On Polarization for the Linear Operator Channel

César Brito and Jörg Kliewer
Klipsch School of Electrical and Computer Engineering
New Mexico State University
Las Cruces, NM, USA
Email: {cob, jkliewer}@nmsu.edu

***Abstract*—We address the problem of reliably transmitting information through a network where the nodes perform random linear network coding and where an adversary potentially injects malicious packets into the network. A good model for such a channel is a linear operator channel, where in this work we employ a combined multiplicative and additive matrix channel. We show that this adversarial channel behaves like a subspace-based symmetric discrete memoryless channel (DMC) under subspace insertions and deletions and typically has an input alphabet with non-prime cardinality. This facilitates the recent application of channel polarization results for DMCs with arbitrary input alphabets by providing a suitable one-to-one mapping from input matrices to subspaces. As a consequence, we show that polarization for this adversarial linear operator channel can be obtained via an element-wise encoder mapping for the input matrices, which replaces the finite field summation in the channel combining step for Arikan's classical polar codes.**

I. Introduction

Channel polarization was proposed by Arikan [1] by constructing a binary block code which achieves the capacity of a binary symmetric memoryless channel. The key idea is to obtain virtual channels by applying a polarizing transform, which either asymptotically converge to an error-free or a completely noisy channel. The fraction of asymptotically error-free channels approaches the symmetric capacity of the original memoryless channel. These ideas have recently been extended to discrete memoryless channels (DMCs) with inputs over arbitrary prime and non-prime alphabets [2–6].

In the following we show that channel polarization can also be applied to a linear operator channel [7], [8] with arbitrary subspace errors and deletions, which to the best of our knowledge has not been addressed in the literature so far. Such a channel is a good model for a network with nodes performing random linear network coding under the action of an adversary, who can inject malicious packets into the network. Despite asymptotically capacity achieving schemes for linear operator channels have recently been presented based on Gabidulin codes (e.g., in [7], [9]), the additional benefit of considering polarization for the operator channel is that this result allows to extend scenarios, where one-dimensional polar codes have proven to be beneficial, to an operator channel framework.

In previous work the capacity of operator channels has been addressed, where in [10] upper and lower bounds for the capacity of operator channels with arbitrary random rank transfer matrices are presented. A similar model is used in [11] with the difference that the transfer matrix is constrained to have full rank. In [12], an exact relation for the capacity of the multiplicative matrix channel (MMC) with constant-rank input is given where the transfer matrix is distributed uniformly for each rank. A more general case is studied in [13] where arbitrary distributions for the transfer matrix are assumed. In contrast, the error model considered in this work extends previous work to a combined MMC and additive matrix channel (AMC) setup.

In particular, we consider a channel model in which we assume that k subspace deletions occur with probability a_k and i subspace errors occur with probability e_i, resp., both determined by the action of the adversary. We provide an exact expression for the capacity of such channel and show that it can asymptotically be obtained by applying a uniform distribution over all the subspaces generated by a full rank input matrix. We show that the resulting combined MMC/AMC subspace channel is symmetric under insertions and deletions and typically has an input alphabet of composite (non-prime) cardinality. This facilitates the recent application of results for polar coding for DMCs with arbitrary input alphabets [4–6] by providing a suitable one-to-one mapping from input matrices, which contain the data injected into the network, to subspace indices. In particular we show that polarization for the linear operator channel case can be obtained by a typically non-linear encoder mapping applied element-wise to the input matrices, which replaces the finite field summation in the channel combining step for Arikan's classical polar codes.

Some remarks about the notation: Fixed matrices and vectors are denoted in boldface, as $\mathbf{A}$ or $\mathbf{a}$, whereas random matrices are denoted in non-boldface capital letters, as A. The (i,j)-th matrix element is indicated by the random variable $A[i,j]$. By $\Pi_A = \langle A \rangle$ we denote the random variable indicating the subspace spanned by the row vectors of the random matrix A, where a specific value of Π_A is denoted as π_A. Further, the Gaussian coefficient $\begin{bmatrix} T \\ n \end{bmatrix}_q \triangleq \prod_{i=0}^{n-1} \frac{q^{T-i}-1}{q^{n-i}-1}$ counts the number of n-dimensional subspaces of a T-dimensional space over a finite field $\mathbb{F}_q$.

II. Adversarial Linear Operator Channel

In the following we consider an adversarial linear operator channel (AOC) which is given by the matrix equation $Y = AX + E$. Here, $A \in \mathbb{F}_q^{n \times n}$ is the channel transfer matrix and

This work was supported in part by the U.S. National Science Foundation under grants CCF-0830666 and CCF-1017632.

assumed to have random rank $r \in [0,\dots,n]$, $X \in \mathbb{F}_q^{n\times T}$ is the input matrix whose rows represent the source packets, and $E \in \mathbb{F}_q^{n\times T}$ is a matrix which incorporates network errors or the injection of malicious packets by an adversary.

In this channel the action of an adversary creates subspace deletions and/or subspace errors, where the case of subspace deletions is modeled as an MMC $Y = AX$ and the case of full rank subspace errors as an AMC $Y = X+E$, respectively. Therefore, the resulting channel can be described as a matrix-based discrete memoryless channel (DMC) $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$ with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$. Note that in general the capacity for the AOC is achieved with an input alphabet consisting of matrices of all ranks, but here we assume $\text{rank}(X) = n$ unless stated otherwise. This limitation is not very restrictive since we will show that as $q \to \infty$ the resulting mutual information terms approach the capacity.

Let e_j, $\sum_{j=0}^{n} e_j = 1$, be the probability that the matrix E inserts j independent subspace vectors into the row space of X for $\text{rank}(A) = n$. Likewise, let a_i, $\sum_{i=0}^{n} a_i = 1$, be the probability of the adversary reducing the rank of A by i. Thus, for $e_0 = 1$ and arbitrary $a_0,\dots,a_n$ the AOC is an MMC, whereas for $a_0 = 1$ and arbitrary $e_0,\dots,e_n$ the AOC becomes a pure AMC. It has been shown that if A is a random matrix, e.g., by representing the system matrix of a network with random linear network coding, the rowspace of the input matrix is preserved if A has full rank n [7], [11]. As a consequence, the AOC can be interpreted as subspace DMC $(\mathcal{X}, W_{\Pi_Y|\Pi_X}, \mathcal{Y})$, where $\langle X\rangle = \Pi_X$ and $\langle Y\rangle = \Pi_Y$ are the corresponding input and output subspaces, resp., and $\mathcal{X}$ and $\mathcal{Y}$ are the corresponding subspace alphabets.

A. Transition probabilities

In the following we describe the transition probabilities of the AOC. As a starting point, consider the quantity

$$\gamma_X(j) \triangleq \binom{n}{j}\begin{bmatrix} T \\ j \end{bmatrix}_q - \binom{n}{j-1}\begin{bmatrix} T \\ j-1 \end{bmatrix}_q. \tag{1}$$

Here, for a given matrix $X \in \mathbb{F}_q^{n\times T}$, $\binom{n}{j}\begin{bmatrix} T \\ j \end{bmatrix}_q$ counts the number of rank j subspaces whose j dimensions can be inserted into n row slots. This term also counts all subspaces of rank v, $0 \le v \le j$, since $j - v$ row vectors can be linearly dependent in X. Therefore, (1) counts the number of subspaces that differ in precisely j dimensions, and $\sum_{j=1}^{n} \gamma_X(j) + 1 = \begin{bmatrix} T \\ n \end{bmatrix}_q$.

The transition probabilities for the AMC/MMC are given as

$$W_{\text{AMC}}(\pi_Y|\pi_X) = \begin{cases} e_0 & \text{if } \pi_Y = \pi_X, \\ \frac{e_j}{\gamma_X(j)} & \text{if } \dim(\pi_Y \cap \pi_X) = n-j \\ & \quad \forall j = 1,\dots,n, \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

$$W_{\text{MMC}}(\pi_Y|\pi_X) = \begin{cases} a_0 & \text{if } \pi_Y = \pi_X, \\ \frac{a_i}{\binom{n}{i}} & \text{if } \pi_y \in \mathcal{S}_{X,n-i}, \\ 0 & \text{otherwise,} \end{cases} \tag{3}$$

where $\mathcal{S}_{X,n-i}$ is the set of all subspaces of X with dimension $n-i$. By combining (2) and (3) we obtain the transition probabilities for the AOC as

$$W_{\Pi_Y|\Pi_X}(\pi_Y|\pi_X) = \begin{cases} a_0 e_0 & \text{if } \pi_Y = \pi_X, \\ \frac{a_0 e_j}{\gamma_X(j)} & \text{if } \dim(\pi_Y \cap \pi_X) = n-j \\ & \quad \forall j = 1,\dots,n, \\ \frac{a_i}{\binom{n}{i}} & \text{if } \pi_y \in \mathcal{S}_{X,n-i}, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

B. Symmetry of the additive matrix subchannel

For the AMC $Y = X + E$ we assume that the rowspace of E trivially intersects the rowspace of X [7], and that the AMC always generates output subspaces with dimension n for full rank input matrices. That means that any deletion of dimensions is solely covered by the MMC. The strong symmetry of this subchannel under full rank inputs can be observed from (2), where each of the $\begin{bmatrix} T \\ n \end{bmatrix}_q$ input symbols has $\begin{bmatrix} T \\ n \end{bmatrix}_q - 1$ transitions each with probability $e_j/\gamma_X(j)$ for $1 \le j \le n$, and one transition to the same output subspace with probability e_0. Likewise, each of the $\begin{bmatrix} T \\ n \end{bmatrix}_q$ output symbols has $\begin{bmatrix} T \\ n \end{bmatrix}_q$ transitions with the same set of transition probabilities as the inputs.

C. Symmetry of the multiplicative matrix subchannel

Note that for the MMC $Y = AX$ there are $\begin{bmatrix} T \\ n \end{bmatrix}_q / \begin{bmatrix} T \\ n-k \end{bmatrix}_q$ possible n-dimensional input subspaces that the channel can rank reduce into a particular $(n-k)$-dimensional output subspace. It is clear that $\begin{bmatrix} T \\ n \end{bmatrix}_q / \begin{bmatrix} T \\ n-k \end{bmatrix}_q$ must be an integer, and the following proposition establishes a sufficient condition on T.

Proposition 1. *The required condition for $\begin{bmatrix} T \\ n \end{bmatrix}_q / \begin{bmatrix} T \\ n-k \end{bmatrix}_q$ being an integer for all possible k imposes $T = c \cdot n! - 1$ where $c \in \mathbb{N}^+$.*

The proof is omitted due to space constraints.

From (3) we observe that there are a total of $|\mathcal{X}| = \begin{bmatrix} T \\ n \end{bmatrix}_q$ subspace inputs and $|\mathcal{Y}| = \sum_{i=0}^{n} \begin{bmatrix} T \\ n-i \end{bmatrix}_q$ subspace outputs. Since each transition has probability $a_i/\binom{n}{i}$, each input subspace symbol has $\sum_{i=0}^{n} \binom{n}{i}$ outgoing channel transitions, and each output subspace symbol of dimension $n-i$ has $\binom{n}{i}\begin{bmatrix} T \\ n \end{bmatrix}_q / \begin{bmatrix} T \\ n-i \end{bmatrix}_q$ incoming channel transitions, which is due to the assumption that the adversary selects $n-i$ subspaces out of n uniformly at random.

This implies that the MMC can be broken up into $n+1$ strongly symmetric subchannels each consisting of all $|\mathcal{X}|$ input subspaces as the input set and an output set with $|\mathcal{Y}_i| = \begin{bmatrix} T \\ n-i \end{bmatrix}_q$ subspaces of fixed rank $n-i$ for $i = 0,\dots,n$ with a_i as the subchannel selection probabilities. By combining these strongly symmetric subchannels the resulting (overall) MMC is shown to be symmetric [14].

D. Capacity

Let $C_{n,\text{AMC}} \triangleq \max_{P_{\Pi_X},\, \text{rank}(X)=n} I(\Pi_X;\Pi_Y)$ be defined as the capacity under the constraint of rank n input matrices, and let $C_{n,\text{MMC}}$ and $C_{n,\text{AOC}}$ be defined likewise. Further, let $C_{n,\text{MMC},i} \triangleq \max_{P_{\Pi_X},\, \text{rank}(X)=n} I(\Pi_X;\Pi_{Y_i})$ be the capacity of the strongly symmetric subchannel with the output alphabet limited to subspaces of dimension $n-i$ and the input constraint

$\text{rank}(X) = n$. By using (2), (3), (4), and the capacity properties of strongly symmetric DMCs [14] we obtain

$$C_{n,\text{AOC}} = a_0 C_{n,\text{AMC}} + \sum_{i=1}^{n} a_i C_{n,\text{MMC},i} \quad \text{with} \tag{5}$$

$$C_{n,\text{AMC}} = \log \begin{bmatrix} T \\ n \end{bmatrix}_q + e_0 \log e_0 + \sum_{j=1}^{n} e_j \log \frac{e_j}{\gamma_X(j)}, \tag{6}$$

$$C_{n,\text{MMC},i} = \log \begin{bmatrix} T \\ n-i \end{bmatrix}_q + \log \frac{1}{\binom{n}{i}} \quad \text{for } 0 \le i \le n, \tag{7}$$

and we note that

$$C_{n,\text{MMC}} = \sum_{i=0}^{n} a_i C_{n,\text{MMC},i}, \tag{8}$$

all with the maximizing distribution P_{Π_x} chosen uniformly over the set of rank n subspaces.

In the following we will show that for $q \to \infty$ uniformly distributed full rank inputs X are sufficient to asymptotically achieve the (unrestricted) capacity for both MMC and AMC.

Proposition 2. *For the AMC we have* $\lim_{q\to\infty} C_{n,AMC} = \lim_{q\to\infty} C_{AMC}$ *for fixed* $T \ge 2n$.

Proof: From [11] we obtain a capacity expression for the AMC based on input and output matrices as

$$\begin{aligned} C_{\text{AMC}} &= \max_{P_X} I(X;Y) \\ &= (T-t)(n-t) + \log_q \prod_{i=0}^{t-1} \frac{1-q^{i-t}}{(1-q^{i-n})(1-q^{i-T})}, \end{aligned} \tag{9}$$

where $t \triangleq \mathbb{E}\{\text{rank}(E)\}$, and C_{AMC} is achieved with P_X uniform over $\mathbb{F}_q^{(n-t)\times(T-t)}$. To show the claim, we first note that in the second term on the right hand side (r.h.s.) in (9) $t, n, T > i$ for all $i = 0, \ldots, t-1$. Thus, for $q \to \infty$, the argument of the log-term approaches one, leading to

$$\lim_{q\to\infty} C_{\text{AMC}} = (T-t)(n-t) = (n-t)T - nt + t^2. \tag{10}$$

In order to compare (10) with $C_{n,\text{AMC}}$ we need to express $C_{n,\text{AMC}}$ in terms of the mutual information between input and output matrices. For large q the term $q^{nd\begin{bmatrix} T \\ d \end{bmatrix}_q}$ describes the number of matrices X of rank d [10]. Applying this to (6) we obtain

$$C_{n,\text{AMC}} = \max_{p_X,\, \text{rank}(X)=n} I(X,Y) \tag{11}$$

$$\begin{aligned} &= \log_q q^{n^2} \begin{bmatrix} T \\ n \end{bmatrix}_q - \sum_{j=1}^{n} e_j \log_q q^{nj} \begin{bmatrix} T \\ j \end{bmatrix}_q + \sum_{j=0}^{n} e_j \log_q e_j \\ &\quad - \sum_{j=1}^{n} e_j \log_q \left[\binom{n}{j} - \binom{n}{j-1} \frac{q^{n(j-1)} \begin{bmatrix} T \\ j-1 \end{bmatrix}_q}{q^{nj} \begin{bmatrix} T \\ j \end{bmatrix}_q} \right]. \end{aligned} \tag{12}$$

One can easily check that for $T \ge 2n$ the last term on the r.h.s. in (12) goes to 0 as $q \to \infty$. By employing $\lim_{q\to\infty} \begin{bmatrix} T \\ n \end{bmatrix}_q = q^{(T-n)n}$ it follows from (12) that

$$\begin{aligned} \lim_{q\to\infty} C_{n,\text{AMC}} &= \log_q q^{n^2} \begin{bmatrix} T \\ n \end{bmatrix}_q - \sum_{j=1}^{n} e_j \log_q q^{nj} \begin{bmatrix} T \\ j \end{bmatrix}_q \\ &= \left(n - \sum_{j=1}^{n} e_j j \right) T - n \sum_{j=1}^{n} e_j j + \sum_{j=1}^{n} e_j j^2. \end{aligned} \tag{13}$$

Comparing (13) with (10) and observing that $\mathbb{E}\{\text{rank}(E)\} = \sum_{j=1}^{n} e_j j = t$ yields the claim. ∎

Proposition 3. *For the MMC we have* $\lim_{q\to\infty} C_{n,MMC} = \lim_{q\to\infty} C_{MMC}$.

Proof: Consider $r = \text{rank}(A)$ which is distributed according to $b_r = \Pr\{\text{rank}(A) = r\}$. Then, by using a subspace-based capacity result from [8] for the MMC with fixed rank for the transfer matrix we obtain with $b_r = a_{n-r}$ that

$$\lim_{q\to\infty} C_{\text{MMC}} = \sum_{r=0}^{n} b_r C_{\text{MMC},r} = \sum_{r=0}^{n} b_r (T-r) r. \tag{14}$$

On the other hand, combining (7) and (8) yields

$$C_{n,\text{MMC}} = \sum_{i=0}^{n} a_i \log_q \begin{bmatrix} T \\ n-i \end{bmatrix}_q + \sum_{i=1}^{n} a_i \log_q \frac{1}{\binom{n}{i}},$$

from which with $\lim_{q\to\infty} \begin{bmatrix} T \\ n \end{bmatrix}_q = q^{(T-n)n}$ we obtain

$$\lim_{q\to\infty} C_{n,\text{MMC}} = \sum_{i=0}^{n} a_i [T-(n-i)](n-i) = \sum_{r=0}^{n} b_r (T-r) r, \tag{15}$$

which coincides with (14). ∎

By combining the results from Proposition 2 and 3 we have the following corollary.

Corollary 4. *The capacity* $C_{AOC} = \max_{P_{\Pi_X}} I(\Pi_X; \Pi_Y)$ *for* $q \to \infty$ *is obtained by full-rank input matrices* X *for fixed* $T \ge 2n$, *i.e.,* $\lim_{q\to\infty} C_{AOC} = \lim_{q\to\infty} C_{n,AOC}$.

It is possible to also show $\lim_{T\to\infty} C_{\text{AOC}} = \lim_{T\to\infty} C_{n,\text{AOC}}$ for all q. We omit these results due to space constraints.

III. Polarization Approach

A. Preliminaries

The key element for polarization is the decomposition of $N \triangleq 2^\eta$, $\eta \in \mathbb{N}$, independent copies of a q-ary symmetric DMC $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$ with symmetric capacity $I(W)$ into N q-ary channels which are either error-free or completely noisy [4–6]. In particular, consider the transformation $\mathbf{G}_N \triangleq \mathbf{B}_N \mathbf{G}_2^{\oplus\eta}$ where $\mathbf{G}_2 \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $\mathbf{B}_N \in \mathbb{F}_2^{N\times N}$ is a bitreversal permutation matrix, and $\oplus$ denotes the Kronecker product. A vector $\mathbf{u} \in \mathbb{F}_q^N$ is then transformed into the codeword $\mathbf{x} = \mathbf{u}\mathbf{G}_N$. A channel splitting operation provides composite channels $(\mathbb{F}_q, W_N^{(i)}, \mathcal{Y}^n \times \mathbb{F}_q^{i-1})$ which are defined by their transition probabilities

$$W_N^{(i)}(\mathbf{y}, \mathbf{u}_1^{i-1} | u_i) \triangleq \frac{1}{q^{N-1}} \sum_{\mathbf{u}_{i+1}^N \in \mathcal{X}^{N-i}} W_{Y|X}(\mathbf{y} | \mathbf{u}\mathbf{G}_N). \tag{16}$$

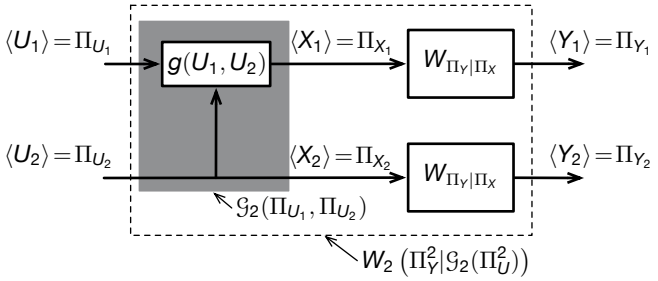

Fig. 1. Initial channel combining step with $W_2(\pi_Y^2|\mathcal{G}_2(\pi_U^2)) = W(\pi_Y|\langle g(U_1,U_2)\rangle)W(\pi_Y|\pi_{U_2})$.

For N large enough, these q-ary symmetric channels *polarize*, i.e., they become either completely noisy or noise-free.

We have shown in Section II that the AOC in (4) behaves like a symmetric DMC $(\mathcal{X}, W_{\Pi_Y|\Pi_X}, \mathcal{Y})$. Therefore, we can apply Arikan's idea of channel combining [1] by considering the one-to-one mapping $U_1, U_2 \to X_1, X_2$ with $X_1 = g(U_1, U_2)$, $X_2 = U_2$, where $U_1, U_2, X_1, X_2 \in \mathbb{F}_q^{n\times T}$, and $g : \mathbb{F}_q^{n\times T} \times \mathbb{F}_q^{n\times T} \to \mathbb{F}_q^{n\times T}$ is an invertible matrix operator which will be clarified in Section III-B. By considering the subspaces $\Pi_{U_i} = \langle U_i\rangle$, $\Pi_{Y_i} = \langle Y_k\rangle$, $i = 1, 2$ we define the subspace operator channels $W^{(1)} : \Pi_{U_1} \to \Pi_Y^2$, $W^{(2)} : \Pi_{U_2} \to \Pi_Y^2\Pi_{U_1}$, where $\Pi_A^N \triangleq [\Pi_{A_1}, \ldots, \Pi_{A_N}]$. These channels are described as

$$W^{(1)}(\pi_Y^2|\pi_{U_1}) = \frac{1}{|\mathcal{X}|}\sum_{\pi_{U_2}\in\mathcal{X}} W(\pi_Y|\langle g(U_1,U_2)\rangle)W(\pi_Y|\pi_{U_2}),$$

$$W^{(2)}(\pi_Y^2, \pi_{U_1}|\pi_{U_2}) = \frac{1}{|\mathcal{X}|}W(\pi_Y|\langle g(U_1,U_2)\rangle)W(\pi_Y|\pi_{U_2}).$$

The underlying channel combining step is shown in Fig. 1 where the input to the combined channel is given as output of a vector operator $\mathcal{G}_2 : \pi_U^2 \to \pi_X^2$. Analogous to (16) we obtain by combining N channels and subsequent channel splitting

$$W_N^{(i)}(\pi_Y^N, \pi_U^{i-1}|\pi_{U_i}) = \frac{1}{|\mathcal{X}|^{N-1}}\sum_{\pi_{U,i+1}^N\in\mathcal{X}^{N-i}} W_N(\pi_Y^N|\mathcal{G}_N(\pi_U^N)) \tag{17}$$

with $\pi_{U,i+1}^N \triangleq [\pi_{U_{i+1}}, \ldots, \pi_{U_N}]$. The N-dimensional vector operator $\mathcal{G}_N : \pi_U^N \to \pi_X^N$ carries out a pairwise application of the operator g whenever a pairwise summation in $\mathbf{u}\mathbf{G}_N$ is performed over $\mathbb{F}_q$ for the case of a scalar q-ary DMC. For $i = 1, \ldots, N$ (17) denotes the channel seen by the subspace π_{U_i} if all previous transmitted subspaces $\pi_{U,i+1}^N$ are available as *a priori* information at a successive cancellation decoder. If N is large enough, the set of channels can be divided into a "good" subset $\mathcal{A}_\delta$ and a "bad" subset $\mathcal{A}_\delta^c$ which are defined as

$$\mathcal{A}_\delta \triangleq \{i : I(W_N^{(i)}) \in (\hat{C} - \delta, \hat{C}]\}, \tag{18}$$

$$\mathcal{A}_\delta^c \triangleq \{i : I(W_N^{(i)}) \in [0, \delta)\}, \quad \delta > 0, \tag{19}$$

where $\hat{C}$ denotes the capacity of a full-rank MMC, which is given by $\hat{C} = \log_q \sum_{k=0}^n \begin{bmatrix} T \\ k \end{bmatrix}_q$ [8], [10], and $I(W_N^{(i)})$ the symmetric capacity of the composite subspace DMCs in (17).

The set of good channels in $\mathcal{A}_\delta$ is now used to transmit input subspaces $\langle U_i\rangle$ uncoded over subspace DMCs $W_N^{(i)}$ generated by matrices $A_i \in \mathbb{F}_q^{n\times n}$ for $i \in \mathcal{A}_\delta$.

We now provide a simple constant dimension code by partitioning the matrix U_i as $U_i = [\mathbf{I}_n\, P_i]$ where $\mathbf{I}_n$ is the $n \times n$ identity matrix and $P_i \in \mathbb{F}_q^{n\times(T-n)}$ [7], [8]. This code is capacity achieving on the full rank MMC with capacity $\hat{C}$.

Proposition 5. *Let $\mathcal{P}(U, n)$ denote the set of all subspaces π_U of $U \in \mathbb{F}_q^{n\times T}$ with dimension n. Consider the set $\mathcal{Q} \subset \mathcal{P}(U, n)$ of spaces $\pi_{U,\ell}$, $\ell = 1, 2, \ldots, |\mathcal{Q}|$ with corresponding generator matrices $U_\ell = [\mathbf{I}_n\, P_\ell]$ where $P_\ell \in \mathbb{F}_q^{n\times(T-n)}$. Then, there exists a one-to-one mapping between $\pi_{U,\ell}$ and P_ℓ with $|\mathcal{Q}| = q^{n(T-n)}$. Further, for $q \to \infty$ and $T \geq 2n$, $U = [\mathbf{I}_n\, P]$ is capacity-achieving on the MMC $Y = AU$ with $A \in \mathbb{F}_q^{n\times n}$ and rank$(A) = n$ with P distributed uniformly over all $q^{n(T-n)}$ possible matrices.*

The proof is a simple consequence of Proposition 3.

B. Polarizing mappings

The next step is to specify the operator g in Fig. 1. Since the subspace input alphabet cardinality of the AOC is given as $|\mathcal{X}| = \begin{bmatrix} T \\ n \end{bmatrix}_q$ the resulting alphabet typically has a composite (non-prime) size. Recently, two approaches have been proposed to deal with the problem of polarization for non-prime source and channel alphabets. The first approach is to consider multilevel polarization [4], [6] where a q-ary word is considered as a collection of individual bit channels which independently polarize. The second approach [5] is based on the observation that for non-prime alphabets any group $(G, +)$ contains a subgroup $(S, +)$ with q-ary summation as group operation [15]. By replacing the summation based channel combining step with an invertible mapping $(U_1, U_2) \to (f(U_1, U_2), U_2)$ where $U_1, U_2, f(U_1, U_2) \in \mathbb{F}_q$, it is shown that a polarizing mapping f exists even for composite alphabets. We will focus on this approach due to the direct applicability to the subspace-based symmetric DMC case.

In particular, it is shown in [5] that f is a polarizing mapping if the following two conditions are satisfied:

(i) f is invertible for mappings $u_1 \to f(u_1, u_2)$ and $u_2 \to f(u_1, u_2)$, respectively.

(ii) For all $2 \leq K \leq q-1$ the matrix $B_{jk} = f(a_j, a_k)$ for $j, k = 0, \ldots, K$–1, $a_j, a_k \in \mathbb{F}_q$ has at least K+1 distinct entries. B is a subset of the Cayley table for $(\mathbb{F}_q, f)$ [15].

Note that condition (ii) enforces all subgroups in $\mathbb{F}_q$ to vanish under the action of the operator f.

By applying an *element-wise* mapping $f(a_j, a_k) = a_j + \pi(a_k)$ based on the permutation $\pi(\cdot)$ [5] to the input matrices in the channel combining step, we can show that polarization for any symmetric operator channel can be achieved for full rank inputs $U \in \mathbb{F}_q^{n\times T}$, $T \geq 2n$.

Proposition 6. *Let $g(U_1, U_2)[j, k] \triangleq f(U_1[j, k], U_2[j, k])$ define the element-wise operation of the mapping $f(U_1[j, k], U_2[j, k]) = U_1[j, k] + \pi(U_2[j, k])$ on the full rank input matrices U_1 and U_2. If the mapping f satisfies conditions (i) and (ii), and $I(W_{\Pi_Y|\Pi_X}) \in (\delta, \hat{C} - \delta)$ for some $\delta > 0$ there exists an $\epsilon(\delta) > 0$ such that*

$$I(W^{(1)}) + \epsilon(\delta) \leq I(W_{\Pi_Y|\Pi_X}) \leq I(W^{(2)}) - \epsilon(\delta), \tag{20}$$

i.e., g is polarizing for the symmetric DMC $W_{\Pi_Y|\Pi_X}$.

Proof: The proof is based on a vectorized version of the proof of [5, Proposition 2], so only a sketch is provided. We employ capacity-achieving input matrices U_i for $q \to \infty$ and the full-rank MMC of the form $U_i = [\mathbf{I}_n\, P_i]$, $P_i \in \mathbb{F}_q^{n\times(T-n)}$, $i = 1, 2$, with a q-ary *element-wise* mapping $g(U_1, U_2)[j, k] = U_1[j, k] + \pi(U_2[j, k])$ satisfying conditions (i) and (ii). Consider the numbers $\hat{u}_i \in \mathbb{F}_{q^{nT}}$, obtained by interpreting the concatenation of all rows of U_i as numbers in $\mathbb{F}_{q^{nT}}$. Note that the Cayley table of size $q^{nT} \times q^{nT}$ of the vectorized (global) mapping $g(\hat{u}_1, \hat{u}_2)$ satisfies condition (ii) if each element-wise mapping $g(U_1, U_2)[j, k]$ in $\mathbb{F}_q$ satisfies (ii) individually. We need to show that for all $2 \le K \le q^{nT} - 1$ and numbers $a_0 < a_1 < \cdots < a_{K-1}$, $a_k \in \mathbb{F}_{q^{nT}}$, $k = 0, \ldots, K-1$, each submatrix of the Cayley table

$$B_{jk} = [a_j^{(0)}, a_j^{(1)}, \ldots, a_j^{(nT-1)}]_{\mathbb{F}_{q^{nT}}} + [\pi(a_k^{(0)}), \pi(a_k^{(1)}), \ldots, \pi(a_k^{(nT-1)})]_{\mathbb{F}_{q^{nT}}}, \quad (21)$$

$j, k = 0, \ldots, K-1$, has at least $K+1$ distinct entries. Here, the numbers a_k are written with their individual q-ary digits $a_k^{(\ell)} \in \mathbb{F}_q$, $\ell \in [0, \ldots, nT-1]$, and $[\cdot]_{\mathbb{F}_{q^{nT}}}$ denotes a number in $\mathbb{F}_{q^{nT}}$.

Exemplarily, we consider the case $K \ge 3$ (the result for $K = 2$ follows similarly), where it suffices to show that the two sets $\{B_{j1}\}$ and $\{B_{j(K-1)}\}$ are not identical for any j. Assume that these sets are identical. Then, there exist numbers $j_1, \ldots, j_L \in \{0, 2, \ldots, K-1\}$ for $L \le K$ such that $B_{1(K-1)} = B_{j_1 1},\ B_{j_1(K-1)} = B_{j_2 1},\ \ldots,\ B_{j_L(K-1)} = B_{11}$. By applying (21) we obtain

$$L\Big([\pi(a_{K-1}^{(0)}), \pi(a_{K-1}^{(1)}), \ldots, \pi(a_{K-1}^{(nT-1)})]_{\mathbb{F}_{q^{nT}}} - [\pi(a_0^{(0)}), \pi(a_0^{(1)}), \ldots, \pi(a_0^{(nT-1)})]_{\mathbb{F}_{q^{nT}}}\Big) = [0, \ldots, 0]_{\mathbb{F}_{q^{nT}}}. \quad (22)$$

However, this is a contradiction since if each element-wise mapping satisfies condition (ii) we must have $\pi(a_{K-1}^{(\ell)}) - \pi(a_0^{(\ell)}) \neq 0$ for all ℓ [5]. Thus, the r.h.s. in (22) cannot be all-zero in general and therefore g is a polarizing mapping. ■

By considering the definition of good and bad channels in (18), (19), (20), and the fact that polarization holds for the q-ary symmetric DMC case [1], [2], [5], the following polarization result follows directly.

Corollary 7. *For all $\delta > 0$ we have*

$$I(W_{\Pi_Y|\Pi_X}) = \lim_{N\to\infty} \frac{|\mathcal{A}_\delta|}{N},\ 1 - I(W_{\Pi_Y|\Pi_X}) = \lim_{N\to\infty} \frac{|\mathcal{A}_\delta^c|}{N}.$$

C. Remarks

By considering a subspace-based successive cancellation decoder, which is analogous to the one for the scalar case, Corollary 7 shows that the AOC capacity C_n under rank(n) input matrices can be asymptotically achieved for $q \to \infty$ and $N \to \infty$ if matrix inputs of the type $U_i = [\mathbf{I}_n\ P_i]$ are applied to the channels for $\mathcal{A}_\delta$. Due to Corollary 4 this also holds for the capacity in the general case where the rank n restriction is removed for the channel inputs. As in Arikan's original polar codes we transmit fixed frozen matrices U_i over those channels for which $i \in \mathcal{A}_\delta^c$, for example all-zero matrices. Note that the choice of an element-wise mapping g for the input matrices significantly simplifies the encoder, compared to a global mapping applied directly to the indices enumerating the *subspaces* $\pi_{U_i} = \langle U_i \rangle$, which must be carried out over a potentially large field size of $\mathbb{F}_{q^{nT}}$. Further, note that the one-to-one mapping between matrix P_i and corresponding subspaces $\pi_{U,i}$ is preserved under the operator g, as $X_1 = g(U_1, U_2)$ can be partitioned as $[g(\mathbf{I}_n, \mathbf{I}_n)\, g(P_1, P_2)]$. Here, $g(\mathbf{I}_n, \mathbf{I}_n)$ serves as a fixed pilot matrix to determine the transfer matrix of the full-rank MMC at the decoder. An example for a suitable element-wise mapping f is given in [5, Proposition 2].

IV. Conclusions

We have shown the applicability of polar coding for q-ary sources and channels to the linear operator channel setting. In particular, we have considered the transmission of subspaces over a combined symmetric multiplicative and additive matrix channel. It was shown that full rank input matrices suffice to achieve the capacity of this channel asymptotically in the field size q. Polarization for block lengths $N \to \infty$ is achieved by applying an element-wise non-linear encoder mapping in the channel combining step, which replaces the q-ary summation in the classical DMC case, and by prepending the input matrix with the identity to achieve capacity on the resulting full-rank (error-free) MMC for $q \to \infty$.

References

[1] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[2] E. Sasoglu, I. E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," in *Proc. IEEE Information Theory Workshop*, Taormina, Italy, Oct. 2009, pp. 144–148.

[3] R. Mori and T. Tanaka, "Channel polarization on q-ary discrete memoryless channels by arbitrary kernels," in *Proc. IEEE Int. Sympos. on Inform. Theory*, Austin, TX, 2010, pp. 894–898.

[4] A. G. Sahebi and S. S. Pradhan, "Multilevel polarization of polar codes over arbitray discrete memoryless channels," in *Proc. 49th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2011, pp. 1718–1725.

[5] E. Sasoglu, "Polar codes for discrete alphabets," in *Proc. IEEE Int. Sympos. on Inform. Theory*, Cambridge, MA, Jul. 2012, pp. 2137–2141.

[6] W. Park and A. Barg, "Polar codes for q-ary channels, $q = 2^r$," in *Proc. IEEE Int. Sympos. on Inform. Theory*, Cambridge, MA, Jul. 2012, pp. 2152–2156.

[7] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[8] D. Silva, F. R. Kschischang, and R. Köetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[9] H. Mahdavifar and A. Vardy, "List-decoding of subspace codes and rank-metric codes up to Singleton bound," in *Proc. IEEE Int. Sympos. on Inform. Theory*, Cambrigde, MA, Jul. 2012, pp. 1493–1497.

[10] M. J. Siavoshani, S. Mohajer, C. Fragouli, and S. N. Diggavi, "On the capacity of noncoherent network coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1046–1066, Feb. 2011.

[11] D. Silva, F. R. Kschischang, and R. Köetter, "Communication over finite-field matrix channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1296–1305, March 2010.

[12] R. W. Nóbrega, B. F. Uchôa-Filho, and D. Silva, "On the capacity of multiplicative finite-field matrix channels," in *Proc. IEEE Int. Sympos. on Inform. Theory*, Saint Petersburg, Russia, Jul. 2011, pp. 341–345.

[13] S. Yang, S.-W. Ho, J. Meng, and E.-H. Yang, "Optimality of subspace coding for linear operator channels over finite fields," in *Proc. IEEE Information Theory Workshop*, Cairo, Egypt, Jan. 2010, pp. 400–404.

[14] R. G. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, Inc., 1968.

[15] M. Artin, *Algebra*. Prentice Hall, 1991.