Countably Infinite Multilevel Source Polarization for Non-Stationary Erasure Distributions

Yuta Sakai Department of ECE, National University of Singapore Email: elevuta@nus.edu.sg

Ken-ichi Iwata University of Fukui Email: k-iwata@u-fukui.ac.jp

Hiroshi Fujisaki Graduate School of Engineering, Graduate School of Natural Science and Technology, Kanazawa University Email: fujisaki@ec.t.kanazawa-u.ac.jp

Abstract—Polar transforms are central operations in the study of polar codes. This paper examines polar transforms for nonstationary memoryless sources on possibly infinite source alphabets. This is the first attempt of source polarization analysis over infinite alphabets. The source alphabet is defined to be a Polish group, and we handle the Arıkan-style two-by-two polar transform based on the group. Defining erasure distributions based on the normal subgroup structure, we give recursive formulas of the polar transform for our proposed erasure distributions. As a result, the recursive formulas lead to concrete examples of multilevel source polarization with countably infinite levels when the group is locally cyclic. We derive this result via elementary techniques in lattice theory.

I. INTRODUCTION

Polar codes were invented by Arıkan [1] as a provably capacity-achieving channel coding technique for binary-input memoryless symmetric channels with low complexity encoding/decoding. The central operation in polar coding is socalled the *polar transform*, which creates worse and better channels than an original channel in a certain sense. It was shown that this coding technique can also be applied to binary source coding problems with side information [2]. Şaşoğlu [3] extended polar source coding from binary to non-binary alphabets. While Sasoğlu's polar transform [3, Definition 4.1] is non-linear in a certain sence, Mori-Tanaka [4] established non-binary polar source coding with linear polar transforms over finite fields. In those studies, the polar transforms asymptotically create either deterministic or equiprobable conditional probability distributions, and these limiting proportions can be fully characterized by the conditional Shannon entropy of the original source. Such a two-level polarization phenomenon is sometimes referred to as strong polarization.¹

A. From Two-Level to Multilevel Polarization

On the other hand, there are studies of investigating polarization phenomena with three or more polarization levels

[5], [7]–[16]. Such a phenomenon is referred to as *multilevel* polarization. Roughly speaking, multilevel polarization means that the polar transform asymptotically creates equiprobable conditional distributions on some cosets of normal subgroups, provided that the polar transform is based on a finite group (cf. [10, Theorem 6] and [15, Theorem V.1]). Unlike twolevel polarization, characterizing the limiting proportions of multilevel polarization still remains an open problem² in general. In this paper, such limiting proportions are referred to as asymptotic distribution of multilevel polarization. In practice, the asymptotic distribution is an important indicator of constructing polar codes [17]. As a special case, the authors of this paper [13], [14] solved the asymptotic distribution for non-binary-input erasure-like channel models proposed in [12]. Particularly, if the input alphabet size is not a prime power, then our previous works [13], [14] give a non-trivial method for calculating the exact asymptotic distribution algorithmically. Recently, Nasser [5] characterized polarization levels, i.e., the support of the asymptotic distribution, for his proposed channels called automorphic-symmetric channels.

B. Binary Operation defining Polar Transform

While the Arıkan-style two-by-two polar transform is always defined on a group of order two³ in the study of binary polar codes, note that it can be defined on several binary operations in the study of non-binary polar codes. Sasoğlu [3, Definition 4.1] considered it based on certain finite quasigroups; Mori-Tanaka [4] on finite fields; Park-Barg [16] on cyclic groups in which those orders are a power of two; Sahebi-Pradhan [15] on finite abelian groups; Nasser–Telatar [10] on finite quasigroups; Nasser–Telatar [11] also on finite abelian groups; Nasser [7], [8] on more weaker finite algebras than quasigroups; Nasser [5] also on finite, not necessarily abelian, groups; and the authors [12]–[14] on finite cyclic groups. It is worth pointing out that by the structure theorem of finite abelian groups, the polar transform based on a finite abelian group can be considered as a polar coding for the multiple-access channel (MAC) [10], [11]. The neccesary and sufficient condition of MACs that the entire capacity region can be achieved by the MAC polarization has

This work is supported in part by JSPS KAKENHI Grant Numbers 26420352; 17K06422; 17J11247; and 18K11465, and a Singapore NRF fellowship (R-263-000-D02-281).

¹Note that the terminology "strong polarization" is somewhat ambiguous in the literature. Mori-Tanaka [4] said that a channel is polarized in a weaker sense if its polar transforms do not behave as the two-level polarization: Nasser [5] said that a channel is strongly polarizing if its polar transforms behave as the two-level polarization; and Błasiok et al. [6, Definition 1.4] defined a meaning of strong polarization in a different way.

²In [9, Section 9.2.1], Nasser raised such an open problem aiming to find a method for calculating the exact or approximated asymptotic distribution of multilevel polarizaiton.

³Groups of order two are unique up to isomorphism.

been characterized by Nasser–Telatar [11] via discrete Fourier analysis over a finite abelian group.

C. Related Problem: Sumset Inequality for Shannon Entropy

Beyond the study of polar codes, bounding some measures and/or entropy of a random variable (r.v.) generated by a group action between two independent r.v.'s are central issues [18]-[25]. This problem is information-theoretically analogous to additive combinatorics or Ruzsa calculus (cf. [26]). Ruzsa [18] and Tao [19] established the sumset and inverse sumset estimates on the Shannon entropy of abelian group-valued r.v.'s with countable order of the group (see also [20]). Kontoyiannis and Madiman [21] extended such estimates to the differential entropy of real-valued r.v.'s, where the group operation is addition of real numbers. Madiman and Kontoviannis [24] further generalized such estimates to the differential entropy of Polish, locally compact, and abelian group-valued r.v.'s, where the probability density functions are defined with respect to a Haar measure. Applications of such sumset inequalities for the Shannon entropy to polar codes have been discussed in the literature [22], [23].

D. Contributions of This Study

In this study, we considers the recursive application of Arıkan-style two-by-two polar transforms based on Polish groups with *possibly infinite* order. This is the first attempt of polarization analysis over infinite alphabets. The main aim of this study is to explore the asymptotic distribution of multilevel polarization. In the context of polar coding for a non-stationary source, we consider a mutually independent, but not necessarily identically distributed, sequence of group-valued r.v.'s with side information. This non-stationary setting is similar to the study of binary polar coding for non-stationary channels [27], [28]. Moreover, examining the asymptotic behavior of the conditional Shannon entropy with the recursive group actions among independent r.v.'s is somewhat related to the study of sumset inequalities for the Shannon entropy [18]–[25].

We tackle this problem by proposing erasure distributions based on the normal subgroup structure of a given group, see Definition 2 of Section III-A. Our group-based erasure distributions are a generalization of Sasoğlu's one [3, Section 3.3.1], which is defined on the binary source alphabet. To simplify our analysis, we derive the recursive formulas of the polar transform for the group-based erasure distributions in Theorem 1 of Section III-B. When the group is locally cyclic, in Theorem 2 of Section IV-B, we give a method of computing the exact asymptotic distribution of multilevel polarization for groupbased erasure distributions. Theorem 2 is proved via the lattice structure of the normal subgroups [29], [30]. These results are more abstractly general than that of the authors' previous works [12]-[14], and the first instance of *countably infinite* polarization levels. We decsribe a relation to our previous works [12]–[14] in Section V-A1; we give the simplest case of countably infinite polarization levels with the Prüfer p-group in Section V-A2.

II. PROBLEM FORMULATION AND BASIC LEMMAS

A. Conditional Distribution and Conditional Shannon Entropy

Let (X, \mathcal{B}) be a standard Borel space, X an (X, \mathcal{B}) -valued r.v., and Y a r.v. Denote by $P_{X|Y}$ a *regular conditional distribution*⁴ of X relative to Y, i.e., it is a r.v. forming a probability measure on (X, \mathcal{B}) almost surely (a.s.) and $P_{X|Y}(B)$ is a version of the conditional probability $\mathbb{P}(X^{-1}(B) | Y)$ for each $B \in \mathcal{B}$. Definition 1 introduces an equivalence relation between two r.v.'s relative to another r.v.

Definition 1. We say that two r.v.'s Y and Z are equivalent relative to an (X, \mathcal{B}) -valued r.v. X, denoted by $Y \equiv_X Z$, if $P_{X|Y}(B) = P_{X|Z}(B)$ a.s. for every $B \in \mathcal{B}$.

Definition 1 can be reduced to the equivalence relation $\stackrel{1}{\sim}$ introduced by Mori–Tanaka [4, p. 2722], provided that X is a finite alphabet. Now, we say that X is *conditionally discrete relative to Y* if there exists a \mathcal{B} -valued r.v. D such that D is countable a.s., and $P_{X|Y}(D) = 1$ a.s. Then, the conditional entropy is defined by

$$H(X \mid Y) \coloneqq \mathbb{E}\bigg[\sum_{x \in \mathcal{X}} P_{X \mid Y}(x) \log \frac{1}{P_{X \mid Y}(x)}\bigg], \tag{1}$$

provided that X is conditionally discrete relative to Y. Here, log stands for the natural logarithm satisfying $0 \log 0 = 0$.

The following lemma is trivial from the definitions.

Lemma 1. If $Y \equiv_X Z$, and if X is conditionally discrete relative to Y or Z, then it holds that

$$H(X \mid Y) = H(X \mid Z).$$
⁽²⁾

Namely, the equivalence relation defined in Definition 1 classifies pairs of r.v.'s having the equal conditional Shannon entropy. Lemma 1 can be straightforwardly extended to a more general conditional quantity [33, Equation (4)].

B. One-Step Polar Transform with a Polish Group

Let *G* be a Polish group with group operation •, i.e., it is a topological group equipped with a complete separable metrizable topology. Here, the group *G* is not necessarily abelian. Denote by \mathcal{B}_G the Borel σ -algebra induced by the Polish topology of *G*. Clearly, the measurable space (G, \mathcal{B}_G) is standard Borel. Assume that the mapping $(g, h) \mapsto g \bullet h$ is Borel-measurable; and consider two independent, but not necessarily identically distributed, (G, \mathcal{B}_G) -valued r.v.'s X_1 and X_2 . The one-step polar transform generates two (G, \mathcal{B}_G) -valued r.v.'s U_1 and U_2 by

$$U_1 = X_1 \bullet X_2, \tag{3}$$

$$U_2 = X_2. \tag{4}$$

The following lemma will be useful to simplify the subsequent analysis on the polar transform (3)–(4) for erasure distributions defined later in Definition 2.

⁴The regular conditional distribution $P_{X|Y}$ always exists, because (X, \mathcal{B}) is standard Borel (see, e.g., [31, Theorem 10.2.2] or [32, Theorem 4.1.17]).

Lemma 2. Given four r.v.'s Y_1 , Y_2 , Z_1 , and Z_2 , suppose that

$$Y_1 \equiv_{X_1} Z_1, \tag{5}$$

$$Y_2 \equiv_{X_2} Z_2, \tag{6}$$

$$(X_1, Y_1, Z_1) \perp (X_2, Y_2, Z_2).$$
 (7)

Then, it holds that

$$(Y_1, Y_2) \equiv_{U_1} (Z_1, Z_2), \tag{8}$$

$$(U_1, Y_1, Y_2) \equiv_{U_2} (U_1, Z_1, Z_2).$$
(9)

Proof of Lemma 2: We first prove $(U_1, Y_1, Y_2) \equiv U_2$ (U_1, Z_1, Z_2) . For each $A_1, A_2 \in \mathcal{B}_G$, it holds that

$$\begin{split} \mathbb{E}[\mathbf{1}_{\{U_{1}\in A_{1}\}}P_{U_{2}|U_{1},Y_{1},Y_{2}}(A_{2}) \mid Y_{1},Y_{2}] \\ \stackrel{(a)}{=} \mathbb{E}[\mathbf{1}_{\{U_{1}\in A_{1}\}}\mathbb{E}[\mathbf{1}_{\{U_{2}\in A_{2}\}} \mid U_{1},Y_{1},Y_{2}] \mid Y_{1},Y_{2}] \\ \stackrel{(b)}{=} \mathbb{E}[\mathbb{E}[\mathbf{1}_{\{(U_{1},U_{2})\in A_{1}\times A_{2}\}} \mid Y_{1},Y_{2}] \mid Y_{1},Y_{2}] \\ \stackrel{(c)}{=} \mathbb{E}[\mathbf{1}_{\{(U_{1},U_{2})\in A_{1}\times A_{2}\}} \mid Y_{1},Y_{2}] \\ \stackrel{(d)}{=} \mathbb{E}[\mathbf{1}_{\{U_{2}\in A_{2}\}}P_{U_{1}|U_{2},Y_{1},Y_{2}}(A_{1}) \mid Y_{1},Y_{2}] \\ \stackrel{(e)}{=} \mathbb{E}[\mathbf{1}_{\{X_{2}\in A_{2}\}}\mathbb{E}[\mathbf{1}_{\{X_{1}\bullet,X_{2}\in A_{1}\}} \mid X_{2},Y_{1},Y_{2}] \mid Y_{1},Y_{2}] \\ \stackrel{(f)}{=} \mathbb{E}[\mathbf{1}_{\{X_{2}\in A_{2}\}}P_{X_{1}|Y_{1}}(A_{1}\bullet X_{2}^{-1}) \mid Y_{1},Y_{2}] \\ \stackrel{(g)}{=} \mathbb{E}[\mathbf{1}_{\{X_{2}\in A_{2}\}}P_{X_{1}|Y_{1}}(A_{1}\bullet X_{2}^{-1}) \mid Y_{1},Y_{2}] \\ \stackrel{(h)}{=} \int_{A_{2}}P_{X_{1}|Y_{1}}(A_{1}\bullet x_{2}^{-1})P_{X_{2}|Y_{1},Y_{2}}(dx_{2}) \\ \stackrel{(i)}{=} \int_{A_{2}}P_{X_{1}|Z_{1}}(A_{1}\bullet x_{2}^{-1})P_{X_{2}|Z_{2}}(dx_{2}) \\ \stackrel{(j)}{=} \int_{A_{2}}P_{X_{1}|Z_{1}}(A_{1}\bullet x_{2}^{-1})P_{X_{2}|Z_{2}}(dx_{2}) \\ \stackrel{(k)}{=} P_{U_{1},U_{2}|Z_{1},Z_{2}}(A_{1}\times A_{2}) \\ \stackrel{(l)}{=} \mathbb{E}[\mathbf{1}_{\{U_{1}\in A_{1}\}}P_{U_{2}|U_{1},Z_{1},Z_{2}}(A_{2}) \mid Z_{1},Z_{2}] \\ (10) \end{split}$$

a.s., where (a) follows by the definition of conditional probabilities; (b) follows from the fact that $\mathbf{1}_{\{U_1 \in A_1\}}$ is $\sigma(U_1, Y_1, Y_2)$ -measurable; (c) follows from the fact that

$$\mathcal{G} \subset \mathcal{H} \implies \mathbb{E}[Z \mid \mathcal{G}] = \mathbb{E}[\mathbb{E}[Z \mid \mathcal{H}] \mid \mathcal{G}] \quad (a.s.) \quad (11)$$

for a real-valued r.v. Z (cf. [34, Theorem 9.1.5]); (d) follows as in (a)–(c); (e) follows by (3)–(4); (f) follows from $X_1 \perp X_2 \mid$ (Y_1, Y_2) together with [34, Theorem 9.2.2]; (g) follows from [34, Theorem 9.2.1] and the fact that $(X_1, Y_1) \perp (X_2, Y_2)$ implies $X_1 \perp Y_2 \mid Y_1$; (h) follows since $P_{X_2|Y_1,Y_2}(\cdot)$ forms a probability measure on (G, \mathcal{B}_G) a.s.; (i) follows from [34, Theorem 9.2.1] and the fact that $(X_1, Y_1) \perp (X_2, Y_2)$ implies $X_2 \perp Y_1 \mid Y_2$; (j) follows by $Y_1 \equiv_{X_1} Z_1$ and $Y_2 \equiv_{X_2} Z_2$; (k) follows as in (d)–(f); and (l) follows as in (a)–(c). Namely, Equation (10) is equivalent to $P_{U_2|U_1,Y_1,Y_2}(A_2) = P_{U_2|U_1,Z_1,Z_2}(A_2)$ a.s. for $A_2 \in \mathcal{B}_G$; and thus, we have $(U_1, Y_1, Y_2) \equiv_{U_2} (U_1, Z_1, Z_2)$, as desired.

We next prove $(Y_1, Y_2) \equiv_{U_1} (Z_1, Z_2)$. By setting $A_2 = G$, it can be verified from (10) that for each $A_1 \in \mathcal{B}_G$,

$$P_{U_1|Y_1,Y_2}(A_1) = \int_G P_{X_1|Y_1}(A_1 \bullet x_2^{-1}) P_{X_2|Y_2}(\mathrm{d}x_2)$$

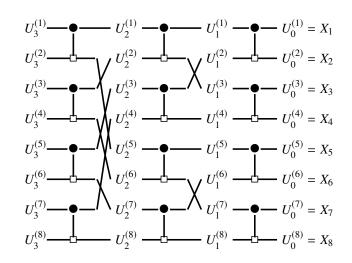


Fig. 1. Recursive construction of polar transforms up to $n \leq 3$ (see (13)–(14)).

$$= \int_{G} P_{X_1|Z_1}(A_1 \bullet x_2^{-1}) P_{X_2|Z_2}(\mathrm{d}x_2)$$

= $P_{U_1|Z_1,Z_2}(A_1)$ (12)

a.s. Thus, we have $(Y_1, Y_2) \equiv_{U_1} (Z_1, Z_2)$, as desired.

Lemma 2 means that the polar transform (3)–(4) preserves the equivalence relation defined in Definition 1. In the context of polar channel codes, as an analoguos result to Lemma 2, the preserving property of a certain channel ordering was firstly shown by Korada [35, Lemma 4.7] (see also [17, Lemma 5]), and its generalization from binary to arbitrary input alphabets was given in [13, Lemma 2] under a quasigroup operation.

C. Recursive Construction of Polar Transforms

This subsection introduces the recursive applications of the polar transform (3)–(4). For a sequence $\{X_i\}_{i=1}^{\infty}$ of (G, \mathcal{B}_G) -valued r.v.'s, we recursively construct the double sequence $\{U_n^{(i)}\}_{i=1,n=0}^{\infty}$ of r.v.'s by⁵

$$U_n^{(2i-1)} \coloneqq U_{n-1}^{(i)} \bullet U_{n-1}^{(i+2^{n-1})}, \tag{13}$$

$$U_n^{(2i)} \coloneqq U_{n-1}^{(i+2^{n-1})} \tag{14}$$

for each $i \ge 1$ and $n \ge 1$, where $\{U_0^{(i)}\}_{i=1}^{\infty} \coloneqq \{X_i\}_{i=1}^{\infty}$. Figure 1 illustrates a diagram of (13) and (14). Note that $U_n^{(i)}$ is also (G, \mathcal{B}_G) -valued for all $n \ge 0$ and $i \ge 1$.

As a non-stationary source with side information, consider a sequence $\{Y_i\}_{i=1}^{\infty}$ of r.v.'s playing the role of side information for $\{X_i\}_{i=1}^{\infty}$. Suppose that the sequence $\{(X_i, Y_i)\}_{i=1}^{\infty}$ is mutually independent. Define the double sequence $\{\mathfrak{H}_n^{(i)}\}_{i=1,n=0}^{\infty}$ of conditional Shannon entropies by

$$\mathfrak{H}_{n}^{(i)} \coloneqq H(U_{n}^{(i)} \mid \{U_{n}^{(j)}\}_{j=1}^{i-1}, \{Y_{j}\}_{j=1}^{\infty})$$
(15)

for each $n \ge 0$ and $i \ge 1$. Roughly speaking, a source polarization theorem explores how the sequence $\{\mathfrak{H}_n^{(i)}\}_{i=1}^{\infty}$ behaves for sufficiently large n. It can

⁵The recursive formulas (13)–(14) for binary-input non-starionary channels can be found in, e.g., [27, Section III] and [28, Equation (7)].

be verified by (13)–(14) that $U_n^{(i)}$ is conditionally independent of $(\{U_n^{(j)}\}_{j=1}^{m2^n}, \{Y_j\}_{j=1}^{m2^n}, \{Y_j\}_{j=(m+1)2^{n+1}}^{\infty})$ relative to $(\{U_n^{(j)}\}_{j=m2^n+1}^i, \{Y_j\}_{j=m2^n+1}^{(m+1)2^n})$, where $m := \lfloor i/2^n \rfloor$, and $\lfloor \cdot \rfloor$ stands for the floor function. Namely, it holds that

$$\mathfrak{H}_{n}^{(i)} = H(U_{n}^{(i)} \mid \{U_{n}^{(j)}\}_{j=m2^{n}+1}^{i-1}, \{Y_{j}\}_{j=m2^{n}+1}^{(m+1)2^{n}}).$$
(16)

The next section analyzes the conditional Shannon entropies $\{\mathfrak{H}_n^{(i)}\}_{i=1,n=0}^{\infty}$ for erasure distributions.

III. POLAR TRANSFORMS FOR ERASURE DISTRIBUTIONS

A. Erasure Distribution Based on Group Structure

It is well-known that the polar transform for binary erasure channels (BECs) can be easily analyzed [1, Proposition 6] by a certain recursive formula. This convenient probabilistic model was translated from channel to source coding problems by Şaşoğlu [3, Section 3.3.1] by defining an *erasure distribution* as an analogy to the BEC. In this subsection, from the group theoretic perspective, we introduce a more general erasure distribution than Şaşoğlu's one.

Let $H \triangleleft G$ be a shorthand for a normal subgroup H of G. The following definition gives an erasure distribution based on the normal subgroup structure of G.

Definition 2 (group-based erasure distribution). Let X be an (G, \mathcal{B}_G) -valued r.v., and Y a \mathcal{Y} -valued r.v., where

$$\mathcal{Y} = \bigcup_{H \triangleleft G: H \text{ is finite}} \frac{G}{H} = \{g \bullet H \mid g \in G \text{ and finite } H \triangleleft G\}.$$

Then, we say that (X, Y) follows an erasure distribution if

$$P_{X|Y}(B) = \frac{|B \cap Y|}{|Y|} \quad (a.s.), \qquad \text{for } B \in \mathcal{B}_G.$$
(17)

The alphabet \mathcal{Y} given in Definition 2 is the collection of finite cosets of G, and note that $X \in Y$ a.s. if (X, Y) follows an erasure distribution. Intuitively, this means that the side information Y only tells us that X belongs to a finite coset Y. It is clear that X is conditionally discrete relative to Y if (X, Y) follows an erasure distribution, because $P_{X|Y}$ is a uniform distribution on a finite coset Y a.s. (see (17)).

If the order of G is two, then Definition 2 coincides with Şaşoğlu's one [3, Section 3.3.1]. Moreover, Definition 2 can be reduced to some know erasure-like channels as follows.

Remark 1. Let (X, Y) a pair of r.v.'s following an erasure distribution in the sense of Definition 2. Suppose that

$$\mathbb{P}\{Y = g \bullet H \mid Y \in G/H\} = \mathbb{P}\{Y = H \mid Y \in G/H\}$$
(18)

for every $g \in G$ and every finite $H \triangleleft G$, provided that $\mathbb{P}{Y \in G/H} > 0$. If G is a finite cyclic group, then the joint probability measure induced by (X, Y) is equivalent to a modular arithmetic erasure channel [13, Definition 2] with uniform input distribution. As summarized in [13, Examples 1– 4], modular arithmetic erasure channels can be further reduced to many other erasure-like channels given in [15], [36]. In addition, if G is a finite elementary abelian group, then the joint probability measure induced by (X, Y) is equivalent to a combination of linear channels [13, Definition 23] with uniform input distribution, where the linear channels are constructed on the set of subspaces of a finite-dimensional vector space over the prime field.

Lemma 3 shows a simple formula for H(X | Y) for an erasure distribution; it can be directly proven by (1) and Definition 2.

Lemma 3. If (X, Y) follows an erasure distribution, then

$$H(X \mid Y) = \mathbb{E}[\log |Y|]. \tag{19}$$

It is worth pointing out that Lemma 3 is analogous to [10, Proposition 3] and [13, Proposition 2].

B. Reduction of Polar Transforms to Erasure Distributions

Suppose that (X_i, Y_i) follows an erasure distribution for $i \ge 1$. Let $\{Y_n^{(i)}\}_{i=1,n=0}^{\infty}$ be a double sequence of r.v.'s defined by⁶

$$Y_n^{(2i-1)} \coloneqq Y_{n-1}^{(i)} \bullet Y_{n-1}^{(i+2^{n-1})}, \tag{20}$$

$$Y_n^{(2i)} \coloneqq \phi(U_n^{(2n-1)}, Y_{n-1}^{(i)}, Y_{n-1}^{(i+2^{n-1})})$$
(21)

for each $i \ge 1$ and $n \ge 1$, where $\{Y_0^{(i)}\}_{i=1}^{\infty} \coloneqq \{Y_i\}_{i=1}^{\infty}$, and the mapping $\phi : G \times \mathcal{Y} \times \mathcal{Y} \to \mathcal{Y} \cup \{\emptyset\}$ is defined by

$$\phi: (g, a \bullet H, b \bullet K) \mapsto (a^{-1} \bullet g \bullet H) \cap (b \bullet K)$$
(22)

for $a, b, g \in G$ and finite $H, K \triangleleft G$. Theorem 1 shows that like the BEC [1, Proposition 6], the polar transform for erasure distributions generates other erasure distributions again.

Theorem 1. The pair $(U_n^{(i)}, Y_n^{(i)})$ also follows an erasure distribution for each $i \ge 1$ and $n \ge 0$. In addition, for each $n \ge 0$ and $i \ge 1$, and with $m := \lfloor i/2^n \rfloor$, it holds that

$$Y_n^{(i)} \equiv_{U_n^{(i)}} \left(\{U_n^{(j)}\}_{j=m2^n+1}^{i-1}, \{Y_j\}_{j=m2^n+1}^{(m+1)2^n} \right).$$
(23)

Corollary 1. If (X_i, Y_i) follows an erasure distribution, then

$$\mathfrak{H}_n^{(i)} = \mathbb{E}[\log |Y_n^{(i)}|] \qquad \text{for } n \ge 0, \ i \ge 1.$$

Proof of Theorem 1: By Lemma 2 and the recursivity of (13)–(14), it suffices to consider the one-step polar transform (3)–(4). Next, we prove Theorem 1 in two parts:

1) Proof for Minus Transform $(U_1, (Y_1, Y_2))$: Since X_1 and X_2 are conditionally discrete relative to Y_1 and Y_2 , respectively, it follows by the first equality of (12) that

$$P_{U_1|Y_1,Y_2}(A_1) = \sum_{u_2 \in G} P_{X_1|Y_1}(A_1 \bullet u_2^{-1}) P_{X_2|Y_2}(u_2)$$

=
$$\sum_{u_1 \in A_1} \sum_{u_2 \in G} P_{X_1|Y_1}(u_1 \bullet u_2^{-1}) P_{X_2|Y_2}(u_2) \quad (25)$$

a.s. for every $A_1 \in \mathcal{B}_G$. Thus, we see that U_1 is conditionally discrete relative to (Y_1, Y_2) as well. It follows from (17) that

$$P_{X_1|Y_1}(u_1 \bullet u_2^{-1}) P_{X_2|Y_2}(u_2) = \frac{\mathbf{I}_{\{u_1 \bullet u_2^{-1} \in Y_1\} \cap \{u_2 \in Y_2\}}}{|Y_1||Y_2|}$$
(26)

a.s. for every $(u_1, u_2) \in G^2$. Now, we readily see that for some $u_1, u_2, g_1, g_2 \in G$ and $H, K \triangleleft G$, both $u_1 \bullet u_2^{-1} \in g_1 \bullet H$ and

⁶Assume w.l.o.g. that
$$Y_n^{(2i)} \coloneqq \{e\}$$
 if $\phi(U_n^{(2n-1)}, Y_{n-1}^{(i)}, Y_{n-1}^{(i+2^{n-1})}) = \emptyset$.

 $u_2 \in g_2 \bullet K$ hold if and only if the following system of two congruences holds:

$$\begin{cases} u_2 \equiv g_1^{-1} \bullet u_1 \quad (\text{mod } H), \\ u_2 \equiv g_2 \quad (\text{mod } K). \end{cases}$$
(27)

By the Chinese Remainder Theorem in group theory, the system (27) has a unique solution $u_2 \in G$ modulo $H \cap K$ if and only if $u_1 \equiv g_1 \bullet g_2 \pmod{H \bullet K}$. Therefore, we have

$$\{u_2 \in G \mid (u_1 \bullet u_2^{-1}, u_2) \in Y_1 \times Y_2\} \in \frac{G}{H \cap K}$$
 (28)

if and only if $Y_1 \in G/H$, $Y_2 \in G/K$, and $u_1 \in Y_1 \bullet Y_2$. Hence, it follows from (25), (26), and (28) that for each $A_1 \in \mathcal{B}_G$,

$$P_{U_{1}|Y_{1},Y_{2}}(A_{1}) = \sum_{u_{1} \in A_{1} \cap (Y_{1} \bullet Y_{2})} \sum_{u_{2} \in \phi(U_{1},Y_{1},Y_{2})} \frac{1}{|Y_{1}| |Y_{2}|}$$
$$= \sum_{u_{1} \in A_{1} \cap (Y_{1} \bullet Y_{2})} \frac{|\phi(U_{1},Y_{1},Y_{2})|}{|Y_{1}| |Y_{2}|}$$
$$= \frac{|A_{1} \cap (Y_{1} \bullet Y_{2})|}{|Y_{1} \bullet Y_{2}|}$$
(29)

a.s., where the last equality follows by the identity⁷

$$|H \bullet K| |H \cap K| = |H| |K| \tag{30}$$

for finite $H, K \triangleleft G$. Equation (29) implies that $(U_1, (Y_1, Y_2))$ follows an erasure distribution (see (17)). Furthermore, since $Y_1 \bullet Y_2$ is a function of (Y_1, Y_2) , we see that $\sigma(Y_1 \bullet Y_2) \subset \sigma(Y_1, Y_2)$. Hence, it can be verified by (11) and (29) that

$$Y_1 \bullet Y_2 \equiv_{U_1} (Y_1, Y_2), \tag{31}$$

completing the proof for minus transform.

2) Proof for Plus Transform $(U_2, (U_1, Y_1, Y_2))$: Since X_1 and X_2 are conditionally discrete relative to Y_1 and Y_2 , respectively, it follows as in Steps (a)–(i) of (10) that for each $A_1, A_2 \in \mathcal{B}_G$,

$$\mathbb{E}[\mathbf{1}_{\{U_{1}\in A_{1}\}}P_{U_{2}|U_{1},Y_{1},Y_{2}}(A_{2}) | Y_{1},Y_{2}]$$

$$= \sum_{u_{1}\in A_{1}}\sum_{u_{2}\in A_{2}}P_{X_{1}|Y_{1}}(u_{1} \bullet u_{2}^{-1})P_{X_{2}|Y_{1}}(u_{2})$$

$$\stackrel{(a)}{=}\sum_{u_{1}\in A_{1}\cap(Y_{1}\bullet Y_{2})}\sum_{u_{2}\in A_{2}\cap\phi(U_{1},Y_{1},Y_{2})}\frac{1}{|Y_{1}||Y_{2}|}$$

$$= \sum_{u_{1}\in A_{1}\cap(Y_{1}\bullet Y_{2})}\frac{|A_{2}\cap\phi(U_{1},Y_{1},Y_{2})|}{|Y_{1}||Y_{2}|}$$

$$\stackrel{(b)}{=}\sum_{u_{1}\in A_{1}\cap(Y_{1}\bullet Y_{2})}\frac{P_{U_{1}|Y_{1},Y_{2}}(u_{1})}{P_{U_{1}|Y_{1},Y_{2}}(u_{1})}\frac{|A_{2}\cap\phi(U_{1},Y_{1},Y_{2})|}{|Y_{1}||Y_{2}|}$$

$$\stackrel{(c)}{=}\sum_{u_{1}\in A_{1}\cap(Y_{1}\bullet Y_{2})}P_{U_{1}|Y_{1},Y_{2}}(u_{1})\frac{|A_{2}\cap\phi(U_{1},Y_{1},Y_{2})|}{|\phi(U_{1},Y_{1},Y_{2})|}$$

$$\stackrel{(d)}{=}\mathbb{E}\Big[\mathbf{1}_{\{U_{1}\in A_{1}\}}\frac{|A_{2}\cap\phi(U_{1},Y_{1},Y_{2})|}{|\phi(U_{1},Y_{1},Y_{2})|}||Y_{1},Y_{2}\Big] \quad (32)$$

a.s., where (a) follows from (26) and (28); (b) follows from the fact that $P_{U_1|Y_1,Y_2}(u_1) > 0$ if and only if $u_1 \in Y_1 \bullet Y_2$ (see (29)); (c) follows from (29)–(30); and (d) follows from the

7Consider the second isomorphism theorem without the topological structure.

fact that $P_{U_1|Y_1,Y_2}(\cdot)$ forms a uniform distribution on $Y_1 \bullet Y_2$ a.s. Therefore, it holds that for each $A_2 \in \mathcal{B}_G$,

$$P_{U_2|U_1,Y_1,Y_2}(A_2) = \frac{|A_2 \cap \phi(U_1,Y_1,Y_2)|}{|\phi(U_1,Y_1,Y_2)|}$$
(33)

a.s. Equation (33) implies that $(U_2, (U_1, Y_1, Y_2))$ follows an erasure distribution. Furthermore, since $\phi(U_1, Y_1, Y_2)$ is a function of (U_1, Y_1, Y_2) , it holds that $\sigma(\phi(U_1, Y_1, Y_2)) \subset \sigma(U_1, Y_1, Y_2)$. Hence, it can be verified by (11) and (33) that

$$\phi(U_1, Y_1, Y_2) \equiv_{U_2} (U_1, Y_1, Y_2), \tag{34}$$

completing the proof for plus transform.

Proof of Corollary 1: Corollary 1 is now obvious from Lemmas 1–3 and Theorem 1.

If the order of G is two, then Theorem 1 can be reduced to the discussion in [3, Section 3.3.1], which is alanogous to the ease of analysing the polar transform for BECs [1, Proposition 6]. As shown in the following remark, Theorem 1 is indeed a generalization of the known formulas in easy case studies of Arıkan-style two-by-two polar transforms.

Remark 2. For a source $\{(X_i, Y_i)\}_{i=1}^{\infty}$, suppose the same hypothesis as Remark 1. If G is a finite cyclic group, then Theorem 1 is a counterpart of the recursive formula for modular arithmetic erasure channels [13, Theorem 1]. In addition, if G is a finite elementary abelian group, then Theorem 1 is a counterpart of the recursive formula for combinations of linear channels [10, Proposition 4] in a stationary setting.

By Corollary 1, the probability measures induced by $\{|Y_n^{(i)}|\}_{i=1}^{\infty}$ are important to analyze the asymptotic distribution of multilevel polarization for sufficiently large *n*. The next section explores the asymptotic distribution in a special case.

IV. MULTILEVEL SOURCE POLARIZATION ANALYSIS

A group *G* is said to be *locally cyclic* if every finitely generated subgroup of *G* is cyclic. In this section, we investigate the multilevel polarization theorem for a non-stationary source $\{(X_i, Y_i)\}_{i=1}^{\infty}$, where (X_i, Y_i) follows an erasure distribution with a locally cyclic group *G* for each $i \ge 1$.

A. Theorem 1 with a Locally Cyclic Group

It is known that every locally cyclic group is isomorphic to a subgroup of the additive rationals \mathbb{Q} or of the additive quotient group \mathbb{Q}/\mathbb{Z} . Namely, the order of every locally cyclic group must be countable; and thus, it is worth mentioning that any subset of a locally cyclic Polish group *G* is Borel.

Fix an index $i \ge 1$. Since every finite subgroup of a locally cyclic group is cyclic, and since every cyclic group of order k is isomorphic to $\mathbb{Z}/k\mathbb{Z}$ under addition, we observe that (i) every locally cyclic group G has at most a countable number of finite normal subgroups $N \triangleleft G$; and (ii) $|Y_i| = k$ if and only if $Y_i \in G/N$ with $N \cong \mathbb{Z}/k\mathbb{Z}$. Hence, it follows that $\mathbb{P}\{|Y_i| = k\} = \mathbb{P}\{Y_i \in G/N \text{ for some } N \text{ isomorphic to } \mathbb{Z}/k\mathbb{Z}\}$, and Lemma 3 can be rewritten by

$$H(X \mid Y) = \sum_{N \triangleleft G: N \text{ is finite}} (\log |N|) \mathbb{P}\{Y_i \in G/N\}.$$
(35)

Namely, the probability $\mathbb{P}{Y_i \in G/N}$ is important in the subsequent analysis. Actually, if we define $\varepsilon_n^{(i)}(N) := \mathbb{P}\{Y_n^{(i)} \in G/N\}$ for each $i \ge 1$, $n \ge 0$, and finite $N \triangleleft G$, then it follows from Theorem 1 that for every $i \ge 1$, $n \ge 1$ and finite $N \triangleleft G$,

$$\varepsilon_n^{(2i-1)}(N) = \sum_{H, K \triangleleft G: H \bullet K = N} \varepsilon_{n-1}^{(i)}(H) \, \varepsilon_{n-1}^{(i+2^{n-1})}(K), \qquad (36)$$

$$\varepsilon_n^{(2i)}(N) = \sum_{H, K \triangleleft G: H \cap K = N} \varepsilon_{n-1}^{(i)}(H) \, \varepsilon_{n-1}^{(i+2^{n-1})}(K). \tag{37}$$

Based on the recursive formulas (36)–(37), we observe from Corollary 1 and (35) that for each $i \ge 1$ and $n \ge 0$,

$$\mathfrak{H}_{n}^{(i)} = \sum_{N \triangleleft G: N \text{ is finite}} (\log |N|) \, \varepsilon_{n}^{(i)}(N). \tag{38}$$

10 11

B. Asymptotic Distribution of Multilevel Polarization

In the previous subsection, the calculations of $\{\mathfrak{H}_n^{(i)}\}_{i=1,n=0}^{\infty}$ have been simplified to (38) via (36)-(37). Based on this, we now give a multilevel polarization theorem for erasure distributions with a locally cyclic group G. To formalize it, we now introduce some notations and definitions as follows:

For each finite $N \triangleleft G$, denote by $\mathcal{S}(N)$ the collection of overgroups $H \triangleright N$ satisfying the following two conditions: (i) there exists a $K \triangleleft G$ satisfying the proper subgroup chain $N \triangleleft K \triangleleft H$ and (ii) there are no distinct $K_1, K_2 \triangleleft G$ satisfying the proper subgroup chain $N \triangleleft K_1 \triangleleft K_2 \triangleleft H$. Moreover, for each finite $N \triangleleft G$ and $H \in \mathcal{S}(N)$, denote by $\mathcal{M}(N, H)$ the collection of finite subgroups $K \triangleleft G$ satisfying the proper subgroup chain $N \triangleleft K \triangleleft H$. These notations will be used in Algorithm 1 later. For each finite $N \triangleleft G$, define

$$Q(N) \coloneqq \lim_{m \to \infty} \frac{1}{m} \sum_{i=1}^{m} \mathbb{P}\{Y_i \in G/N\},\tag{39}$$

provided that the limit exists. Henceforth, assume that the limit Q(N) always exists for each finite $N \triangleleft G$, and $Q(N) \coloneqq 0$ if N is infinite. This existence of limits is a similar assumption to [27, Remark 1] in the study of polar codes for non-stationary channels, which can be considered as the existence of entropy rate for a sequence of independent r.v.'s (see also [28]). The following example shows some simple cases of (39).

Example 1. If $\{(X_i, Y_i)\}_{i=1}^{\infty}$ is a stationary source with generic distribution $P_{X,Y}$, i.e., if $P_{X_i,Y_i} = P_{X,Y}$ for all $i \ge 1$, then it is clear that $Q(H) = \mathbb{P}\{Y \in G/H\}$. Similarly, if Y_i converges in distribution to Y as $i \to \infty$, then it follows from the Cesáro mean that $Q(H) = \mathbb{P}\{Y \in G/H\}$.

It is clear that $Q(\cdot)$ forms a discrete probability distribution on the set of normal subgroups of G. As will be seen in Theorem 2 and Algorithm 1, the distribution $Q(\cdot)$ plays a significant role to characterize the asymptotic distribution of multilevel source polarization. For each $H, K, N \triangleleft G$, we define

$$\chi(N, K, H) \coloneqq \sum_{J \triangleleft G: J \bullet N = J \bullet K, J \cap H = J \cap K} Q(J), \qquad (40)$$

$$\beta(N,H) := \sum_{J \triangleleft G: J \cap H = J \cap N} Q(J).$$
(41)

Algorithm 1: Solving $\mu(N)$ used in (43) of Theorem 2

Data: A locally cyclic group G; a finite normal subgroup $N \triangleleft G$; and a distribution $Q(\cdot)$ defined in (39)

Kesuft: Probability masses {
$$\mu(H)$$
} $_{H \lhd N}$
1 $\alpha \leftarrow 0$; $K \leftarrow \{e\}$; and $\mu(H) \leftarrow 0$ for all $H \lhd N$
2 while $K \lhd N$ do
3 if $S(K)$ is nonempty then
4 $(H_1, H_2) \leftarrow \arg \max_{(K_1, K_2): K_1 \in S(K), K_2 \in \mathcal{M}(K, K_1)} \chi(K, K_2, K_1)$
5 $\mu(K) \leftarrow \beta(K, H_1) - \alpha$
6 if there exists $H_3 \in \mathcal{M}(K, H_1)$ s.t. $H_3 \neq H_2$ then
7 $\lfloor \mu(K) \leftarrow \mu(K) + \chi(K, H_3, H_1)$
8 $K \leftarrow H_2$
9 else if there exists an overgroup $H \triangleright K$ then
10 $\mu(K) \leftarrow \beta(K, H) - \alpha$
11 $K \leftarrow H$
12 else
13 $\lfloor \mu(K) \leftarrow 1 - \alpha$
14 $\lfloor \alpha \leftarrow \alpha + \mu(K)$

The definitions (40)–(41) will be also used in Algorithm 1. Finally, according to (15), we define

$$\mathfrak{H}_{n}^{(i)}[N] \coloneqq H(U_{n}^{(i)} \bullet N \mid \{U_{n}^{(j)}\}_{j=1}^{i-1}, \{Y_{j}\}_{j=1}^{\infty})$$
(42)

for each $i \ge 1$, $n \ge 0$, and $N \triangleleft G$. Since $U_n^{(i)} \bullet N$ is a function of $U_n^{(i)}$, it is clear that $\mathfrak{H}_n^{(i)}[N] \le \mathfrak{H}_n^{(i)}$ for each $N \triangleleft G$. In addition, we readily see that $\mathfrak{H}_n^{(i)}[G] = 0$ and $\mathfrak{H}_n^{(i)}[\{e\}] = \mathfrak{H}_n^{(i)}$, where $e \in G$ stands for the identity element of G.

The following theorem characterizes the asymptotic distribution of multilevel polarization for a non-stationary source following erasure distributions.

Theorem 2. For any $\delta > 0$ and finite $N \triangleleft G$, it holds that

$$\lim_{n \to \infty} \lim_{m \to \infty} \frac{1}{m 2^n} \left| \left\{ 1 \le i \le m 2^n : \mathfrak{H}_n^{(i)}[N] < \delta, \\ \left| \mathfrak{H}_n^{(i)} - \log |N| \right| < \delta \right\} \right| = \mu(N), \quad (43)$$

where $\mu(N)$ can be exactly calculated by Algorithm 1.

In (43), the limit with respect to *m* is taken due to the non-stationarity of the source and the dependence of r.v.'s induced by the polar transforms (13)–(14), see Section III-B. Here, note that the number m plays a similar role to that of Section III-B; however, it is not given as $m := \lfloor i/2^n \rfloor$ but given as independent of n in Theorem 2.

We shall prove Theorem 2 by employing elementary techniques in lattice theory [30]. Basic notions and definitions in lattice theory can be found in Appendix A.

Proof of Theorem 2: Since the lattice of normal subgroups of a group is distributive if and only if the group is locally cyclic (cf. [29, Theorem 4 of Chapter 3]), it suffices to consider a distributive lattice (L, \lor, \land, \le) . Define the double sequence $\{\boldsymbol{\varepsilon}_n^{(i)}\}_{i=1,n=0}^{\infty}$ of probability vectors $\boldsymbol{\varepsilon}_n^{(i)} \coloneqq \{\boldsymbol{\varepsilon}_n^{(i)}(j)\}_{j \in L}$ by

$$\varepsilon_n^{(2i-1)}(j) \coloneqq \sum_{k,l \in L: k \lor l=j} \varepsilon_{n-1}^{(i)}(k) \, \varepsilon_{n-1}^{(i+2^{n-1})}(l), \tag{44}$$

$$\varepsilon_n^{(2i)}(j) \coloneqq \sum_{k,l \in L: k \land l=j} \varepsilon_{n-1}^{(i)}(k) \varepsilon_{n-1}^{(i+2^{n-1})}(l)$$
(45)

for each $i \ge 1$ and $n \ge 1$, where $\{\varepsilon_0^{(i)}\}_{i=1}^{\infty} := \{\varepsilon_i\}_{i=1}^{\infty}$ is a given initial probability vector. Note that (44) and (45) correspond to (36) and (37), respectively. To analyze the probability vectors $\varepsilon_n^{(i)}$, we further define partial sums of elements in $\varepsilon_n^{(i)}$ by

$$\theta_n^{(i)}(a,b) \coloneqq \sum_{j \in L: j \lor a = j \lor b} \varepsilon_n^{(i)}(j), \tag{46}$$

$$\chi_n^{(i)}(a,c,b) \coloneqq \sum_{\substack{j \in L: j \lor a = j \lor c, j \land b = j \land c}} \varepsilon_n^{(i)}(j), \tag{47}$$

$$\beta_n^{(i)}(a,b) \coloneqq \sum_{j \in L: j \land a = j \land b} \varepsilon_n^{(i)}(j) \tag{48}$$

for each $a, b, c \in L$. When elements $a, b \in L$ are clear from the context, we simply write (46)–(48) as $\theta_n^{(i)}$, $\chi_n^{(i)}(c)$, and $\beta_n^{(i)}$. By defining

$$\mathcal{M}(a,b) \coloneqq \{c \in L \mid a < c < b\}$$

$$\tag{49}$$

for each $a, b \in L$, we can show the following lemma.

Lemma 4. Let $a, b \in L$ be chosen so that a < b and there is no pair $x, y \in L$ satisfying a < x < y < b. If (L, \leq) is modular, then it holds that

$$\theta_n^{(i)} + \beta_n^{(i)} + \sum_{c \in \mathcal{M}(a,b)} \chi_n^{(i)}(c) = 1$$
(50)

for every $a, b \in L$, $i \ge 1$, and $n \ge 0$.

Proof of Lemma **4**: See Appendix **B**.

Note that every distributive lattice is modular. Lemma 4 means that the probability masses of $\varepsilon_n^{(i)}$ are well-partitioned by (46)–(48). Let *a* and *b* be chosen so that a < b and there is no pair $x, y \in L$ satisfying a < x < y < b. If (L, \leq) is modular, then $|\mathcal{M}(a, b)|$ can be an arbitrary nonnegative integer. Particularly, if (L, \leq) is distributive, then it can be verified that $0 \leq |\mathcal{M}(a, b)| \leq 2$. Noting this fact, we can observe:

Lemma 5. Let (L, \leq) be a distributive lattice, and let $a, b \in L$ be chosen so that a < b. Suppose that there is no pair $x, y \in L$ satisfying a < x < y < b. Then, it holds that

$$\theta_n^{(2i-1)} = \theta_{n-1}^{(i)} + \theta_{n-1}^{(i+2^{n-1})} - \theta_{n-1}^{(i)} \theta_{n-1}^{(i+2^{n-1})} + C_n^{(i)}, \tag{51}$$

$$\beta_n^{(2l-1)} = \beta_{n-1}^{(l)} \beta_{n-1}^{(l+2)},$$
(52)
$$\theta_{-1}^{(2l)} = \theta_{-1}^{(l)} \theta_{-1}^{(l+2^{n-1})},$$
(53)

$$\begin{aligned}
\theta_n &= \theta_{n-1} \,\theta_{n-1} , \\
\beta_n^{(2i)} &= \beta_{n-1}^{(i)} + \beta_{n-1}^{(i+2^{n-1})} - \beta_{n-1}^{(i)} \,\beta_{n-1}^{(i+2^{n-1})} + C_n^{(i)} \end{aligned}$$
(54)

for every $n \ge 1$ and $i \ge 1$, where

$$C_n^{(i)} \coloneqq \sum_{c_1, c_2 \in \mathcal{M}(a, b): c_1 \neq c_2} \chi_{n-1}^{(i)}(c_1) \chi_{n-1}^{(i+2^{n-1})}(c_2).$$
(55)

Moreover, if there exists an $x \in L$ satisfying $a \prec x \prec b$, then it holds that

$$\chi_{n}^{(2i-1)}(c) = \chi_{n-1}^{(i)}(c) \chi_{n-1}^{(i+2^{n-1})}(c) + \chi_{n-1}^{(i)}(c) \beta_{n-1}^{(i+2^{n-1})} + \beta_{n-1}^{(i)} \chi_{n-1}^{(i+2^{n-1})}(c), \quad (56)$$

$$\chi_{n}^{(2i)}(c) = \chi_{n-1}^{(i)}(c) \chi_{n-1}^{(i+2^{n-1})}(c) + \chi_{n-1}^{(i)}(c) \theta_{n-1}^{(i+2^{n-1})} + \theta_{n-1}^{(i)} \chi_{n-1}^{(i+2^{n-1})}(c)$$
(57)

for every $n \ge 1$, every $i \ge 1$ and every $c \in \mathcal{M}(a, b)$.

Since the positive divisors of a positive integer form a distributive lattice, Lemma 5 is a generalization of [13, Lemma 6] from a lattice of positive divisors with the stationary source setting to general distributive lattices with the non-stationary source setting. Therefore, as in [13, Lemma 7], we can obtain the following lemma.

Lemma 6. Let (L, \leq) be a distributive lattice, and let $a, b \in L$ be chosen so that a < b. Suppose that there is no pair $x, y \in L$ satisfying a < x < y < b. Then, it holds that

$$\theta_n^{(2i-1)} + \theta_n^{(2i)} = \theta_{n-1}^{(i)} + \theta_{n-1}^{(i+2n-1)} + C_n^{(i)}, \tag{58}$$

$$\beta_n^{(2i-1)} + \beta_n^{(2i)} = \beta_{n-1}^{(i)} + \beta_{n-1}^{(i+2^{n-1})} + C_n^{(i)}$$
(59)

for every $n \ge 1$ and $i \ge 1$. Moreover, if there exists an $x \in L$ satisfying a < x < b, then it holds that

$$\chi_n^{(2i-1)}(c) + \chi_n^{(2i)}(c) = \chi_{n-1}^{(i)} \left(1 - \chi_{n-1}^{(i+2^{n-1})} \right) + \chi_{n-1}^{(i+2^{n-1})} \left(1 - \chi_{n-1}^{(i)} \right)$$
(60)

Proof of Lemma 6: Lemma 6 is a direct consequence from Lemmas 4 and 5.

Based on this observation, we can prove Theorem 2 in a similar fashion to [13, Section IV].

V. CONCLUDING REMARKS

We have explored the asymptotic distribution of multilevel source polarization over possibly infinite source alphabets by defining a convenient probabilistic model called an erasure distribution, which is defined in Definition 2. The analysis of Arıkan-style two-by-two polar transforms (13)–(14) based on a Polish group was simplified by Theorem 1 establishing recursive formulas of the polar transforms for erasure distributions. When the group is locally cyclic, Theorem 2 and Algorithm 1 give a method for calculating the exact asymptotic distributions. This is the first instance of multilevel source polarization with countably infinite levels, which is characterized by the structure of distributive lattices.

A. Simple Instances of Theorem 2

In the following, we mention two examples of Theorem 2. 1) Modular Arithmetic Erasure Channels: As explained in Remarks 1 and 2, the erasure distribution defined in Definition 2 can be reduced to the modular arithmetic erasure channel [13, Definition 2], provided that G is a finite cyclic group. Since every cyclic group is locally cyclic, Theorem 2 can also be reduced to the authors' previous results [13], [14], which is described in a stationary setting. 2) *Prüfer p-group:* Let $p \ge 2$ be a prime number. The *Prüfer p-group G* can be defined by the Sylow *p*-subgroup of \mathbb{Q}/\mathbb{Z} up to isomorphism, i.e., $G \simeq \{m/p^n + \mathbb{Z} \mid m \in \mathbb{Z} \text{ and } n \in \mathbb{Z}_{\ge 0}\}$. It is known that $H \triangleleft K$ or $K \triangleleft H$ for any $H, K \triangleleft G$, provided that *G* is the Prüfer *p*-group. Thus, Corollary 2 can simplify Theorem 2 without Algorithm 1.

Corollary 2. Suppose that G is the Prüfer p-group. For any $\delta > 0$ and finite $N \triangleleft G$, and $Q(\cdot)$ as in (39), it holds that

$$\lim_{n \to \infty} \lim_{m \to \infty} \frac{1}{m \, 2^n} \left| \left\{ 1 \le i \le m \, 2^n : \mathfrak{H}_n^{(i)}[N] < \delta, \\ \left| \mathfrak{H}_n^{(i)} - \log |N| \right| < \delta \right\} \right| = Q(N).$$
(61)

Therefore, the source polarization for erasure distributions can be simply characterized by the initial condition (39) without any other compulation method like Algorithm 1, provided that G is the Prüfer *p*-group. This gives a simple and concrete instance of countably infinite polarization levels.

B. Future Works

We have shown a possibility of multilevel polarization phenomena over infinite alphabets. Multilevel polarization analysis for more general source distributions than erasure distributions is an open problem; and inventing practical encoding/decoding schemes with the infinite polarization levels is also of interest in the study of source coding over an infinite source alphabet.

While Theorem 2 can be reduced to the authors' previous results [13], [14] as discussed in Section V-A1, it cannot be reduced to Nasser–Telatar's case study [10, Section VIII], because an elementary abelian group is not locally cyclic in general (cf. Remarks 1 and 2). Generalizing Theorem 2 from locally cyclic to abelian, or not necessarily abelian, groups is highly of interest in terms of the MAC polarization [10], [11].

ACKNOWLEDGEMENTS

The authors would like to thank to Dr. Jun Muramatsu for his helpful discussions; Dr. Mine Alsan for her valuable comments greatly improving this paper; and the anonymous reviewers in ISIT'19 for carefully reading this paper and for giving many valuable advices.

Appendix A

BRIEF INTRODUCTION TO LATTICE THEORY

Definition 3 (partially ordered sets; posets). For a binary relation \leq on a nonempty set L, the system (L, \leq) is called a poset if it satisfies the following three properties: (i) $a \leq a$; (ii) $a \leq b$ and $b \leq a$ imply that a = b; and (iii) $a \leq b$ and $b \leq c$ imply that $a \leq c$, for all $a, b, c \in L$.

Let (L, \leq) be a poset. As a strict relation, the binary relation a < b is a shorthand for $a \leq b$ and $a \neq b$.

Definition 4 (predecessors and followers). For two elements $a, b \in L$ of a poset (L, \leq) , we say that b covers a, or a is covered by b, if a < b and there is no $x \in L$ such that a < x < b. This relation is denoted by a < b.

For each $a, b \in L$, an *upper bound* of a and b is an element $u \in L$ satisfying $a \leq u$ and $b \leq u$; and a *least upper bound* s of a and b is an upper bound of a and b satisfying $s \leq u$ for every upper bound u of a and b. If a least upper bound s of a and b exists, then it is unique; and thus, it can be denoted by $a \lor b := s$, provided that it exists. Analogously, for each $a, b \in L$, a *lower bound* of a and b is an element $l \in L$ satisfying $l \leq a$ and $l \leq b$; and a *greatest lower bound* i of a and b is an upper bound of a and b satisfying $l \leq i$ for every lower bound i of a and b. If a greatest lower bound i of a and b exists, then it is unique; and thus, it can be denoted by $a \lor b := i$, provided that it exists.

Definition 5 (lattices). A poset (L, \leq) is called a lattice if every two elements $a, b \in L$ have the least upper bound $a \lor b$ and the greatest lower bound $a \land b$.

Given a lattice (L, \leq) , the binary operations \lor and \land are called a *join* and a *meet*, respectively, and the lattice is sometimes denoted by (L, \lor, \land, \leq) . These binary operations \lor and \land satisfy the following identities:

Lemma 7 ([30, Lemma 1 in page 8]). Let (L, \leq) be a lattice. For every $a, b, c \in L$, it holds that

- (i) $a \lor b = b \lor a$ and $a \land b = b \land a$;
- (ii) $a \lor (b \lor c) = (a \lor b) \lor c$ and $a \land (b \land c) = (a \land b) \land c$; and (iii) $a \lor (a \land b) = a \land (a \lor b) = a$.

We now give the notion of modularity as follows:

Definition 6 (modular lattices; [30, Section 7 of Chapter I]). A lattice (L, \leq) is said to be modular if $a \leq c$ implies that $a \lor (b \land c) = (a \lor b) \land c$ for every $a, b, c \in L$.

We readily see that Definition 6 is equivalent to the following two identities:

$$[(x \land y) \lor z] \land y = (x \land y) \lor (z \land y), \tag{62}$$

$$[(x \lor y) \land z] \lor y = (x \lor y) \land (z \lor y).$$
(63)

We next give the notion of distributivity as follows:

Definition 7 (distributive lattices; [30, Section 6 of Chapter I]). A lattice (L, \leq) is said to be distributive if

$$a \lor (b \land c) = (a \lor b) \land (a \lor c), \tag{64}$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \tag{65}$$

for every $a, b, c \in L$.

Note that every distributive lattice is modular, but there is a modular lattice which is not distributive. Finally, we give the following lemma under the distributivity.

Lemma 8. Let (L, \leq) be a distributive lattice, and let $a, b \in L$ be chosen so that $a \leq b$. Then, it holds that

$$j \wedge a = j \wedge b$$
 and $k \wedge a = k \wedge b$ (66)

if and only if

$$(j \lor k) \land a = (j \lor k) \land b, \tag{67}$$

for every $j, k \in L$.

Proof of Lemma <mark>8</mark>:

1) If part \Leftarrow : We readily see that

$$j \wedge a = [(j \vee k) \wedge j] \wedge a$$

= $[(j \vee k) \wedge a] \wedge j$
= $[(j \vee k) \wedge b] \wedge j$
= $[(j \vee k) \wedge j] \wedge b$
= $j \wedge b.$ (68)

The identity $k \wedge a = k \wedge b$ can be shown similarly; and these imply the sufficiency, as desired.

2) Only if part \Rightarrow : We readily see that

$$(j \lor k) \land a = (j \land a) \lor (k \land a)$$
$$= (j \land b) \lor (k \land b)$$
$$= (j \lor k) \land b, \tag{69}$$

which implies the necessity, as desired.

While Lemma 8 is elementary, this lemma is important in proving Theorem 2. Note that Lemma 8 does not hold, provided that a lattice (L, \leq) is modular but not distributive.

Appendix B

Proof of Lemma 4

Let $a, b \in L$ be chosen so that a < b, and let $i \in L$ be an arbitrary element. Since $a \wedge b = a < b = a \lor b$, note that $i \lor a \le i \lor b$ and $i \land a \le i \land b$. If $i \lor a = i \lor b$, then

$$a = (i \land a) \lor a$$

$$\leq (i \land b) \lor a$$

$$\stackrel{(a)}{=} (i \lor a) \land b$$

$$= (i \lor b) \land b$$

$$= b, \qquad (70)$$

where (a) follows by the modularity (see Definition 6). As a < b, this implies that $i \land a \neq i \land b$; and therefore, since $i \land a \leq i \land b$, it follows that $i \land a < i \land b$ if $i \lor a = i \lor b$. Similarly, it can be dually verified that $i \lor a < i \lor b$ if $i \land a = i \land b$. Therefore, we have

$$\{j \in L \mid j \lor a = j \lor b\} \cap \{k \in L \mid k \land a = k \land b\} = \emptyset.$$
(71)

On the other hand, if $i \lor a < i \lor b$ and $i \land a < i \land b$, then it holds that $a < (i \land b) \lor a < b$, which implies the existence of $x \in L$ satisfying a < x < b.

We first consider the case where there is no $x \in L$ satisfying a < x < b, i.e., suppose that a < b. Then, the set $\mathcal{M}(a, b)$ defined in (49) is empty, and we observe that

$$\{\{j \in L \mid j \lor a = j \lor b\}, \{k \in L \mid k \land a = k \land b\}\}$$
(72)

forms a partition of *L*. Therefore, since $\varepsilon_n^{(i)}$ is a probability vector for each $n \ge 0$ and $i \ge 1$, it follows from (46)–(48) that Lemma 4 holds, provided that a < b.

We next consider the case where there is at least one $x \in L$ such that a < x < b. Then, the set $\mathcal{M}(a, b)$ defined in

(49) is nonempty. Moreover, it follows by the modularity of Definition 6 that a < y < b for every $y \in \mathcal{M}(a, b)$. Hence, we observe that neither $c_1 \le c_2$ nor $c_2 \le c_1$ for every distinct $c_1, c_2 \in \mathcal{M}(a, b)$. If $i \lor a = i \lor b$, then it is clear that $i \lor c = i \lor b$ for every $c \in \mathcal{M}(a, b)$; and it follows that

$$a = (i \land a) \lor a$$

$$\leq (i \land c) \lor a$$

$$= (i \lor a) \land c$$

$$= (i \lor c) \land c$$

$$= c$$
(73)

for every $c \in \mathcal{M}(a, b)$, which implies that $i \wedge a < i \wedge c$ for every $c \in \mathcal{M}(a, b)$. Similarly, if $i \wedge a = i \wedge b$, then it can be dually verified that $i \vee c < i \vee b$ and $i \wedge c = i \wedge a$ for every $c \in \mathcal{M}(a, b)$. Now, suppose that $i \vee a < i \vee b$ and $i \wedge a < i \wedge b$. As shown in the two paragraphs back, there exists $c \in \mathcal{M}(a, b)$ such that

$$a < c = (i \land b) \lor a < b.$$
(74)

For such an element $c = (i \land b) \lor a = (i \lor a) \land b$, it holds that

$$i \wedge c = i \wedge [(i \wedge b) \vee a]$$

$$\stackrel{(a)}{=} (i \wedge b) \vee (i \wedge a)$$

$$= i \wedge b$$
(75)

$$i \lor c = i \lor [(i \lor a) \land b]$$

$$\stackrel{\text{(b)}}{=} (i \lor a) \land (i \lor b)$$

$$= i \lor a,$$
(76)

where (a) and (b) follow from (62) and (63), respectively. For each $c \in \mathcal{M}(a, b)$, define

$$S(c) \coloneqq \{x \in L \mid x \lor a = x \lor c \text{ and } x \land b = x \land c\}.$$
(77)

We now prove by contradiction that $S(c_1) \cap S(c_2) = \emptyset$ for every distinct $c_1, c_2 \in \mathcal{M}(a, b)$. That is, suppose that there exists an element $d \in L$ satisfying $d \in S(c_1) \cap S(c_2)$. Then, we observe that

$$c_{1} \stackrel{(a)}{=} c_{1} \wedge b$$

$$\stackrel{(b)}{\leq} (d \vee c_{1}) \wedge b$$

$$\stackrel{(c)}{=} (d \vee c_{2}) \wedge b$$

$$\stackrel{(d)}{=} (d \wedge b) \vee c_{2}$$

$$\stackrel{(e)}{=} (d \wedge c_{2}) \vee c_{2}$$

$$\stackrel{(f)}{=} c_{2}, \qquad (78)$$

where (a) follows from $c_1 < b$; (b) follows from $c_1 \le d \lor c_1$; (c) follows from $d \in S(c_1) \cap S(c_2)$, i.e., $d \lor c_1 = d \lor a = d \lor c_2$; (d) follows from $c_2 \le b$ and the modular equality (6); (e) follows from $d \in S(c_1) \cap S(c_2)$, i.e., $d \land c_1 = d \land b = d \land c_2$; and (f) follows from the absorption law: $(x \land y) \lor y = y$. This, however,

contradicts to $c_1 \not\leq c_2$. Therefore, we have $S(c_1) \cap S(c_2) = \emptyset$. Concluding discussions of this paragraph, we observe that

$$\emptyset = \{j \in L \mid j \lor a = j \lor b\} \cap \{k \in L \mid k \land a = k \land b\}$$
(79)

$$= \{j \in L \mid j \lor a = j \lor b\} \cap S(c)$$

$$(80)$$

$$= \{k \in L \mid k \land a = k \land b\} \cap S(c)$$

$$(81)$$

$$= S(c_1) \cap S(c_2) \tag{82}$$

for every $c \in \mathcal{M}(a, b)$ and every distinct $c_1, c_2 \in \mathcal{M}(a, b)$; and

$$\bigcup_{c \in \mathcal{M}(a,b)} S(c)$$

= $\left(\{ j \in L \mid j \lor a = j \lor b \} \cup \{ k \in L \mid k \land a = k \land b \} \right)^{\complement},$
(83)

where \mathcal{A}^{C} stands for the complement of a set \mathcal{A} . Thus, we have that

$$\{\{j \in L \mid j \lor a = j \lor b\}, \{k \in L \mid k \land a = k \land b\}\} \cup \{S(c) \mid c \in \mathcal{M}(a, b)\}$$
(84)

forms a partition of *L*. Therefore, since $\varepsilon_n^{(i)}$ is a probability vector for each $n \ge 0$ and $i \ge 1$, it follows from (46)–(48) that Lemma 4 holds, provided that there exists an $x \in L$ satisfying a < x < b. This completes the proof of Lemma 4.

Appendix C Proof of Lemma 5

By the duality between the join \lor and the meet \land , it suffices to prove the identities of Lemma 5 only for the minus transforms (44). Let $a, b \in L$ be chosen so that a < b. A direct calculation shows

$$\begin{split} \beta_{n}^{(2i-1)} &\stackrel{(a)}{=} \sum_{\substack{j \in L: \\ j \land a = j \land b}} \varepsilon_{n}^{(2i-1)}(j) \\ &\stackrel{(b)}{=} \sum_{\substack{j \in L: \\ j \land a = j \land b}} \sum_{\substack{k,l \in L: \\ k \lor l = j}} \varepsilon_{n-1}^{(i)}(k) \varepsilon_{n-1}^{(i+2^{n-1})}(l) \\ &= \sum_{\substack{k,l \in L: \\ (k \lor l) \land a = (k \lor l) \land b}} \varepsilon_{n-1}^{(i)}(k) \varepsilon_{n-1}^{(i+2^{n-1})}(l) \\ &\stackrel{(c)}{=} \sum_{\substack{k \in L: \\ k \land a = k \land b}} \varepsilon_{n-1}^{(i)}(k) \sum_{\substack{l \in L: \\ l \land a = l \land b}} \varepsilon_{n-1}^{(i+2^{n-1})}(l) \\ &= \beta_{n-1}^{(i)} \beta_{n-1}^{(i+2^{n-1})} \end{split}$$
(85)

for every $n \ge 1$ and $i \ge 1$, where (a) follows from (48); (b) follows from (44); and (c) follows from Lemma 8.

Suppose that there is at least one $x \in L$ such that a < x < b, i.e., *b* covers *x* and *x* covers *a*. For each $c \in \mathcal{M}(a, b)$, we have

$$\chi_{n}^{(2i-1)}(c) \stackrel{(a)}{=} \sum_{\substack{j \in L: \\ j \lor a = j \lor c, \\ j \land b = j \land c}} \varepsilon_{n}^{(2i-1)}(j)$$

$$\stackrel{(b)}{=} \sum_{\substack{i \in L: \\ i \lor c = i \lor a, \\ k \lor l = j}} \sum_{\substack{k,l \in L: \\ n-1}} \varepsilon_{n-1}^{(i)}(k) \varepsilon_{n-1}^{(i+2^{n-1})}(l)$$

$$+ \sum_{\substack{k,l \in L: \\ k \land c = k \land b, \\ l \land c = l \land b, \\ k \lor c = k \lor a, \\ l \lor c = l \lor a}} \varepsilon_{n-1}^{(i)}(k) \varepsilon_{n-1}^{(i+2^{n-1})}(l)$$

$$= \beta_{n-1}^{(i)} \chi_{n-1}^{(i+2^{n-1})}(c) + \chi_{n-1}^{(i)}(c) \beta_{n-1}^{(i+2^{n-1})}$$

$$+ \chi_{n-1}^{(i)}(c) \chi_{n-1}^{(i+2^{n-1})}(c)$$

$$(86)$$

for every $n \ge 1$ and $i \ge 1$, where (a) follows from (47); (b) follows from (44); (c) follows from the fact that $j \lor a = j \lor b$ implies $j \lor c = j \lor a$, as shown in the proof of Lemma 4; (d) follows from Lemma 8; and (e) follows from the fact that (i) $k \land c = k \land b$ implies $k \lor a < k \lor b$ and (ii) $j \land c = j \land b$ and $j \lor a < j \lor b$ imply $j \lor c = j \lor a$, as shown in the proof of Lemma 4.

Finally, we observe that

$$\begin{aligned} \theta_n^{(2i-1)} &\stackrel{(a)}{=} 1 - \left(\beta_n^{(2i-1)}(a,b) + \sum_{c \in \mathcal{M}(a,b)} \chi_n^{(2i-1)}(c) \right) \\ &\stackrel{(b)}{=} 1 - \left(\beta_{n-1}^{(i)} \beta_{n-1}^{(i+2^{n-1})} + \sum_{c \in \mathcal{M}(a,b)} \chi_n^{(2i-1)}(c) \right) \\ &\stackrel{(c)}{=} 1 - \left(\beta_{n-1}^{(i)} \beta_{n-1}^{(i+2^{n-1})} + \sum_{c \in \mathcal{M}(a,b)} \left(\beta_{n-1}^{(i)} \chi_{n-1}^{(i+2^{n-1})}(c) + \chi_{n-1}^{(i)}(c) \beta_{n-1}^{(i+2^{n-1})} + \chi_{n-1}^{(i)}(c) \chi_{n-1}^{(i+2^{n-1})}(c) \right) \right) \end{aligned}$$

$$\stackrel{\text{(d)}}{=} 1 - \left(\beta_{n-1}^{(i)} \beta_{n-1}^{(i+2^{n-1})} + \beta_{n-1}^{(i)} \sum_{c \in \mathcal{M}(a,b)} \chi_{n-1}^{(i+2^{n-1})}(c) + \beta_{n-1}^{(i+2^{n-1})} \sum_{c \in \mathcal{M}(a,b)} \chi_{n-1}^{(i)}(c) - C_n^{(i)} + \left(\sum_{c \in \mathcal{M}(a,b)} \chi_{n-1}^{(i)}(c) \right) \left(\sum_{c \in \mathcal{M}(a,b)} \chi_{n-1}^{(i+2^{n-1})}(c) \right) \right)$$

$$= 1 + C_n - \left(\beta_{n-1} + \sum_{c \in \mathcal{M}(a,b)} \chi_{n-1}(c)\right) \times \left(\beta_{n-1}^{(i+2^{n-1})} + \sum_{c \in \mathcal{M}(a,b)} \chi_{n-1}^{(i+2^{n-1})}(c)\right)$$
^(e) 1 - C⁽ⁱ⁾ - (1 - C⁽ⁱ⁾) (1 - C^(i+2^{n-1}))

$$= 1 + C_n^{(i)} - \left(1 - \theta_{n-1}^{(i)}\right) \left(1 - \theta_{n-1}^{(i+2^{-1})}\right) = \theta_{n-1}^{(i)} + \theta_{n-1}^{(i+2^{n-1})} - \theta_{n-1}^{(i)} \theta_{n-1}^{(i+2^{n-1})} + C_n^{(i)},$$
(87)

where (a) follows from Lemma 4; (b) follows from (85); (c) follows from (86); (d) follows from (55); and (e) follows from Lemma 4. This completes the proof of Lemma 5.

References

- E. Arıkan, "Channel polarization: A method for constructing capacityachieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
- [2] —, "Source polarization," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 13–18.
- [3] E. Şaşoğlu, "Polarization and polar codes," Found. Trends Commun. Inf. Theory, vol. 8, no. 4, pp. 259–381, Oct. 2012.

- [4] R. Mori and T. Tanaka, "Source and channel polarization over finite fields and Reed–Solomon matrices," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2720–2736, May 2014.
- [5] R. Nasser, "On the polarization levels of automorphic-symmetric channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Paris, France, Jul. 2019, [Online]. Available at https://arxiv.org/abs/1811.05203.
- [6] J. Błasiok, V. Guruswami, P. Nakkiran, A. Rudra, and M. Sudan, "General strong polarization," Feb. 2018, [Online]. Avaibalbe at https://arxiv.org/ abs/1802.02718.
- [7] R. Nasser, "An ergodic theory of binary operations—Part I: Key properties," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 6931–6952, Dec. 2016.
- [8] —, "An ergodic theory of binary operations—Part II: Applications to polarization," *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 1063–1083, Feb. 2017.
- [9] —, "Polarization and channel ordering: Characterizations and topological structures," Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2017.
- [10] R. Nasser and E. Telatar, "Polarization theorems for arbitrary DMCs and arbitrary MACs," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 2917–2936, Jun. 2016.
- [11] ——, "Fourier analysis of MAC polarization," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3600–3620, Jun. 2017.
- [12] Y. Sakai and K. Iwata, "A generalized erasure channel in the sense of polarization for binary erasure channels," in *Proc. IEEE Inf. Theory Workshop*, Cambridge, UK, Sept. 2016.
- [13] Y. Sakai, K. Iwata, and H. Fujisaki, "Modular arithmetic erasure channels and their multilevel channel polarization," Apr. 2018, submitted to *IEEE Trans. Inf. Theory*, [Online]. Available at https://arxiv.org/abs/1804.09016.
- [14] —, "Asymptotic distribution of multilevel channel polarization for a certain class of erasure channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, Jun. 2018, pp. 856–860.
- [15] A. G. Sahebi and S. S. Pradhan, "Multilevel channel polarization for arbitrary discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7839–7857, Dec. 2013.
- [16] W. Park and A. Barg, "Polar codes for q-ary channels, q = 2^r," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 955–969, Feb. 2013.
- [17] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6562–6582, Oct. 2013.
- [18] I. Z. Ruzsa, "Sumsets and entropy," *Random Struct. Alg.*, vol. 34, no. 1, pp. 1–10, 2009.
- [19] T. Tao, "Sumset and inverse sumset theory for Shannon entropy," *Combin. Probab. Comput.*, vol. 19, no. 4, pp. 603–639, Jan. 2010.
- [20] M. Madiman, A. W. Marcus, and P. Tetali, "Entropy and set cardinality inequalities for partition-determined functions," *Random Struct. Alg.*, vol. 40, no. 4, pp. 399–424, Jul. 2012.
- [21] I. Kontoyiannis and M. Madiman, "Sumset and inverse sumset inequalities for differential entropy and mutual information," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4503–4514, Aug. 2014.
- [22] V. Guruswami and A. Velingker, "An entropy sumset inequality and polynomially fast convergence to Shannon capacity over all alphabets," in *Proc. 30th Conf. Comput. Complex.*, Portland, Oregon, USA, Jun. 2015, pp. 42–57.
- [23] E. Abbe, J. Li, and M. Madiman, "Entropies of weighted sums in cyclic groups and an application to polar codes," *Entropy*, vol. 19, no. 9, Sept. 2017.
- [24] M. Madiman and I. Kontoyiannis, "Entropy bounds on abelian groups and the Ruzsa divergence," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 77–92, Jan. 2018.
- [25] J. Li and M. Madiman, "A combinatorial approach to small ball inequalities for sums and differences," *Combin. Probab. Comput.*, vol. 28, no. 1, pp. 100–129, Jan. 2019.
- [26] T. Tao and V. Vu, Additive Combinatorics. Cambridge, UK: Cambridge University Press, 2006.
- [27] M. Alsan and E. Telatar, "A simple proof of polarization and polarization for non-stationary memoryless channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 9, pp. 4873–4878, Sept. 2016.
- [28] H. Mahdavifar, "Polar coding for non-stationary channels," Dec. 2018, [Online]. Available at https://arxiv.org/abs/1611.04203v3.
- [29] O. Ore, "Structures and group theory II," *Duke Math. J.*, vol. 4, no. 2, pp. 247–269, 1938.
- [30] G. Birkhoff, *Lattice Theory*, 3rd ed. Providence: American Mathematical Society, 1967.

- [31] R. M. Dudley, *Real Analysis and Probability*. Cambridge, UK: Cambridge University Press, 2002.
- [32] R. Durrett, Probability: Theory and Examples, 5th ed. Cambridge, UK: Cambridge University Press, 2019.
- [33] Y. Sakai, "Fano-type inequalities based on general conditional information measures over countably infinite alphabets with list decoding," Dec. 2018, submitted to *IEEE Trans. Inf. Theory*, [Online]. Available at https://arxiv.org/abs/1801.02876v6.
- [34] K. L. Chung, *A Course in Probability Theory*, 3rd ed. San Diego: Academic Press, 2001.
- [35] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2009.
- [36] W. Park and A. Barg, "The ordered Hamming metric and ordered symmetric channels," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Peterburg, Russia, Aug. 2011, pp. 2283–2287.