1	BPSK / 16-QAM	GF(2^4)	$n_1 = 16,\ k_1 = 8,\ t_1 = 2$ $\mathcal{L}_S = \mathbb{F}_{16}$ $G_S(x) = x^2 + x + \alpha^3$	$n_2 = 16,\ k_2 = 4,\ t_2 = 3$ $\mathcal{L}_R = \mathbb{F}_{16}$ $G_R(x) = x^3 + \alpha$	$C_{\mathrm{D_e}} = [32, 8, 5]$	$\frac{8}{32}$	70
2	BPSK / 32-QAM	GF(2^5)	$n_1 = 32,\ k_1 = 17,\ t_1 = 3$ $\mathcal{L}_S = \mathbb{F}_{32}$ $G_S(x) = x^3 + x + 1$	$n_2 = 32,\ k_2 = 12,\ t_2 = 4$ $\mathcal{L}_R = \mathbb{F}_{32}$ $G_R(x) = x^4 + x + \alpha^{18}$	$C_{\mathrm{D_e}} = [64, 17, 7]$	$\frac{17}{64}$	6188
3	BPSK / 64-QAM	GF(2^6)	$n_1 = 64,\ k_1 = 40,\ t_1 = 4$ $\mathcal{L}_S = \mathbb{F}_{64}$ $G_S(x) = x^4 + x + 1$	$n_2 = 64,\ k_2 = 34,\ t_2 = 5$ $\mathcal{L}_R = \mathbb{F}_{64}$ $G_R(x) = x^5 + x^2 + 1$	$C_{\mathrm{D_e}} = [128, 40, 11]$	$\frac{40}{128}$	3838380

Tab. 8. Specific code and simulation parameters for the proposed general GCC scheme.

Case	Mod	Galois field	Common Goppa polynomial	Source Goppa coding	Relay Goppa coding	Joint codes	R_{CC}	$\binom{k_1}{k_2}$
4	BPSK / 32-QAM	GF(2^5)	$G(x) = x^2 + x + 1$	$n_1 = 18,\ k_1 = 8,\ t_1 = 2$ $\mathcal{L}_S = \{0, \ldots, \alpha^{16}\}$	$n_2 = 14,\ k_2 = 4,\ t_2 = 2$ $\mathcal{L}_R = \{\alpha^{17}, \ldots, \alpha^{30}\}$	$C_{D_e} = [32, 8]$ $\Gamma_{D_e} = [32, 22, 5]$	$\frac{8}{32}$	70
5	BPSK / 64-QAM	GF(2^6)	$G(x) = x^3 + \alpha$	$n_1 = 36,\ k_1 = 18,\ t_1 = 3$ $\mathcal{L}_S = \{0, \ldots, \alpha^{34}\}$	$n_2 = 28,\ k_2 = 10,\ t_2 = 3$ $\mathcal{L}_R = \{\alpha^{35}, \ldots, \alpha^{62}\}$	$C_{D_e} = [64, 18]$ $\Gamma_{D_e} = [64, 46, 7]$	$\frac{18}{64}$	43758

Tab. 9. Specific code and simulation parameters for the proposed joint Goppa-structured subcode $C_{D_e} \subsetneq \Gamma_{D_e}$.

gains without fading, the Rayleigh-BPSK results show the effect of multipath fading on system reliability, while the higher-order QAM results over flat Rayleigh fading illustrate the additional performance tradeoff introduced by increased spectral efficiency.

6.1 BER Performance Comparison of Full, Target and Random Selection Methods

Figures 6, 7, and 8 illustrate the BER performance of the GCC scheme for Case 1 under the ideal source-to-relay channel, ($\gamma_{S,R} = \infty$), for full search, target search, and random message selection at the relay. In these simulations, the smart decoder is employed for cooperative decoding at the destination node. In Fig. 6, which corresponds to BPSK transmission over the flat Rayleigh fading channel, the GCC scheme with the full search information selection method achieves the best performance, followed by the target search method, while the random selection method gives the worst performance.

For example, at $E_b/N_0 = 10\,\text{dB}$, the BER of the full search, target search, and random selection methods are approximately 2.0×10^{-4}, 5×10^{-4}, and 7×10^{-4}, respectively. In Fig. 7, which corresponds to BPSK transmission over the AWGN channel, all three schemes exhibit improved BER compared with the Rayleigh fading case, while preserving the same performance ordering. For instance, at $E_b/N_0 = 9\,\text{dB}$, the full search, target search, and random selection methods achieve BERs of about 2×10^{-6}, 5.0×10^{-6}, and 8×10^{-6}, respectively.

Figure 8 shows the Case 1 performance under 16-QAM over the flat Rayleigh fading channel. As expected, the BER performance degrades relative to the BPSK cases because the higher-order constellation is more sensitive to noise and fading. Nevertheless, the target search method still remains very close to the full search method. For example, at $E_b/N_0 = 10\,\text{dB}$, the BER of the full search, target search, and random selection methods are approximately 6.0×10^{-3}, 7×10^{-3}, and 8×10^{-3}, respectively. These results confirm that the proposed target search algorithm retains near-optimal performance while significantly reducing the search complexity, thereby demonstrating the effectiveness of Algorithm 2.

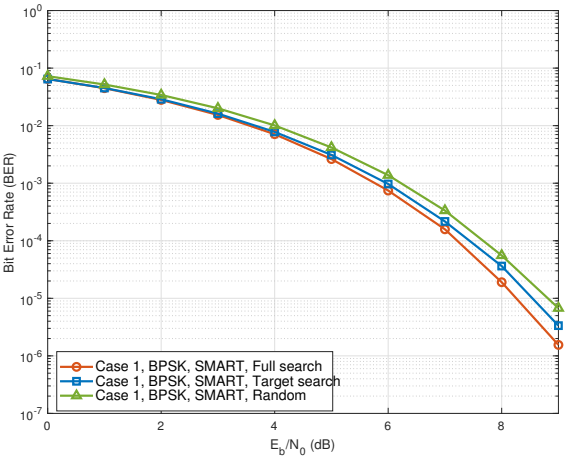


Fig. 7. BER performance comparison of the GCC scheme of Case 1 over the AWGN channel for full search, target search, and random message selection at the relay.

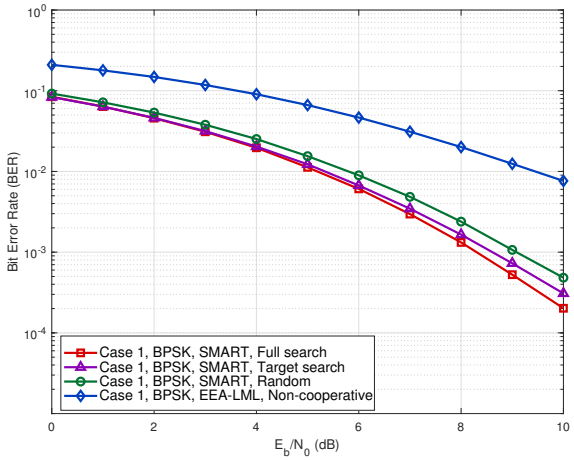


Fig. 6. BER performance comparison of the GCC scheme of Case 1 over the flat Rayleigh fading channel for full search, target search, and random message selection at the relay.

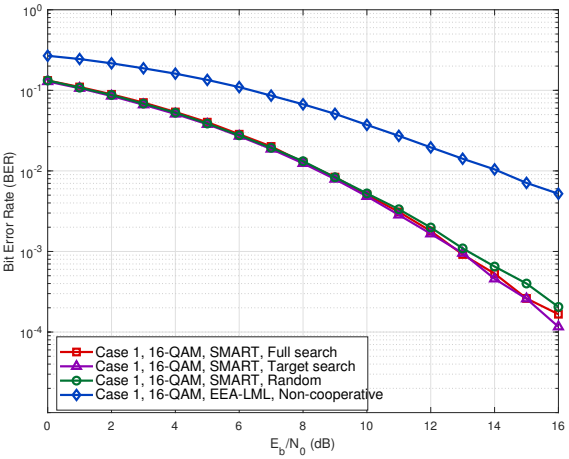


Fig. 8. BER performance comparison of the GCC scheme of Case 1 over the flat Rayleigh fading channel using 16-QAM for full search, target search, and random message selection at the relay.

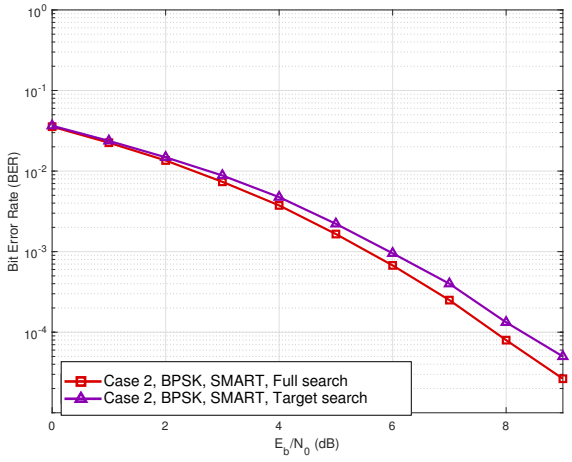


Fig. 9. BER performance comparison of the GCC scheme of Case 2 over the flat Rayleigh fading channel for full search and target search message selection at the relay.

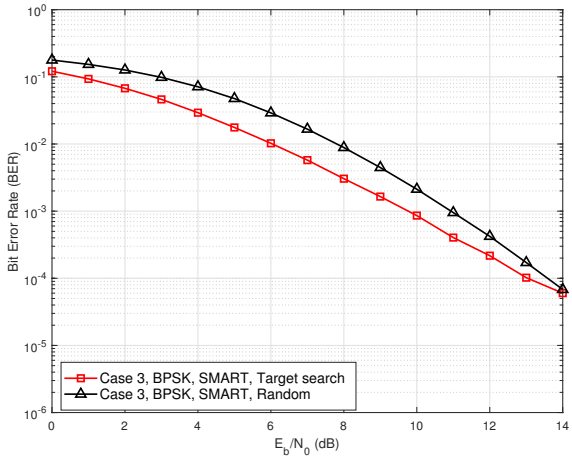


Fig. 10. BER performance comparison of the GCC scheme of Case 3 over the flat Rayleigh fading channel for target search and random message selection at the relay.

Figure 9 presents the BER performance of the GCC scheme for Case 2. The performance curves show that the target search method remains very close to the full search method. For instance, at $E_b/N_0 = 6$ dB, the BER achieved by the full search and target search methods are approximately 9.0×10^{-4} and 1.0×10^{-3}, respectively, which indicates only a marginal loss in performance for the target search method. This further confirms the effectiveness of the proposed search strategy. For Case 3, where the value of $\binom{k_1}{k_2}$ is large, only the target search and random selection methods are compared, as shown in Fig. 10. The performance curves in Fig. 10 clearly demonstrate the advantage of the target search method over the random selection method. For example, at $E_b/N_0 = 10$ dB, the target search method achieves a BER of approximately 9×10^{-4}, whereas the random selection method gives a BER of about 2.1×10^{-3}. Moreover, at BER $\approx 10^{-4}$, the target search method attains this error rate at about 13 dB, while the random selection method requires approximately 14 dB, corresponding to a performance gain of roughly 1 dB. Together, Figs. 6–10 constitute a component-wise comparison isolating the contribution of the relay-selection algorithm: the code design $(C_{\mathrm{So}}, C_{\mathrm{Re}})$ and the destination decoder are held fixed across the full search, target search, and random selection curves. This complements the decoder comparison of Sec. 6.2 (Figs. 11–13) and the theoretical guarantee of Sec. 3.1.2, together validating the three contributions listed in Sec. 1: the algebraically-coupled code design is validated analytically (Equation (16), $d_{\min}(C_{\mathrm{De}}) \geq 2t + 1$ holds for the entire coupled code family, independent of parameter choice), while the relay-selection algorithm and the destination decoder are each validated empirically by the component-wise comparisons above.

6.2 BER Comparison of the Proposed Joint Decoder with Other Existing Decoding Algorithms

Figures 11, 12, and 13 show the performance comparison of the GCC scheme under the ideal source-to-relay channel condition, $(\gamma_{S,R} = \infty)$, with different decoding algorithms, namely, the proposed joint decoder in Algorithm 3, the smart decoding algorithm [18], and the naive decoding algorithm [20]. Figures 11 and 13 correspond to transmission over the flat Rayleigh fading channel for Cases 4 and 5, respectively, while Figure 12 presents the corresponding performance of Case 4 over the AWGN channel.

As evident in Figs. 11 and 13, the GCC scheme with the proposed joint decoder in Algorithm 3 outperforms the schemes employing the existing decoding algorithms. In Case 4 over the flat Rayleigh fading channel, the proposed decoder achieves a performance gain of more than 1.8 dB at BER $\approx 7 \times 10^{-4}$. Similarly, in Case 5 over the flat Rayleigh fading channel, the proposed decoder attains a gain of more than 1.1 dB at BER $\approx 1.4 \times 10^{-4}$. In Fig. 12, the AWGN results for Case 4 show that all the considered decoding methods achieve improved BER compared with the flat Rayleigh fading case due to the absence of fading, while the proposed joint decoder still preserves its superiority over the smart and naive decoding algorithms.

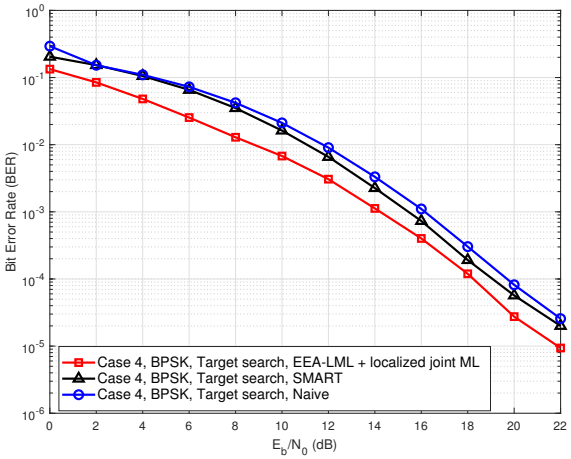


Fig. 11. BER performance comparison of the GCC scheme of Case 4 over the flat Rayleigh fading channel using Algorithm 3, the Smart decoding algorithm [18], and the Naive decoding algorithm [20].

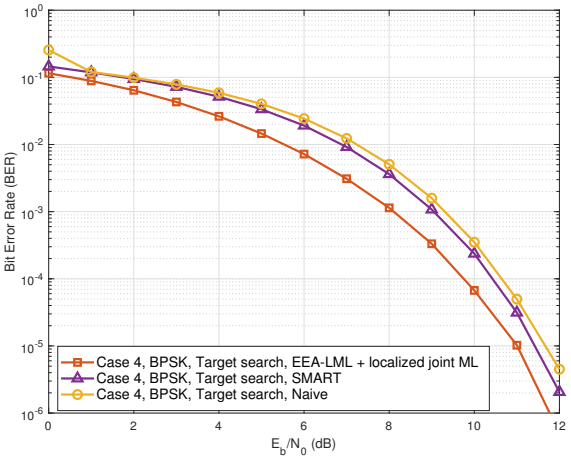


Fig. 12. BER performance comparison of the GCC scheme of Case 4 over the AWGN channel using Algorithm 3, the Smart decoding algorithm [18], and the Naive decoding algorithm [20].

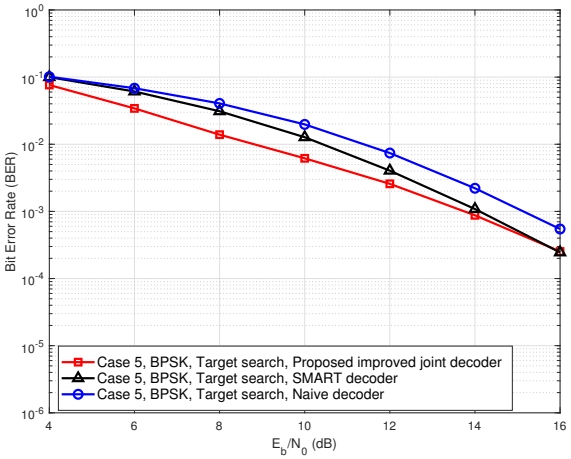


Fig. 13. BER performance comparison of the GCC scheme of Case 5 over the flat Rayleigh fading channel using Algorithm 3, the Smart decoding algorithm [18], and the Naive decoding algorithm [20].

The naive decoder [20] exhibits the worst performance because its decoding process first decodes the joint received signal using the source and relay codes separately and then performs a straightforward substitution. The improved performance of Algorithm 3 stems from the fact that it exploits the Goppa structure of the joint code $C_{\mathrm{D_e}}$ in the proposed joint Goppa subcode at the destination node. This special construction enables the joint code to employ the improved EEA-LML decoder together with an MLD that requires a reduced number of search candidates. Together, Figs. 11–13 constitute a component-wise comparison isolating the contribution of the destination decoder: the code design and relay-selection pattern are held fixed across the proposed, Smart, and Naive decoder curves. This complements the relay-selection comparison of Sec. (Figs. 6–10) and the theoretical minimum-distance guarantee of Sec. 3.1.2 (Equation (16)), which together validate all three contributions of Sec. 1.

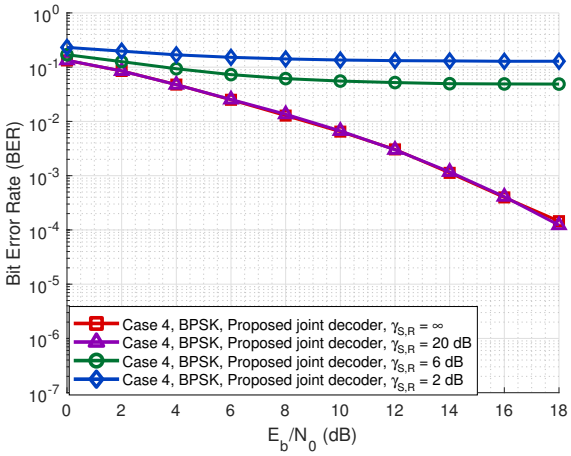


Fig. 14. BER performance curves of the GCC scheme for Case 4 over the flat Rayleigh fading channel under non-ideal ($\gamma_{S,R} = 2$ dB, $\gamma_{S,R} = 6$ dB, $\gamma_{S,R} = 20$ dB) and ideal ($\gamma_{S,R} = \infty$) source-to-relay links.

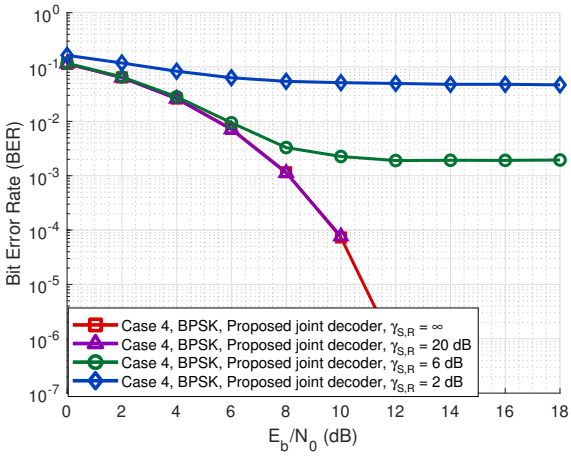


Fig. 15. BER performance curves of the GCC scheme for Case 4 over the AWGN channel under non-ideal ($\gamma_{S,R} = 2$ dB, $\gamma_{S,R} = 6$ dB, $\gamma_{S,R} = 20$ dB) and ideal ($\gamma_{S,R} = \infty$) source-to-relay links.

6.3 Error Performance of the GCC Scheme through Various Source-to-Relay Link Conditions

The preceding simulations assume an ideal (perfect) source-to-relay link, under which the relay always recovers the source information correctly.

However, in practical relay-assisted transmission systems, such an idealized S-R link is rarely attainable. Therefore, to evaluate the robustness of the proposed GCC scheme under more realistic operating conditions, we now examine its BER performance for non-ideal source-to-relay links of varying quality. Figures 14, 15, 16, and 17 show the BER performance of the GCC scheme under poor ($\gamma_{S,R} = 2$ dB, $\gamma_{S,R} = 6$ dB), good ($\gamma_{S,R} = 20$ dB), and ideal ($\gamma_{S,R} = \infty$) source-to-relay links. In particular, Figs. 14 and 15 correspond to Case 4 under BPSK transmission over flat Rayleigh fading and AWGN channels, respectively, Fig. 16 corresponds to Case 4 under higher-order M-QAM over the flat Rayleigh fading channel,

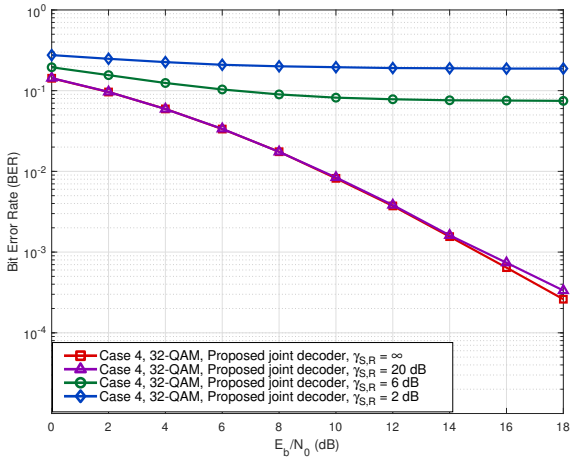


Fig. 16. BER performance curves of the GCC scheme for Case 4 over the flat Rayleigh fading channel using 32-QAM under non-ideal ($\gamma_{S,R}$ = 2 dB, $\gamma_{S,R}$ = 6 dB, $\gamma_{S,R}$ = 20 dB) and ideal ($\gamma_{S,R} = \infty$) source-to-relay links.

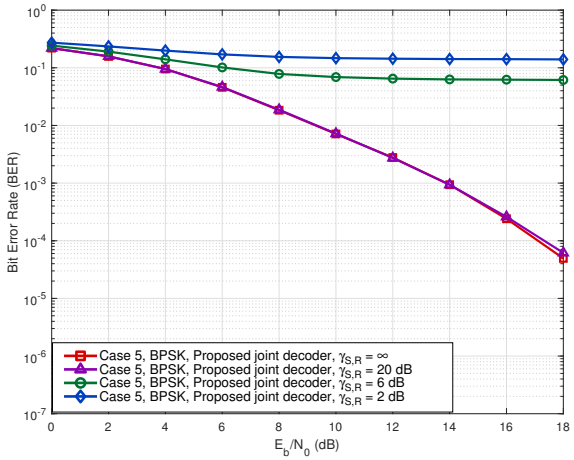


Fig. 17. BER performance curves of the GCC scheme for Case 5 over the flat Rayleigh fading channel under non-ideal ($\gamma_{S,R}$ = 2 dB, $\gamma_{S,R}$ = 6 dB, $\gamma_{S,R}$ = 20 dB) and ideal ($\gamma_{S,R} = \infty$) source-to-relay links.

while Figure 17 shows the corresponding results for Case 5. Under poor S-R links, the relay frequently decodes the source message incorrectly and consequently forwards an erroneous codeword to the destination. This uncontrolled error propagation introduces a pronounced degradation in performance and may even result in an error floor in the BER curves.

On the other hand, when the S-R link quality is good, the BER performance of the GCC scheme approaches that obtained under the ideal S-R link. This is clearly evident from Figs. 14–17, where the curves corresponding to $\gamma_{S,R}$ = 20 dB lie very close to those of the ideal source-to-relay link. Moreover, the AWGN results in Fig. 15 show improved BER relative to the flat Rayleigh fading case due to the absence of fading, while the M-QAM results in Fig. 16 show the expected performance loss relative to BPSK because of the increased sensitivity of higher-order constellations to noise and channel variations. Nevertheless, the overall trends remain consistent, thereby demonstrating that the proposed GCC scheme can still achieve excellent performance in practical scenarios provided that the source-to-relay link is of sufficiently good quality. It is worth noting that the BER performance of BPSK and 32-QAM in Figs. 14 and 16 appears closer than the gap typically expected between these modulation orders. This is a direct consequence of the proposed joint decoding structure: Stage 2 of Algorithm 3 accepts a frame outright whenever the EEA-LML-decoded ambient codeword already lies in C_{De}, while Stage 3 falls back to the full localized joint ML search otherwise. Because the 32-QAM constellation is more densely packed, its Stage-1–2 path succeeds considerably less often than that of BPSK, so a substantially larger fraction of 32-QAM frames are rescued by the more powerful Stage-3 search. This yields a larger effective coding gain for 32-QAM relative to its own uncoded baseline, which compresses the coded BER gap between the two modulations relative to what would be expected under conventional (non-joint) decoding.

6.4 Comparison with Existing Distributed Coded-Cooperative Schemes

Since binary Goppa codes belong to the family of short-to-medium length algebraic codes, it is convenient to benchmark their BER performance against coded cooperative schemes employing binary Bose-Chaudhuri-Hocquenghem (BCH) codes [39], binary Reed Solomon (RS) codes [31], and binary Reed-Muller (RM) codes [31], which lie in the same general class of algebraic block codes. The RSCC and RMCC benchmark schemes are constructed to match the source and relay block lengths and dimensions of the proposed GCC scheme.

However, after binary imaging, puncturing, and subcode selection, their resulting component minimum distances are not identical in all cases. Consequently, the relative BER ordering of RSCC and RMCC is case-dependent, as observed in Cases 4 and 5. To make the comparison explicit, Table 10 summarizes the component-code parameters, decoding methods, relative complexity, and observed BER behavior of the GCC, BCHCC, RSCC, and RMCC schemes used in this section. For the BCHCC and RMCC schemes, the Smart decoding algorithm [18] and the Naive decoding algorithm [20] are employed, while the GCC scheme uses the proposed improved joint decoder in Algorithm 3. Figures 18 and 19 show that, under flat Rayleigh fading in Case 4, the GCC scheme outperforms the BCHCC, RSCC and RMCC schemes. In particular, at BER = 1×10^{-4}, the GCC scheme in Fig. 18 achieves a performance gain of approximately 2.2 dB over the BCHCC scheme and more than 4 dB over both the RSCC and RMCC schemes. Likewise, Figure 19 shows that when both Smart and Naive decoding are considered, the GCC scheme still maintains a clear advantage over the BCHCC, RSCC, and RMCC schemes under the same channel conditions. Fig. 20 further shows that, over the AWGN channel, all the considered schemes exhibit improved BER performance relative to the flat Rayleigh fading case due to the absence of fading, while the GCC scheme

Scheme	Case 4 codes	Case 5 codes	Decoder shown	BER performance	Ref.
GCC	$C_S[18, 8, \geq 5]$, $C_R[14, 4, \geq 5]$ over GF(32)	$C_S[36, 18, \geq 7]$, $C_R[28, 10, \geq 7]$ over GF(64)	Proposed improved joint decoder; EEA–LML with localized search 2^ℓ	Best overall; reference curve	This work
BCHCC	$[18, 8, \geq 5]$, $[14, 4, \geq 5]$ shortened BCH	$[36, 18, \geq 7]$, $[28, 10, \geq 7]$ shortened BCH	Smart/naive decoding	Inferior to GCC; closest benchmark in the low-BER region	[18]
RSCC	$[18, 8, 3]$, $[14, 4, 3]$ binary-image RS over GF(32)	$[36, 18, 5]$, $[28, 10, 3]$ binary-image RS over GF(64)	Smart/naive decoding	Inferior to GCC; relative ordering with RMCC is case-dependent	[29], [19]
RMCC	$[18, 8, 4]$, $[14, 4, 6]$ punctured/subcode RM	$[36, 18, 4]$, $[28, 10, 4]$ punctured/subcode RM	Smart/naive decoding	Inferior to GCC; weaker especially in Case 5	[16]

Tab. 10. Summary comparison of the proposed GCC scheme with algebraic coded-cooperative benchmarks.

still preserves its superiority. On the other hand, Figure 21 shows that when higher-order M-QAM is employed over the flat Rayleigh fading channel, the BER performance degrades compared to the BPSK cases because of the increased sensitivity of higher-order constellations to noise and fading. Nevertheless, the GCC scheme continues to outperform both the BCHCC and RMCC schemes. A similar trend is observed in Case 5. As shown in Fig. 22, the GCC scheme under the proposed improved decoder outperforms the BCHCC, RSCC and RMCC schemes by a gain of around 2 dB and more than 2 and 3 dB, respectively, at BER $= 1 \times 10^{-4}$. The corresponding M-QAM results in Fig. 23 also preserve the same overall ordering, although with the expected BER degradation relative to the BPSK case. The superior performance of the GCC scheme under Algorithm 3 is due to the fact that the joint code $C_{\mathrm{D_e}}$ preserves the Goppa structure, thereby enabling the use of the EEA-LML decoder as part of the joint decoding process, whereas the BCHCC and RMCC schemes rely only on heuristic Smart and Naive decoding approaches for their joint linear block codes.

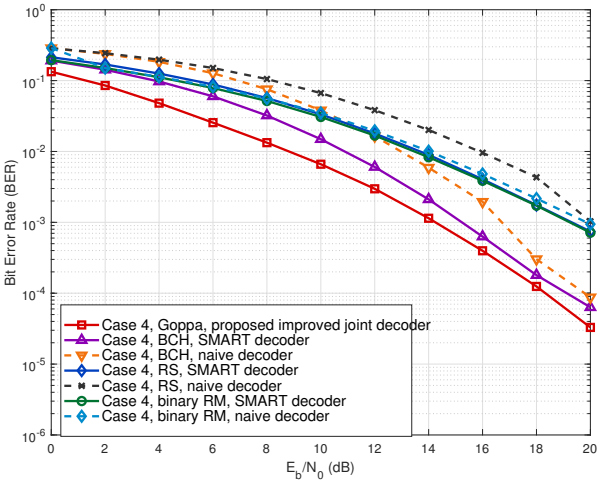


Fig. 19. BER performance curves of the GCC, BCHCC, RSCC, and RMCC schemes with Smart [18] and Naive [20] decoding for Case 4 over a flat Rayleigh fading channel. The GCC outperforms the BCHCC, RSCC, and RMCC schemes under similar channel conditions.

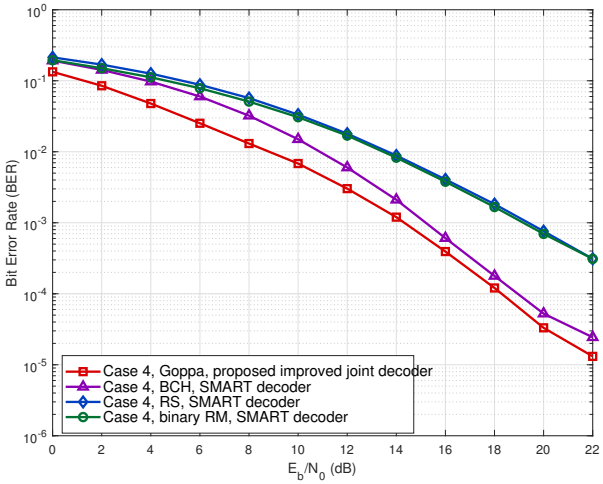


Fig. 18. BER performance curves of the GCC, BCHCC, RSCC, and RMCC schemes with smart decoding [18] for Case 4. The GCC outperforms the BCHCC, RSCC, and RMCC schemes under similar channel conditions.

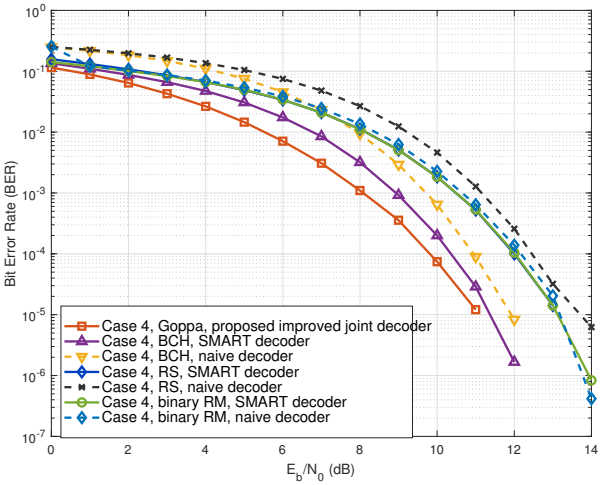


Fig. 20. BER performance curves of the GCC, BCHCC, RSCC, and RMCC schemes with Smart [18] and Naive [20] decoding for Case 4 over the AWGN channel. The GCC outperforms the BCHCC, RSCC and RMCC schemes under similar channel conditions.

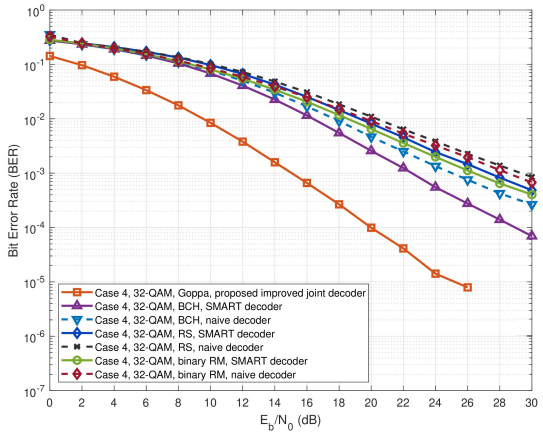


Fig. 21. BER performance curves of the GCC, BCHCC, RSCC, and RMCC schemes with Smart [18] and Naive [20] decoding for Case 4 over the flat Rayleigh fading channel using 32-QAM. The GCC outperforms the BCHCC, RSCC, and RMCC schemes under similar channel conditions.

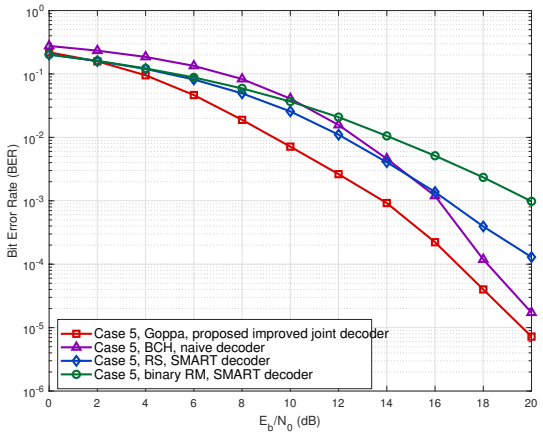


Fig. 22. BER performance curves of the GCC, BCHCC, RSCC, and RMCC schemes with Smart decoding [18] for Case 5 over the flat Rayleigh fading channel. The GCC outperforms the BCHCC, RSCC, and RMCC schemes under similar channel conditions.

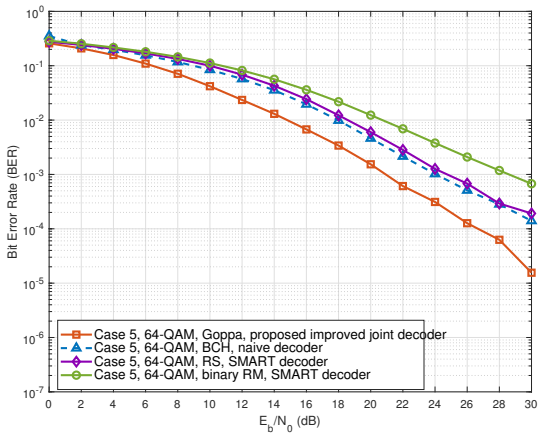


Fig. 23. BER performance curves of the GCC, BCHCC, RSCC, and RMCC schemes with Smart decoding [18] for Case 5 over the flat Rayleigh fading channel using 64-QAM. The GCC outperforms the BCHCC, RSCC, and RMCC schemes under similar channel conditions.

6.5 BER Performance under Imperfect Channel State Information

To further evaluate the robustness of the proposed GCC scheme, we consider imperfect channel state information (CSI) at the receiver. In the preceding simulations, coherent detection was performed using the true channel coefficient. In this subsection, the receiver instead uses an estimated coefficient $\hat{\alpha}^i = \alpha^i + \epsilon^i, \epsilon^i \sim \mathcal{CN}(0, \sigma_e^2)$where α^i denotes the true channel coefficient and ϵ^i is the channel-estimation error. Thus, the received signal is generated using α^i, while the coherent detector uses $\hat{\alpha}^i$. The values $\sigma_e^2 \in \{0.001, 0.01, 0.1\}$ are considered, together with the perfect CSI case $\sigma_e^2 = 0$. The source-to-relay link is kept ideal in this experiment so that the effect of CSI mismatch at the destination can be isolated from relay error propagation.

Figures 24–26 show that small estimation-error variance, such as $\sigma_e^2 = 0.001$, gives BER performance close to the perfect-CSI case. As σ_e^2 increases, the coherent detector becomes increasingly mismatched, causing a visible BER degradation.

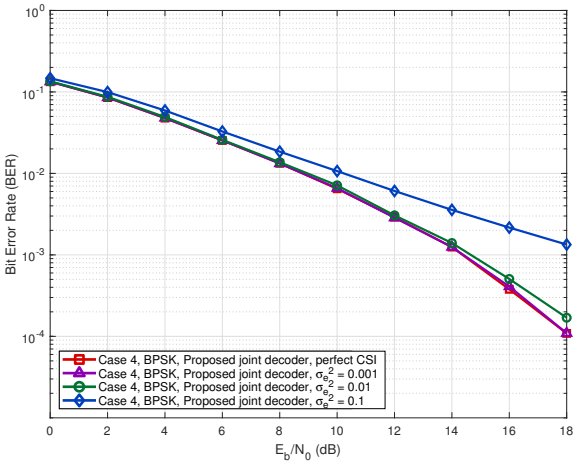


Fig. 24. BER performance of the proposed GCC scheme for Case 4 over the flat Rayleigh fading channel under perfect and imperfect CSI.

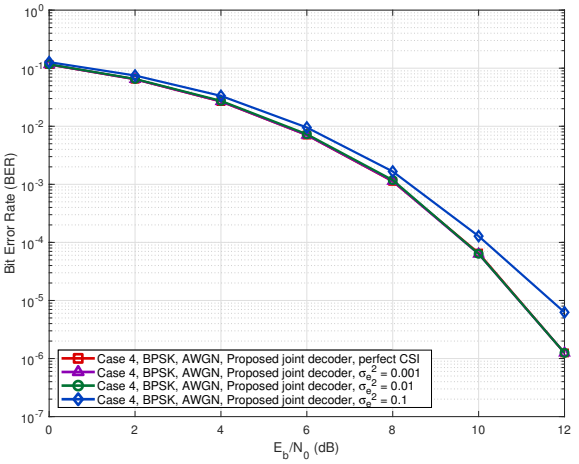


Fig. 25. BER performance of the proposed GCC scheme for Case 4 over the AWGN channel under perfect and imperfect CSI.

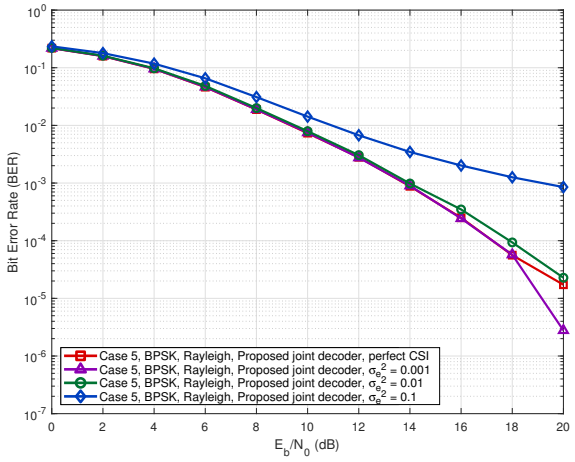


Fig. 26. BER performance of the proposed GCC scheme for Case 5 over the flat Rayleigh fading channel under perfect and imperfect CSI.

The degradation is especially pronounced for $\sigma_e^2 = 0.1$, where the channel-estimation error dominates the high-SNR region and produces an error-floor-like behavior. These results confirm that the proposed decoder remains effective under mild CSI errors, but accurate channel estimation is still important for preserving the full coding gain of the GCC scheme.

7. Conclusion

In this manuscript, two binary Goppa codes defined over the same finite field, with a common Goppa polynomial and disjoint locator sets, were employed at the source and relay nodes to construct a joint Goppa subcode at the destination. Full search and target search algorithms were developed to obtain suitable relay information-selection patterns, with the simulation results showing that the target search method achieves performance close to that of the full search method with significantly lower search complexity. An improved EEA-LML-based joint decoding approach, combined with ML search over a reduced number of candidates, was also developed for decoding the destination Goppa subcode. The simulation results over flat Rayleigh fading and AWGN channels, under both BPSK and higher-order M-QAM signaling, show that the proposed decoder consistently outperforms the existing Smart and Naive decoding algorithms. Furthermore, the GCC scheme was shown to achieve superior BER performance compared with BCHCC and RMCC schemes under the same channel conditions, thereby confirming the effectiveness of the proposed code construction and decoding framework. The present work considers a single relay cooperative system. Extending the algebraically coupled code design and the EEA-LML decoder to a multi-relay setting is a natural direction for future work, since the structure of the joint destination code, and consequently the complexity of the destination decoder would need to be re-derived for more than one relay.

Acknowledgments

Funding: This research is supported by the National Natural Science Foundation of China under the contract No. 61771241.

Data Availability Statement: All the source codes and mathematical models are available from the authors upon reasonable request.

References

[1] HUANG, K., XIAO, Y., LIU, L., et al. Integrated spatial modulation and STBC-VBLAST design toward efficient MIMO transmission. *Sensors*, 2022, vol. 22, no. 13, p. 1–14. DOI: 10.3390/s22134719

[2] LU, H., ZENG, Y., YOU, C., et al. A tutorial on near-field XL-MIMO communications toward 6G. *IEEE Communications Surveys & Tutorials*, 2024, vol. 26, no. 4, p. 2213–2257. DOI: 10.1109/COMST.2024.3387749

[3] BOCCUZZI, J. Spectral efficiency considerations for 6G. *arXiv*, 2025, p. 1–13. DOI: 10.48550/arXiv.2508.09117

[4] THAI, T. V., LE, M. T. P., NGUYEN, H., et al. Next-generation MIMO empowered mobile edge computing: A comprehensive survey toward 6G systems. *Ad Hoc Networks*, 2026, vol. 182, p. 1–28. DOI: 10.1016/j.adhoc.2025.104095

[5] BOUTEGGUI, M., MERAZKA, F. Performance of source transmit antenna selection for MIMO cooperative communication system based DF protocol: Symbol error rate and diversity order. In *International Conference on Wireless Networks and Mobile Communications (WINCOM)*. Rabat (Morocco), 2017, p. 1–8. DOI: 10.1109/WINCOM.2017.8238193

[6] KAMRUZZAMAN, M. M. Relay-assisted multiple-input multiple-output wireless communication system for multiple-access channel using hybrid STBC-VBLAST. In *26th Wireless and Optical Communication Conference (WOCC)*. Newark, NJ (USA), 2017, p. 1–6. DOI: 10.1109/WOCC.2017.7929011

[7] SHI, Z., WANG, H., FU, Y., et al. Zero-forcing-based downlink virtual MIMO–NOMA communications in IoT networks. *IEEE Internet of Things Journal*, 2020, vol. 7, no. 4, p. 2716–2737. DOI: 10.1109/JIOT.2019.2957209

[8] VAN DER MEULEN, E. C. Three-terminal communication channels. *Advances in Applied Probability*, 1971, vol. 3, no. 1, p. 120–154. DOI: 10.2307/1426331

[9] HUNTER, T. E., NOSRATINIA, A. Diversity through coded cooperation. *IEEE Transactions on Wireless Communications*, 2006, vol. 5, no. 2, p. 283–289. DOI: 10.1109/TWC.2006.1611050

[10] LANEMAN, J. N., WORNELL, G. W., TSE, D. N. C. An efficient protocol for realizing cooperative diversity in wireless networks. In *IEEE International Symposium on Information Theory*. Washington, DC (USA), 2001, p. 294. DOI: 10.1109/ISIT.2001.936157

[11] LANEMAN, J. N., TSE, D. N. C., WORNELL, G. W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 12, p. 3062–3080. DOI: 10.1109/TIT.2004.838089

[12] SENDONARIS, A., ERKIP, E., AAZHANG, B. User cooperation diversity. Part I. System description. *IEEE Transactions on Communications*, 2003, vol. 51, no. 11, p. 1927–1938. DOI: 10.1109/TCOMM.2003.818096

[13] OU, Q., HOU, X., LIU, F., et al. Joint partial relay and antenna selection for full-duplex amplify-and-forward relay networks. In *Wireless Internet. WICON 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Vol. 214. Cham (Switzerland): Springer, 2018, p. 149–154. DOI: 10.1007/978-3-319-72998-5_16

[14] DAI, B., YU, L., MA, Z. Compress-and-forward strategy for the relay broadcast channel with confidential messages. In *IEEE International Conference on Communications Workshops (ICC)*. Kuala Lumpur (Malaysia), 2016, p. 254–259. DOI: 10.1109/ICCW.2016.7503796

[15] LIANG, H., LIU, A., DAI, J., et al. Design and analysis of polar coded cooperation with incremental redundancy for IoT in fading channels. *IET Communications*, 2021, vol. 15, no. 4, p. 595–602. DOI: 10.1049/cmu2.12091

[16] EJAZ, S., YANG, F. Jointly optimized Reed–Muller codes for multilevel multirelay coded-cooperative VANETs. *IEEE Transactions on Vehicular Technology*, 2017, vol. 66, no. 5, p. 4017–4028. DOI: 10.1109/TVT.2016.2604320

[17] ZHAN, Q., DU, M., WANG, Y., et al. Half-duplex relay systems based on polar codes. *IET Communications*, 2014, vol. 8, no. 4, p. 433–440. DOI: 10.1049/iet-com.2013.0521

[18] WAWERU, D. K., YANG, F., ZHAO, C., et al. Design of optimized distributed Goppa codes and joint decoding at the destination. *Telecommunication Systems*, 2022, vol. 81, no. 3, p. 341–355. DOI: 10.1007/s11235-022-00948-5

[19] GUO, P., YANG, F., ZHAO, C., et al. Jointly optimized design of distributed Reed–Solomon codes by proper selection in relay. *Telecommunication Systems*, 2021, vol. 78, no. 3, p. 391–403. DOI: 10.1007/s11235-021-00822-w

[20] ZHAO, C., YANG, F., ULLAH, W., et al. Jointly optimized design of distributed RS-coded spatial modulation by appropriate selection at the relay. *EURASIP Journal on Wireless Communications and Networking*, 2023, vol. 2023, no. 1, p. 1–29. DOI: 10.1186/s13638-023-02211-0

[21] CHEN, C., YANG, F. Distributed GRS-coded differential spatial modulation for half-duplex cooperative network based on relay optimization and joint decoding. *IET Communications*, 2024, vol. 18, no. 20, p. 1795–1812. DOI: 10.1049/cmu2.12867

[22] HUNTER, T. E., NOSRATINIA, A. Cooperation diversity through coding. In *IEEE International Symposium on Information Theory (ISIT)*. Lausanne (Switzerland), 2002, p. 220. DOI: 10.1109/ISIT.2002.1023492

[23] FANG, Y., LIEW, S. C., WANG, T. Design of distributed protograph LDPC codes for multi-relay coded-cooperative networks. *IEEE Transactions on Wireless Communications*, 2017, vol. 16, no. 11, p. 7235–7251. DOI: 10.1109/TWC.2017.2743699

[24] ZHANG, S., YANG, F., TANG, L., et al. Joint design of QC-LDPC codes for coded cooperation system with joint iterative decoding. *International Journal of Electronics*, 2016, vol. 103, no. 3, p. 384–405. DOI: 10.1080/00207217.2015.1036374

[25] ZENG, J., LIU, S., WANG, H. Generalized distributed multiple turbo coded cooperative differential spatial modulation. *KSII Transactions on Internet & Information Systems*, 2023, vol. 17, no. 3, p. 999–1021. DOI: 10.3837/tiis.2023.03.017

[26] BLASCO-SERRANO, R., THOBABEN, R., ANDERSSON, M., et al. Polar codes for cooperative relaying. *IEEE Transactions on Communications*, 2012, vol. 60, no. 11, p. 3263–3273. DOI: 10.1109/TCOMM.2012.081412.110266

[27] LIANG, H., LIU, A., LIU, X., et al. Construction and optimization for adaptive polar coded cooperation. *IEEE Wireless Communications Letters*, 2020, vol. 9, no. 8, p. 1187–1190. DOI: 10.1109/LWC.2020.2984738

[28] EJAZ, S., YANG, F., XU, H., et al. Jointly optimized multiple Reed–Muller codes for wireless half-duplex coded-cooperative network with joint decoding. *EURASIP Journal on Wireless Communications and Networking*, 2015, vol. 2015, no. 1, p. 1–15. DOI: 10.1186/s13638-015-0334-1

[29] ALMAWGANI, A. H. M. and SALLEH, M. F. M. RS coded cooperation with adaptive cooperation level scheme over multipath Rayleigh fading channel. In *IEEE 9th Malaysia International Conference on Communications (MICC)*. Kuala Lumpur (Malaysia), 2009, p. 480–484. DOI: 10.1109/MICC.2009.5431555

[30] BERLEKAMP, E. R. Goppa codes. *IEEE Transactions on Information Theory*, 1973, vol. 19, no. 5, p. 590–592. DOI: 10.1109/TIT.1973.1055088

[31] MACWILLIAMS, F. J., SLOANE, N. J. A. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland Publishing Company, 1977. ISBN: 978-0-444-85009-6 (vol. I); 978-0-444-85010-2 (vol. II).

[32] MORENO, C. J. *Algebraic Curves over Finite Fields*. Cambridge: Cambridge University Press, 1991. DOI: 10.1017/CBO9780511608766

[33] LI, X., YUE, Q. Non-binary irreducible quasi-cyclic parity-check subcodes of Goppa codes and extended Goppa codes. *Designs, Codes and Cryptography*, 2022, vol. 90, no. 7, p. 1629–1647. DOI: 10.1007/s10623-022-01062-y

[34] TSFASMAN, M. A., VLADUT, S. G., ZINK, T. Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound. *Mathematische Nachrichten*, 1982, vol. 109, no. 1, p. 21–28. DOI: 10.1002/mana.19821090103

[35] SUGIYAMA, Y., KASAHARA, M., HIRASAWA, S., et al. A method for solving key equation for decoding Goppa codes. *Information and Control*, 1975, vol. 27, no. 1, p. 87–99. DOI: 10.1016/S0019-9958(75)90090-X

[36] FENG, F. A., YANG, F. F., CHEN, C., et al. Jointly optimized design of distributed Goppa codes and decoding. *Radioengineering*, 2023, vol. 32, no. 1, p. 23–32. DOI: 10.13164/re.2023.0023

[37] LIN, S., COSTELLO, D. J. *Error Control Coding*. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2004. ISBN: 978-0-13-042672-7.

[38] PATTERSON, N. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 1975, vol. 21, no. 2, p. 203–207. DOI: 10.1109/TIT.1975.1055350

[39] BOSE, R. C., RAY-CHAUDHURI, D. K. On a class of error correcting binary group codes. *Information and Control*, 1960, vol. 3, no. 1, p. 68–79. DOI: 10.1016/S0019-9958(60)90287-4

About the Authors ...

Lawrence Muthama PAUL (corresponding author) obtained his Bachelor of Science (B.Sc.) degree in Mathematics from the University of Nairobi, Kenya, in 2017, and his Master of Science (M.Sc.) degree in Pure Mathematics from the same institution in 2019. He is currently pursuing a Ph.D. at the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), China. His research interests lie in the areas of Algebraic Codes and Algebraic Geometry (AG) codes, with a particular focus on their applications in wireless communications. His work aims to explore and develop advanced coding techniques to improve the performance and efficiency of modern communication systems.

Fengfan YANG received his M.Sc. and Ph.D. degrees from the North-western Polytechnical University and Southeast University, China in 1993, and 1997, respectively, all in Electronic Engineering. He has been with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, since May 1997. From October 1999 to May 2003, he was a research associate at the Centre for Communication Systems Research, University of Surrey, UK, and Dept. of Electrical and Computer Engineering, McGill University, Canada. His major research interests are information theory, channel coding, and their applications for mobile and satellite communications.

Viola Amondi OCHIENG obtained her Bachelor of Science (B.Sc.) degree in Electrical and Electronic Engineering from the University of Nairobi, Kenya, in 2021. Between 2022 and 2024, she worked as a Design Electrical Engineer at a construction consulting firm, creating detailed electrical designs with AutoCAD and Revit, and preparing accurate Bills of Quantities for project planning. She is currently pursuing a Masters degree in Information and Communication Engineering at the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), China. Her research interests are information theory, signal processing and channel coding for wireless communications. She is interested in leveraging mathematical structures to develop more robust and efficient coding strategies that can enhance data transmission reliability and optimize the performance of next-generation communication technologies.

Daniel Kariuki WAWERU received his B.Sc. degree in Mathematics and M.Sc. degree in Pure Mathematics from the University of Nairobi, Kenya, in 2015 and 2017, respectively. He obtained his Ph.D. in Information and Communication Engineering from the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), China, in 2025. He is currently a lecturer at Egerton University in the Department of Mathematics. His research interests lie in algebraic coding theory, particularly in the connections between codes, algebraic geometry, and computer algebra tools. His recent work focuses on algebraic-geometric codes and their applications in wireless communications.