Syndrome-Coupled Rate-Compatible Error-Correcting Codes

Pengfei Huang[*], **Yi Liu**[*], **Xiaojie Zhang**[†], **Paul H. Siegel**[*], and **Erich F. Haratsch** [‡]
[*]Electrical and Computer Engineering Dept., University of California, San Diego, La Jolla, CA 92093 U.S.A
[†]CNEX Labs, San Jose, CA 95128 U.S.A [‡]Seagate Technology, Fremont, CA 94538 U.S.A
{*pehuang,yil333,psiegel*}*@ucsd.edu*

***Abstract*—Rate-compatible error-correcting codes (ECCs), which consist of a set of extended codes, are of practical interest in both wireless communications and data storage. In this work, we first study the lower bounds for rate-compatible ECCs, thus proving the existence of good rate-compatible codes. Then, we propose a general framework for constructing rate-compatible ECCs based on cosets and syndromes of a set of nested linear codes. We evaluate our construction from two points of view. From a combinatorial perspective, we show that we can construct rate-compatible codes with increasing minimum distances. From a probabilistic point of view, we prove that we are able to construct capacity-achieving rate-compatible codes.**

I. Introduction

Rate-compatible error-correcting codes (ECCs) consist of a set of extended codes, where all symbols of the higher rate code are part of the lower rate code. This allows to match the code rate of the sent data to the channel conditions by retransmitting incremental redundancy to the receiver. Such a scheme is known as hybrid automatic repeat request (HARQ) in wireless communications [10].

The idea of rate-compatible codes dates back to Davida and Reddy [2]. The most commonly used way to construct such codes is by puncturing; that is, to start with a good low-rate code and then successively discard some of the coded symbols (parity-check symbols) to produce higher-rate codes. This approach has been used for convolutional codes [4], turbo codes [13], and low-density parity-check (LDPC) codes [3]. The performance of punctured codes depends on the selected puncturing pattern. However, in general, determining good puncturing patterns is non-trivial, usually done with the aid of computer simulations.

The second approach is by extending; that is, to start with a good high-rate code and then successively add more parity-check symbols to generate lower-rate codes. A two-level extending method called Construction X was introduced in [11] to find new codes with good minimum distance, and later was generalized to Construction XX [1]. Extension-based rate-compatible LDPC codes were designed in [9], [15]. More recently, the extending approach was used to construct capacity-achieving rate-compatible polar codes [5], [8].

The goal of this paper is to provide a systematic approach for constructing rate-compatible codes with theoretically guaranteed properties. We use the extending approach and propose a new algebraic construction for rate-compatible codes; the properties of constructed codes are then analyzed from both combinatorial and probabilistic perspectives. Our contributions are as follows: 1) lower bounds are derived for rate-compatible codes, which have not been fully explored before; 2) a simple and general construction based on cosets and syndromes is proposed to construct rate-compatible codes, and some examples are given; 3) minimum distances of the constructed codes are determined, decoding algorithms are presented, and correctable error-erasure patterns are studied; 4) a connection to recent capacity-achieving rate-compatible polar codes is made.

The remainder of the paper is organized as follows. In Section II, we give the formal definition of rate-compatible codes and introduce notation used in the paper. In Section III, we study lower bounds for rate-compatible codes. In Section IV, we present a general construction for M-level rate-compatible codes, whose minimum distances are studied. Correctable patterns of errors and erasures are also investigated. In Section V, we show our construction can generate capacity-achieving rate-compatible codes by choosing the component codes properly. Section VI concludes the paper. Due to space constraints, we omit some detailed proofs, which can be found online in the longer version of this paper [6].

II. Definitions and Preliminaries

In this section, we give the basic definitions and preliminaries that will be used in the paper.

We use the notation $[n]$ to denote the set $\{1,\dots,n\}$. For a length-n vector $\boldsymbol{v}$ over $\mathbb{F}_q$ and a set $\mathcal{I}\subseteq[n]$, the operation $\pi_{\mathcal{I}}(\boldsymbol{v})$ denotes the restriction of the vector $\boldsymbol{v}$ to coordinates in the set $\mathcal{I}$, and $w_q(\boldsymbol{v})$ represents the Hamming weight of the vector $\boldsymbol{v}$ over $\mathbb{F}_q$. For two vectors $\boldsymbol{v}$ and $\boldsymbol{u}$ over $\mathbb{F}_q$, we use $\mathrm{d}_q(\boldsymbol{v},\boldsymbol{u})$ to denote their Hamming distance. The transpose of a matrix H is written as H^T. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, dimension k, and minimum distance d will be denoted by $\mathcal{C}=[n,k,d]_q$ or by $[n,k,d]_q$ for simplicity; in some cases, we will use notation $[n,k]_q$ to indicate only length and dimension. For any integers $a>b$, the summation in the form of $\sum_{i=a}^{b} X_i$ is defined to be 0. A binomial coefficient $\binom{a}{b}$ is defined to be 0 if $a<b$. For a set $\mathcal{C}$, $|\mathcal{C}|$ represents its cardinality. The q-ary entropy function H_q: $[0,1]\to[0,1]$, is defined by $H_q(x)=-x\log_q x-(1-x)\log_q(1-x)+x\log_q(q-1)$.

Now, we present the definition of rate-compatible codes.

Definition 1. *For $1\leqslant i\leqslant M$, let $\mathcal{C}_i$ be an $[n_i,k,d_i]_q$ linear code, where $n_1<n_2<\cdots<n_M$. The encoder of $\mathcal{C}_i$ is denoted by $\mathcal{E}_{\mathcal{C}_i}:\mathbb{F}_q^k\to\mathcal{C}_i$. These M linear codes are said to be M-level rate-compatible, if for each i, $1\leqslant i\leqslant M-1$, the following condition is satisfied for every possible input $\boldsymbol{u}\in\mathbb{F}_q^k$,*

$$\mathcal{E}_{\mathcal{C}_i}(\boldsymbol{u})=\pi_{[n_i]}\Big(\mathcal{E}_{\mathcal{C}_{i+1}}(\boldsymbol{u})\Big). \tag{1}$$

We denote this M-level rate-compatible relation among these codes by $\mathcal{C}_1\prec\mathcal{C}_2\prec\cdots\prec\mathcal{C}_M$.

Remark 1. For $1\leqslant i\leqslant M-1$, the rates satisfy $R_i=\frac{k}{n_i}>R_{i+1}=\frac{k}{n_{i+1}}$, but the minimum distances obey $d_i\leqslant d_{i+1}$. For

978-1-5090-3097-2/17/$31.00 ©2017 IEEE

systematic codes, the condition in (1) indicates that the set of parity-check symbols of a higher rate code is a subset of the parity-check symbols of a lower rate code.

In this paper, we will use the memoryless q-ary symmetric channel W with crossover probability p. For every pair of a sent symbol $x \in \mathbb{F}_q$ and a received symbol $y \in \mathbb{F}_q$, the conditional probability is:

$$\Pr\{y|x\} = \begin{cases} 1-p & \text{if } y = x \\ p/(q-1) & \text{if } y \neq x \end{cases}$$

The capacity of this channel is $C(W) = 1 - H_q(p)$ [12].

For a linear code $\mathcal{C} = [n, k, d]_q$ over a q-ary symmetric channel, let $P_e^{(n)}(\boldsymbol{x})$ denote the conditional block probability of error, assuming that $\boldsymbol{x}$ was sent, $\boldsymbol{x} \in \mathcal{C}$. Let $P_e^{(n)}(\mathcal{C})$ denote the average probability of error of this code. Due to symmetry, assuming equiprobable codewords, it is clear that,

$$P_e^{(n)}(\mathcal{C}) = \frac{1}{|\mathcal{C}|} \sum_{\boldsymbol{x} \in \mathcal{C}} P_e^{(n)}(\boldsymbol{x}) = P_e^{(n)}(\boldsymbol{x}).$$

III. Lower Bounds for Rate-Compatible Codes

In this section, we derive lower bounds for rate-compatible codes.

A. A General Lower Bound for M-Level Rate-Compatible Codes

Based on the technique used in the derivation of the Gilbert-Varshamov (GV) bound, we derive a GV-like lower bound for M-level rate-compatible codes.

Theorem 2. *There exist M-level rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$, where $\mathcal{C}_i = [n_i = n_1 + \sum_{j=2}^{i} r_j,\ k,\ \geqslant d_i]_q$ for $1 \leqslant i \leqslant M$, if the following inequalities are satisfied for all $1 \leqslant i \leqslant M$,*

$$d_i = \max\left\{ d : \sum_{m=0}^{d-2} \binom{n_1 + \sum_{j=2}^{i} r_j - 1}{m} (q-1)^m < \frac{q^{n_1 + \sum_{j=2}^{i} r_j - k}}{M} \right\}. \tag{2}$$

Proof: The proof is based on a combinatorial argument. See the longer version [6]. ∎

The following corollary follows from Theorem 2, which shows that there exist good rate-compatible codes in the sense that each code can meet the corresponding asymptotic GV-bound.

Corollary 3. *There exist M-level rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$, where $\mathcal{C}_i = [n_i,\ k = R_i n_i,\ \geqslant \delta_i n_i]_q$ for $1 \leqslant i \leqslant M$ and $\delta_M \leqslant 1 - (1/q)$, simultaneously meeting the asymptotic GV bound:*

$$R_i \geqslant 1 - H_q(\delta_i). \tag{3}$$

Proof: Let $V_q(n,t) = \sum_{m=0}^{t} \binom{n}{m} (q-1)^m$. From Theorem 2, there exist M-level rate-compatible codes $\mathcal{C}_i = [n_i,\ k = R_i n_i,\ \geqslant \delta_i n_i]_q$ for $1 \leqslant i \leqslant M$ such that

$$V_q(n_i - 1, \delta_i n_i - 1) \geqslant \frac{q^{n_i - k}}{M}. \tag{4}$$

Since $V_q(n,t) \leqslant q^{nH_q(t/n)}$ for $0 \leqslant t/n \leqslant 1 - (1/q)$ [12], we have

$$q^{n_i H_q(\delta_i)} \geqslant V_q(n_i, \delta_i n_i) \geqslant V_q(n_i - 1, \delta_i n_i - 1) \geqslant \frac{q^{n_i - k}}{M},$$

which gives $R_i \geqslant 1 - H_q(\delta_i) - \frac{\log_q M}{n_i}$. As n_i goes to infinity, we obtain the result. ∎

B. A Lower Bound for Two-Level Rate-Compatible Codes with Known Weight Enumerator

For two-level rate-compatible codes, if the weight enumerator of the higher rate code is known, we have the following lower bound.

Theorem 4. *Let $\mathcal{C}_1$ be an $[n_1, k, d_1]_q$ code with weight enumerator $A(s) = \sum_{w=0}^{n_1} A_w s^w$, where A_w is the number of codewords of Hamming weight w. There exist two-level rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 = [n_2 = n_1 + r_2,\ k,\ \geqslant d_2]_q$, if*

$$\sum_{w=1}^{d_2 - 1} B_w < q^{r_2},$$

where $B_w = \frac{1}{q-1} \sum_{m=1}^{w} A_m \binom{r_2}{w-m} (q-1)^{w-m}$, for $1 \leqslant w \leqslant n_2$.

Proof: The proof is based on a probabilistic argument. See the longer version [6]. ∎

IV. A General Construction for M-Level Rate-Compatible Codes

In this section, we present a general construction for M-level rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$. We then derive their minimum distances. The decoding algorithm and correctable error-erasure patterns are studied. We focus on the combinatorial property here and will leave the discussion on the capacity-achieving property of our construction to the next section.

In our construction for M-level rate-compatible codes, we need a set of component codes which are defined as follows.

1) Choose a set of nested codes $\mathcal{C}_1^M \subset \mathcal{C}_1^{M-1} \subset \cdots \subset \mathcal{C}_1^1 = \mathcal{C}_1 = [n_1, k, d_1]_q$, where $\mathcal{C}_1^i = [n_1, n_1 - \sum_{m=1}^{i} v_m, d_i]_q$ for $1 \leqslant i \leqslant M$. We have $k = n_1 - v_1$ and $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_M$. Define $\mathcal{C}_1^0 = \emptyset$ and for $1 \leqslant \ell \leqslant i$, let matrix $H_{\mathcal{C}_1^\ell \setminus \mathcal{C}_1^{\ell-1}}$ represent a $v_\ell \times n_1$ matrix over $\mathbb{F}_q$ such that $\mathcal{C}_1^i$ has the following parity-check matrix:

$$H_{\mathcal{C}_1^i} = \begin{bmatrix} H_{\mathcal{C}_1^1} \\ H_{\mathcal{C}_1^2 \setminus \mathcal{C}_1^1} \\ \vdots \\ H_{\mathcal{C}_1^i \setminus \mathcal{C}_1^{i-1}} \end{bmatrix}.$$

The encoder of code $\mathcal{C}_1$ is denoted by $\mathcal{E}_{\mathcal{C}_1} : \mathbb{F}_q^k \to \mathcal{C}_1$. We also use $\mathcal{E}_{\mathcal{C}_1}^{-1}$ as the inverse of the encoding mapping.

2) For ith level, $2 \leqslant i \leqslant M$, consider a set of auxiliary nested codes $\mathcal{A}_i^M \subset \mathcal{A}_i^{M-1} \subset \cdots \subset \mathcal{A}_i^{i+1} \subset \mathcal{A}_i^i$, where $\mathcal{A}_i^j = [n_i, v_i + \sum_{m=2}^{i-1} \lambda_m^i - \sum_{\ell=i+1}^{j} \lambda_i^\ell, \delta_i^j]_q$ for $i \leqslant j \leqslant M$. Let matrix $H_{\mathcal{A}_i^i}$ represent an $(n_i - v_i - \sum_{m=2}^{i-1} \lambda_m^i) \times n_i$ matrix over $\mathbb{F}_q$ and matrix $H_{\mathcal{A}_i^\ell \setminus \mathcal{A}_i^{\ell-1}}$, $i+1 \leqslant \ell \leqslant j$, represent a $\lambda_i^\ell \times n_i$ matrix over $\mathbb{F}_q$, such that $\mathcal{A}_i^j$ has the following parity-check matrix:

$$H_{\mathcal{A}_i^j} = \begin{bmatrix} H_{\mathcal{A}_i^i} \\ H_{\mathcal{A}_i^{i+1} \setminus \mathcal{A}_i^i} \\ \vdots \\ H_{\mathcal{A}_i^j \setminus \mathcal{A}_i^{j-1}} \end{bmatrix}.$$

For each $2 \leqslant i \leqslant M$, the encoder of code $\mathcal{A}_i^i$ is denoted by $\mathcal{E}_{\mathcal{A}_i^i} : \mathbb{F}_q^{v_i + \sum_{m=2}^{i-1} \lambda_m^i} \to \mathcal{A}_i^i$. We also use $\mathcal{E}_{\mathcal{A}_i^i}^{-1}$ as the inverse of the encoding mapping.

Note that we also define $\mathcal{C}_1^{M+1} = \emptyset$ and $\mathcal{A}_i^{M+1} = \emptyset$ for $2 \leqslant i \leqslant M$.

A. Construction and Minimum Distance

Now, we give a general algebraic construction for rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$ by using the nested component codes introduced above.

Construction 1: Encoding Procedure

Input: A length-k vector $\boldsymbol{u}$ of information symbols over $\mathbb{F}_q$.
Output: A codeword $\boldsymbol{c}_i \in \mathcal{C}_i$ over $\mathbb{F}_q$, for $i = 1, \ldots, M$.

1: $\boldsymbol{c}_1 = \mathcal{E}_{\mathcal{C}_1}(\boldsymbol{u})$.
2: $\boldsymbol{s}_i = \boldsymbol{c}_1 H^T_{\mathcal{C}_1^i \setminus \mathcal{C}_1^{i-1}}$ for $i = 2, 3, \ldots, M$.
3: **for** $i = 2, \ldots, M$ **do**
4: $\quad \boldsymbol{a}_i^i = \mathcal{E}_{\mathcal{A}_i^i}\Big((\boldsymbol{s}_i, \Lambda_2^i, \cdots, \Lambda_{i-1}^i)\Big)$. // comment [1] //
5: $\quad \boldsymbol{c}_i = (\boldsymbol{c}_1, \boldsymbol{a}_2^2, \cdots, \boldsymbol{a}_i^i)$.
6: $\quad$ **for** $j = i+1, \ldots, M$ **do**
7: $\quad\quad \Lambda_i^j = \boldsymbol{a}_i^i H^T_{\mathcal{A}_i^j \setminus \mathcal{A}_i^{j-1}}$.
8: $\quad$ **end for**
9: **end for**

Remark 2. To make Construction 1 clear, consider the case of $M = 3$ as an example. Then a codeword $\boldsymbol{c}_3 \in \mathcal{C}_3$ has the form: $\boldsymbol{c}_3 = \Big(\boldsymbol{c}_1, \mathcal{E}_{\mathcal{A}_2^2}(\boldsymbol{s}_2), \mathcal{E}_{\mathcal{A}_3^3}(\boldsymbol{s}_3, \Lambda_2^3)\Big)$. The main idea of Construction 1 is to extend the base code $\mathcal{C}_1$ by progressively generating and encoding syndromes of component codes in a proper way. Thus, we call it a *syndrome-coupled* construction.

We have the following theorem on the code parameters of the constructed rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$.

Theorem 5. *From Construction 1, the code $\mathcal{C}_i$, $1 \leqslant i \leqslant M$, has length $N_i = \sum_{j=1}^{i} n_j$ and dimension $K_i = k$. Moreover, assume that $\mathcal{A}_i^j$, $2 \leqslant i \leqslant M$ and $i \leqslant j \leqslant M$, has minimum distance $\delta_i^j \geqslant d_j - d_{i-1}$. Then $\mathcal{C}_i$ has minimum distance $D_i = d_i$. There exists a decoder for $\mathcal{C}_i$ that can correct any error pattern whose Hamming weight is less than $d_i/2$.*

Proof: The code length and dimension are obvious. In the following, we prove the minimum distance. Since the proofs for all $\mathcal{C}_i$, $1 \leqslant i \leqslant M$, are similar, we only give a proof for the code $\mathcal{C}_M$.

We first prove $D_M \geqslant d_M$ by showing that any nonzero codeword $\boldsymbol{c}_M \in \mathcal{C}_M$ has weight at least d_M. To see this, for any nonzero codeword $\boldsymbol{c}_1 \in \mathcal{C}_1$, there exists an integer γ_1, $1 \leqslant \gamma_1 \leqslant M$, such that $\boldsymbol{c}_1 \in \mathcal{C}_1^{\gamma_1}$ and $\boldsymbol{c}_1 \notin \mathcal{C}_1^{\gamma_1+1}$. Let $\boldsymbol{c}_M \in \mathcal{C}_M$ be the codeword derived from $\boldsymbol{c}_1$. Then, we have $w_q(\boldsymbol{c}_M) \geqslant w_q(\boldsymbol{c}_1) \geqslant d_{\gamma_1}$. If $\gamma_1 = M$, we are done; otherwise if $1 \leqslant \gamma_1 \leqslant M-1$ we have $\boldsymbol{s}_{\gamma_1+1} \neq \boldsymbol{0}$ and $\boldsymbol{a}_{\gamma_1+1}^{\gamma_1+1} \neq \boldsymbol{0}$.

Now, for $\boldsymbol{a}_{\gamma_1+1}^{\gamma_1+1}$, there exists an integer γ_2, $\gamma_1 + 1 \leqslant \gamma_2 \leqslant M$, such that $\boldsymbol{a}_{\gamma_1+1}^{\gamma_1+1} \in \mathcal{A}_{\gamma_1+1}^{\gamma_2}$ and $\boldsymbol{a}_{\gamma_1+1}^{\gamma_1+1} \notin \mathcal{A}_{\gamma_1+1}^{\gamma_2+1}$. Then, we have $w_q(\boldsymbol{c}_M) \geqslant w_q(\boldsymbol{c}_1) + w_q(\boldsymbol{a}_{\gamma_1+1}^{\gamma_1+1}) \geqslant d_{\gamma_1} + d_{\gamma_2} - d_{\gamma_1} = d_{\gamma_2}$. If $\gamma_2 = M$, done; otherwise for $\gamma_1 + 1 \leqslant \gamma_2 \leqslant M-1$, we have $\Lambda_{\gamma_1+1}^{\gamma_2+1} \neq \boldsymbol{0}$ and $\boldsymbol{a}_{\gamma_2+1}^{\gamma_2+1} \neq \boldsymbol{0}$.

Using the same argument as above, it is clear that we can find a sequence of $\gamma_1 < \gamma_2 < \cdots < \gamma_i$, where i is a certain integer $1 \leqslant i \leqslant M$ and $\gamma_i = M$, such that $w_q(\boldsymbol{c}_1) \geqslant d_{\gamma_1}$, $w_q(\boldsymbol{a}_{\gamma_1+1}^{\gamma_1+1}) \geqslant d_{\gamma_2} - d_{\gamma_1}$, $w_q(\boldsymbol{a}_{\gamma_2+1}^{\gamma_2+1}) \geqslant d_{\gamma_3} - d_{\gamma_2}$, $\cdots$, $w_q(\boldsymbol{a}_{\gamma_{i-1}+1}^{\gamma_{i-1}+1}) \geqslant d_{\gamma_i} - d_{\gamma_{i-1}} = d_M - d_{\gamma_{i-1}}$. Then, we have $w_q(\boldsymbol{c}_M) \geqslant w_q(\boldsymbol{c}_1) + \sum_{j=1}^{i-1} w_q(\boldsymbol{a}_{\gamma_j+1}^{\gamma_j+1}) \geqslant d_M$. Thus, we have $D_M \geqslant d_M$.

There exists a codeword $\boldsymbol{c}_1 \in \mathcal{C}_1^M$ such that $w_q(\boldsymbol{c}_1) = d_M$, so we have $w_q(\boldsymbol{c}_M) = d_M$, implying $D_M \leqslant d_M$.

A decoder which can correct any error pattern of Hamming weight less than $d_i/2$ is given in the longer version [6]. ■

Next, we provide an example of three-level rate-compatible codes to illustrate Construction 1.

Example 1. Consider a set of nested binary BCH codes $\mathcal{C}_1^3 = [15, 5, 7]_2 \subset \mathcal{C}_1^2 = [15, 7, 5]_2 \subset \mathcal{C}_1^1 = [15, 11, 3]_2$. Choose a set of auxiliary codes $\mathcal{A}_2^3 = [5, 1, 4]_2 \subset \mathcal{A}_2^2 = [5, 4, 2]_2$, and $\mathcal{A}_3^3 = [6, 5, 2]_2$, where the code $\mathcal{A}_2^3$ is obtained by shortening an $[8, 4, 4]_2$ extended Hamming code by three information bits.

Then, from Construction 1 and Theorem 5, we obtain three-level rate-compatible codes $\mathcal{C}_1 = [15, 11, 3]_2 \prec \mathcal{C}_2 = [20, 11, 5]_2 \prec \mathcal{C}_3 = [26, 11, 7]_2$. Note that $\mathcal{C}_1$ and $\mathcal{C}_2$ are optimal, achieving the maximum possible dimensions with the given code length and minimum distance. The dimension of $\mathcal{C}_3$ is close to the upper bound 13 according to the online Table [14]. □

B. Decoding Algorithm and Correctable Error-Erasure Patterns

In the following, we study decoding algorithms and correctable patterns of errors and erasures for rate-compatible codes obtained from Construction 1. For simple notation and concise analysis, we focus on the code $\mathcal{C}_M$. Any results obtained for $\mathcal{C}_M$ can be easily modified for other codes $\mathcal{C}_i$, $1 \leqslant i \leqslant M-1$, so details are omitted.

Assume a codeword $\boldsymbol{c}_M \in \mathcal{C}_M$, $\boldsymbol{c}_M = (\boldsymbol{c}_1, \boldsymbol{a}_2^2, \cdots, \boldsymbol{a}_M^M)$, is transmitted. Let the corresponding received word be $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_M)$ with errors and erasures, i.e., $\boldsymbol{y} \in (\mathbb{F}_q \cup \{?\})^{N_M}$, where the symbol ? represents an erasure. For $1 \leqslant i \leqslant M$, let t_i and τ_i denote the number of errors and erasures in the sub-block $\boldsymbol{y}_i$ of the received word $\boldsymbol{y}$.

The code $\mathcal{C}_M$ can correct any combined error and erasure pattern that satisfies the following condition:

$$\begin{aligned} &2t_1 + \tau_1 \leqslant d_M - 1, \\ &2t_i + \tau_i \leqslant \delta_i^M - 1, \ \forall\ 2 \leqslant i \leqslant M. \end{aligned} \tag{5}$$

To see this, we present a decoding algorithm, referred to as Algorithm 1, for $\mathcal{C}_M$. It uses the following component error-erasure decoders:

a) The error-erasure decoder $\mathcal{D}_{\mathcal{C}_1^i}$ for a coset of the code $\mathcal{C}_1^i$, for $1 \leqslant i \leqslant M$, is defined by

$$\mathcal{D}_{\mathcal{C}_1^i} : (\mathbb{F}_q \cup \{?\})^{n_1} \times (\mathbb{F}_q \cup \{?\})^{\sum_{j=1}^{i} v_j} \to \mathcal{C}_1^i + \boldsymbol{e} \cup \{\text{“e”}\}$$

The decoder $\mathcal{D}_{\mathcal{C}_1^i}$ either produces a codeword in the coset $\mathcal{C}_1^i + \boldsymbol{e}$ or a decoding failure “e”. For our purpose, we require that $\mathcal{D}_{\mathcal{C}_1^i}$ have the following error-erasure correcting capability. For a sent codeword $\boldsymbol{c}$ in the coset $\mathcal{C}_1^i + \boldsymbol{e}$, where the vector $\boldsymbol{e}$ is a coset leader, if the inputs of $\mathcal{D}_{\mathcal{C}_1^i}$ are a length-n_1 received word $\boldsymbol{y}$ having t errors and τ erasures, where $2t + \tau \leqslant d_i - 1$, and a correct length-$\sum_{j=1}^{i} v_j$ syndrome vector $\boldsymbol{s}$, $\boldsymbol{s} = \boldsymbol{e} H^T_{\mathcal{C}_1^i}$, then $\mathcal{D}_{\mathcal{C}_1^i}$ can correct all these errors and erasures. It is well known that such a decoder exists [12].

[1] For $i = 2$, we define $(\boldsymbol{s}_i, \Lambda_2^i, \cdots, \Lambda_{i-1}^i) = \boldsymbol{s}_2$.

b) The error-erasure decoder $\mathcal{D}_{\mathcal{A}_i^j}$ for a coset of the code $\mathcal{A}_i^j$, for $2 \leqslant i \leqslant M$ and $i \leqslant j \leqslant M$, is defined by

$$\mathcal{D}_{\mathcal{A}_i^j} : (\mathbb{F}_q \cup \{?\})^{n_i} \times (\mathbb{F}_q \cup \{?\})^{n_i - v_i - \sum_{m=2}^{i-1} \lambda_m^i + \sum_{\ell=i+1}^{j} \lambda_i^\ell} \to \mathcal{A}_i^j + \boldsymbol{e} \cup \{\text{“e”}\}$$

The decoder $\mathcal{D}_{\mathcal{A}_i^j}$ either produces a codeword in the coset $\mathcal{A}_i^j + \boldsymbol{e}$ or a decoding failure “e”. Similar to $\mathcal{D}_{\mathcal{C}_1^i}$, we assume that $\mathcal{D}_{\mathcal{A}_i^j}$ has the following error-erasure correcting capability. For a sent codeword $\boldsymbol{c}$ in the coset $\mathcal{A}_i^j + \boldsymbol{e}$, where $\boldsymbol{e}$ is a coset leader, if the inputs of $\mathcal{D}_{\mathcal{A}_i^j}$ are a length-n_i received word $\boldsymbol{y}$ having t errors and τ erasures, where $2t + \tau \leqslant \delta_i^j - 1$, and a correct length-$(n_i - v_i - \sum_{m=2}^{i-1} \lambda_m^i + \sum_{\ell=i+1}^{j} \lambda_i^\ell)$ syndrome vector $\boldsymbol{s}$, $\boldsymbol{s} = \boldsymbol{e} H_{\mathcal{A}_i^j}^T$, then $\mathcal{D}_{\mathcal{A}_i^j}$ can correct all these errors and erasures.

Now, we present the decoding algorithm as follows.

Algorithm 1: Decoding Procedure for $\mathcal{C}_M$

Input: received word $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_M)$.
Output: A length-k vector $\boldsymbol{u}$ of information symbols over $\mathbb{F}_q$ or a decoding failure “e”.

1: **for** $i = M, M-1, \ldots, 2$ **do**
2: Let the syndrome $\Lambda_i^i = \boldsymbol{0}$.
3: $\hat{\boldsymbol{a}}_i^i = \mathcal{D}_{\mathcal{A}_i^M}\Big(\boldsymbol{y}_i, (\Lambda_i^i, \Lambda_i^{i+1}, \cdots, \Lambda_i^M)\Big)$.
4: $(\boldsymbol{s}_i, \Lambda_2^i, \cdots, \Lambda_{i-1}^i) = \mathcal{E}_{\mathcal{A}_i^i}^{-1}(\hat{\boldsymbol{a}}_i^i)$. // comment [2] //
5: **end for**
6: Let the syndrome $\boldsymbol{s}_1 = \boldsymbol{0}$.
7: $\boldsymbol{c}_1 = \mathcal{D}_{\mathcal{C}_1^M}\big(\boldsymbol{y}_1, (\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_M)\big)$.
8: Output $\boldsymbol{u} = \mathcal{E}_{\mathcal{C}_1}^{-1}(\boldsymbol{c}_1)$ if all above steps are successful; otherwise, return “e”.

Theorem 6. *The code $\mathcal{C}_M$ can correct any combined error and erasure pattern that satisfies the condition in (5), by using Algorithm 1.*

Proof: We use Algorithm 1 to decode sub-blocks from $\boldsymbol{y}_M$ to $\boldsymbol{y}_1$. Each sub-block $\boldsymbol{y}_i$ can be corrected successfully due to the condition in (5) and the correcting capability of each component decoder. See the longer version [6]. ∎

Using nested MDS codes as component codes, Construction 1 can generate an *optimal* code $\mathcal{C}_M$ with respect to the capability of correcting certain error-erasure patterns. For simple notation, we present the case of $M = 3$ as an example.

Example 2. Consider a set of nested MDS codes $\mathcal{C}_1^3 = [n_1, n_1 - d_3 + 1, d_3]_q \subset \mathcal{C}_1^2 = [n_1, n_1 - d_2 + 1, d_2]_q \subset \mathcal{C}_1^1 = [n_1, n_1 - d_1 + 1, d_1]_q$. Choose a set of auxiliary MDS codes $\mathcal{A}_2^3 = [2(d_2 - d_1) - 1, 2d_2 - d_3 - d_1, d_3 - d_1]_q \subset \mathcal{A}_2^2 = [2(d_2 - d_1) - 1, d_2 - d_1, d_2 - d_1]_q$, and $\mathcal{A}_3^3 = [3(d_3 - d_2) - 1, 2(d_3 - d_2), d_3 - d_2]_q$.

Then, from Construction 1 and Theorem 5, we obtain three-level rate-compatible codes $\mathcal{C}_1 = [n_1, n_1 - d_1 + 1, d_1]_q \prec \mathcal{C}_2 = [n_1 + 2(d_2 - d_1) - 1, n_1 - d_1 + 1, d_2]_q \prec \mathcal{C}_3 = [n_1 + 2(d_2 - d_1) + 3(d_3 - d_2) - 2, n_1 - d_1 + 1, d_3]_q$.

[2] For $i = 2$, we define $(\boldsymbol{s}_i, \Lambda_2^i, \cdots, \Lambda_{i-1}^i) = \boldsymbol{s}_2$.

From the condition in (5) and Theorem 6, the code $\mathcal{C}_3$ can correct any pattern of errors and erasures satisfying

$$2t_i + \tau_i \leqslant d_3 - d_{i-1} - 1, \ \forall\ 1 \leqslant i \leqslant 3, \tag{6}$$

where d_0 is defined to be 0.

In general, the dimension of $\mathcal{C}_3$ cannot achieve the upper bounds given by traditional bounds (e.g., Singleton and Hamming bounds). However, $\mathcal{C}_3$ is optimal in the sense of having the largest possible dimension among all codes with the three-level structure and the same error-erasure correcting capability; that is, we have the following lemma, whose proof is in the longer version [6].

Lemma 7. *Let $\mathcal{C}_3$ be a code of length $n_1 + 2(d_2 - d_1) + 3(d_3 - d_2) - 2$ and dimension k_3 over $\mathbb{F}_q$. Each codeword $\boldsymbol{c}_3 \in \mathcal{C}_3$ has three sub-blocks $(\boldsymbol{c}_1, \boldsymbol{a}_2^2, \boldsymbol{a}_3^3)$: 1) $\boldsymbol{c}_1$ of length n_1, 2) $\boldsymbol{a}_2^2$ of length $2(d_2 - d_1) - 1$, and 3) $\boldsymbol{a}_3^3$ of length $3(d_3 - d_2) - 1$. Assume that each sub-block of $\mathcal{C}_3$ can correct all error and erasure patterns satisfying the condition in (6). Then, we must have $k_3 \leqslant n_1 - d_1 + 1$.* □

In Algorithm 1, the code $\mathcal{C}_M$ is decoded by M steps, so we can bound the decoding error probability $P_e^{(N_M)}(\mathcal{C}_M)$ of $\mathcal{C}_M$ by the decoding error probability of each step as

$$P_e^{(N_M)}(\mathcal{C}_M) \leqslant 1 - \Big(1 - P_e^{(n_1)}(\mathcal{C}_1^M)\Big) \prod_{i=2}^{M} \Big(1 - P_e^{(n_i)}(\mathcal{A}_i^M)\Big),$$

which provides a fast way to predict the performance of $\mathcal{C}_M$. In particular, if each component code is (shortened) BCH code, then $P_e^{(N_M)}(\mathcal{C}_M)$ can be easily estimated by some calculations. We use a simple example to illustrate this estimation.

Example 3. Consider two nested binary BCH codes $\mathcal{C}_1^2 = [8191, 7411]_2 \subset \mathcal{C}_1^1 = [8191, 7671]_2$. The codes $\mathcal{C}_1^1$ and $\mathcal{C}_1^2$ can correct 40 and 60 errors, respectively. Choose an auxiliary shortened BCH code $\mathcal{A}_2^2 = [359, 260]_2$, which can correct 11 errors. Then, from Construction 1, we obtain two-level rate-compatible codes $\mathcal{C}_1 = [8191, 7671]_2 \prec \mathcal{C}_2 = [8550, 7671]_2$. Now, send $\mathcal{C}_2$ over a binary symmetric channel (BSC) with crossover probability p. The error probability of $\mathcal{C}_2$ satisfies

$$\begin{aligned} P_e^{(N_2)}(\mathcal{C}_2) &\leqslant 1 - \big(1 - P_e^{(n_1)}(\mathcal{C}_1^2)\big)\big(1 - P_e^{(n_2)}(\mathcal{A}_2^2)\big) \\ &\leqslant 1 - \Big(\sum_{i=0}^{t_1} \binom{n_1}{i} p^i (1-p)^{n_1 - i}\Big)\Big(\sum_{i=0}^{t_2} \binom{n_2}{i} p^i (1-p)^{n_2 - i}\Big), \end{aligned}$$

where $N_2 = 8550$, $n_1 = 8191$, $n_2 = 359$, $t_1 = 60$, and $t_2 = 11$. For instance, for $p = 0.0035$, we compute $P_e^{(N_2)}(\mathcal{C}_2) \leqslant 1.049 \times 10^{-7}$; for $p = 0.004$, we have $P_e^{(N_2)}(\mathcal{C}_2) \leqslant 6.374 \times 10^{-6}$. For $p \geqslant 0.0035$, the performance of $\mathcal{C}_2$ (rate 0.8972) is comparable to, although still worse than, a shortened $[8553, 7671]_2$ BCH code $\mathcal{C}_2'$ that has rate 0.8969 and can correct 63 errors. For instance, for $p = 0.0035$ and 0.004, $\mathcal{C}_2'$ has error probabilities 4.035×10^{-8} and 3.315×10^{-6}. □

V. Capacity-Achieving Rate-Compatible Codes

In this section, we show that if we choose component codes properly, Construction 1 can generate rate-compatible codes which achieve the capacities of a set of degraded q-ary symmetric channels simultaneously.

More specifically, consider a set of M degraded q-ary symmetric channels $W_1 \succ W_2 \succ \cdots \succ W_M$ with crossover probabilities $p_1 < p_2 < \cdots < p_M$ respectively, where $p_1 > 0$ and $p_M < 1-(1/q)$. Let $C(W_i)$ denote the capacity of the channel W_i, i.e., $C(W_i) = 1 - H_q(p_i)$. It is clear that $C(W_1) > C(W_2) > \cdots > C(W_M)$. For any rates $R_1 > R_2 > \cdots > R_M$ such that $R_i < C(W_i)$ for all $1 \leqslant i \leqslant M$, we will show that Construction 1 can generate rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$ where $\mathcal{C}_i = [N_i, R_i N_i]_q$ such that the decoding error probability of each $\mathcal{C}_i$ over channel W_i satisfies $P_e^{(N_i)}(\mathcal{C}_i) \to 0$, as N_i goes to infinity.

To this end, we first present the following lemma on the existence of nested capacity-achieving linear codes. Its proof can be found in the longer version [6].

Lemma 8. *Consider a set of M degraded q-ary symmetric channels $W_1 \succ W_2 \succ \cdots \succ W_M$ with capacities $C(W_1) > C(W_2) > \cdots > C(W_M)$. For any rates $R_1 > R_2 > \cdots > R_M$ such that $R_i < C(W_i)$, there exists a sequence of nested linear codes $\mathcal{C}_1^M = [n, k_M = R_M n]_q \subset \mathcal{C}_1^{M-1} = [n, k_{M-1} = R_{M-1} n]_q \subset \cdots \subset \mathcal{C}_1^1 = [n, k_1 = R_1 n]_q$ such that the decoding error probability of each $\mathcal{C}_1^i$ over channel W_i, under nearest-codeword (ML) decoding, satisfies $P_e^{(n)}(\mathcal{C}_1^i) \to 0$, as n goes to infinity.*

Now, we are ready to construct capacity-achieving rate-compatible codes from Construction 1. To do so, we choose a set of nested capacity-achieving codes to be the component codes, which exist according to Lemma 8.

1) Choose a set of nested capacity-achieving codes $\mathcal{C}_1^M \subset \mathcal{C}_1^{M-1} \subset \cdots \subset \mathcal{C}_1^1 = \mathcal{C}_1 = [n_1, k]_q$, where $\mathcal{C}_1^i = [n_1, n_1 - \sum_{m=1}^{i} v_m]_q$ for $1 \leqslant i \leqslant M$. Let $\mathcal{C}_1^i$ have the required rate $R_i < C(W_i)$, and for $\mathcal{C}_1^i$ over channel W_i, its error probability satisfies $P_e^{(n_1)}(\mathcal{C}_1^i) \to 0$, as n_1 goes to infinity.

2) For ith level, $2 \leqslant i \leqslant M$, choose a set of auxiliary nested capacity-achieving codes $\mathcal{A}_i^M \subset \mathcal{A}_i^{M-1} \subset \cdots \subset \mathcal{A}_i^{i+1} \subset \mathcal{A}_i^i$, where $\mathcal{A}_i^j = [n_i, v_i + \sum_{m=2}^{i-1} \lambda_m^i - \sum_{\ell=i+1}^{j} \lambda_i^\ell]_q$ for $i \leqslant j \leqslant M$. Let $\mathcal{A}_i^j$ have the required rate $R_j < C(W_j)$, and for $\mathcal{A}_i^j$ over channel W_j, the decoding error probability satisfies $P_e^{(n_i)}(\mathcal{A}_i^j) \to 0$, as n_i goes to infinity.

Note that compared to Section IV, here we care about rate and capacity-achieving property, instead of minimum distance, of each component code.

Theorem 9. *With the above component codes, from Construction 1, we obtain a sequence of rate-compatible codes $\mathcal{C}_1 \prec \mathcal{C}_2 \prec \cdots \prec \mathcal{C}_M$, where $\mathcal{C}_i$, $1 \leqslant i \leqslant M$, has length $N_i = \sum_{j=1}^{i} n_j$, dimension $K_i = k$, and rate R_i. Moreover, for each $\mathcal{C}_i$ over channel W_i, it is capacity-achieving, i.e., the error probability $P_e^{(N_i)}(\mathcal{C}_i) \to 0$, as N_i goes to infinity.*

Proof: The proof has two parts. First, we need prove the rate of $\mathcal{C}_i$ is R_i. Second, we can show that the code $\mathcal{C}_i$ can be decoded by i steps. For each step, the decoding error probability goes to zero, as the code length of $\mathcal{C}_i$ goes to infinity. Thus, the error probability $P_e^{(N_i)}(\mathcal{C}_i) \to 0$, as N_i goes to infinity. See the longer version [6] for details. ∎

Remark 3. Polar codes were proved to have the nested capacity-achieving property [7]. Thus, they can be used as the component codes to construct capacity-achieving rate-compatible codes.

When we were preparing this work, we found recent independent works on capacity-achieving rateless and rate-compatible codes based on polar codes [5], [8]. By investigating the construction in [5] carefully, we find our construction with polar codes as component codes is equivalent to theirs by one-to-one mapping the *syndrome* in our construction to the *frozen bits* in their construction by a *full rank* matrix; see the longer version [6] for the proof. Since the construction in [5] is based on the generator matrix, our construction can be seen as another interpretation of their construction from a parity-check matrix perspective.

VI. Conclusion

This work proposed a new algebraic construction for generating rate-compatible codes with increasing minimum distances. We also proved that our construction can be capacity-achieving by using proper component codes, validating the optimality of the construction. With polar codes as component codes, the equivalence between our construction and the one in [5] was identified.

Our construction is very general. Many linear codes (e.g., BCH, RS, and LDPC codes) can be used as its component codes, and some of them were shown as examples. Our parity-check matrix based approach enables us to conveniently obtain the combinatorial property (e.g., minimum distance) of the constructed rate-compatible codes, as well as their decoders.

Acknowledgment

This work was supported by Seagate Technology and NSF Grants CCF-1405119 and CCF-1619053.

References

[1] W. Alltop, "A method for extending binary linear codes," *IEEE Trans. Inf. Theory*, vol. 30, no. 6, pp. 871–872, 1984.
[2] G. I. Davida and S. M. Reddy, "Forward-error correction with decision feedback," *Information and Control*, vol. 21, no. 2, pp. 117–133, 1972.
[3] J. Ha, J. Kim, and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2824–2836, 2004.
[4] J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," *IEEE Trans. Commun.*, vol. 36, no. 4, pp. 389–400, 1988.
[5] S.-N. Hong, D. Hui, and I. Marić, "Capacity-achieving rate-compatible polar codes," in *Proc. IEEE ISIT*, 2016, pp. 41–45.
[6] P. Huang, L. Yi, X. Zhang, P. H. Siegel, and E. F. Haratsch. (2017) Syndrome-coupled rate-compatible error-correcting codes. [Online]. Available: http://arxiv.org/abs/1705.06847
[7] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, Ecole Polytechnique Fédérale de Lausanne, 2009.
[8] B. Li, D. Tse, K. Chen, and H. Shen, "Capacity-achieving rateless polar codes," in *Proc. IEEE ISIT*, 2016, pp. 46–50.
[9] J. Li and K. R. Narayanan, "Rate-compatible low density parity check codes for capacity-approaching ARQ schemes in packet data communications," in *Proc. CIIT*, 2002, pp. 201–206.
[10] S. Lin and D. J. Costello, *Error Control Coding*. Prentice Hall, 2004.
[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, 1977.
[12] R. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.
[13] D. N. Rowitch and L. B. Milstein, "On the performance of hybrid FEC/ARQ systems using rate compatible punctured turbo (RCPT) codes," *IEEE Trans. Commun.*, vol. 48, no. 6, pp. 948–959, 2000.
[14] W. C. Schmid and R. Schürer. (2014) MinT: Table for Linear Codes. [Online]. Available: http://mint.sbg.ac.at/index.php
[15] T. Van Nguyen, A. Nosratinia, and D. Divsalar, "The design of rate-compatible protograph LDPC codes," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 2841–2850, 2012.