Spatially-Coupled Low-Density Parity-Check Lattices with Applications

Avinash Vem, Yu-Chih Huang, Krishna R. Narayanan, Henry D. Pfister
Department of Electrical and Computer Engineering
Texas A&M University
{your email, jerry.yc.huang@gmail.com, krn@ece.tamu.edu, hpfister@tamu.edu}

Abstract

We propose a class of lattices constructed using Construction D where the underlying linear codes are nested binary spatially-coupled low density parity check codes (SC-LDPC) codes with uniform left and right degrees. By leveraging recent results on the optimality of spatially-coupled codes for binary input memoryless channels and Forney *et al.*'s earlier results on the optimality of construction D, we show that the proposed lattices achieve the Poltyrev limit under multistage belief propagation decoding. Lattice codes constructed from these lattices are shown to provide excellent performance for the three user symmetric interference channel. They can also be naturally used in applications such as integer-forcing and compute-and-forward.

I. Introduction

Lattice codes obtained from nested lattices have been shown to be optimal coding solutions to several problems in information theory [1]. In most of these cases, the underlying lattices are constructed using Construction A and it has been shown that such lattices are simultaneously good for shaping (Roger's good) and for channel coding (Poltyrev good) [1]. There are two important drawbacks in using optimal lattices constructed using Construction A. On the theoretical side, the use of non-binary codes makes it difficult to prove the optimality of these lattices and lattice codes under practical decoding algorithms such as belief propagation (BP) decoding and so far, we are not aware of any results showing the optimality of Construction A lattices under BP decoding. On the practical side, optimal lattices constructed from Construction A typically require the underlying linear codes to work over large fields and hence, result in formidable decoding complexity, even with BP decoding.

In this paper, we propose a class of lattices constructed using Construction D [2] where the underlying linear codes are nested binary spatially-coupled low density parity check codes (SC-LDPC) codes with uniform left and right degrees. By using the result that regular SC-LDPC codes can universally achieve capacity under BP decoding for the class of binary memoryless symmetric (BMS) channels [3], [4] and by leveraging Forney *et al*'s result [5], we show that the proposed lattices allow us to achieve the Poltyrev limit under multistage BP decoding. We refer to the proposed lattices as SC-LDPC lattices. Density evolution thresholds show that the proposed SC-LDPC lattices can approach the Poltyrev limit to within 0.2 dB under multistage BP decoding. Very recently, binary polar codes have been used in conjunction with Construction D to obtain Poltyrev-good lattices in [6]. The focus of this paper is on the use of SC-LDPC codes.

We then construct lattice codes from this class of lattices and apply them to the symmetric interference channel [7]. Recently, it has been pointed out in [8] that there is a natural connection between lattices generated by Construction D (or Construction D′) and the interference alignment scheme in [7]. Thus, one can directly implement interference alignment by replacing the Barnes-Wall lattices in [8] by our proposed SC-LDPC lattices. Simulation results show that this replacement leads us to a significant gain in terms of bit error probability. This class of lattice codes can also be applied to Integer-forcing or compute-and-forward in the multiple access stage [9].

Throughout the rest of the paper, vectors and matrices are written in lowercase boldface and uppercase boldface, respectively.

II. Background

A. Lattices and Poltyrev Limit

Consider a lattice Λ with a fundamental volume $V(\Lambda)$. Let us assume that some $\lambda \in \Lambda$ is transmitted through an additive white Gaussian noise (AWGN) channel of variance σ^2 and denote the noise vector by $\mathbf{z}$. Let us denote the probability of decoding error, conditional on codeword $\lambda \in \Lambda$ being transmitted, as $P(\lambda, \sigma^2)$ which is defined as

$$P(\lambda, \sigma^2) := \Pr(d(\lambda, \lambda + \mathbf{z}) \geq d(\lambda', \lambda' + \mathbf{z}) \text{ for some } \lambda' \in \Lambda),$$

where $d(\mathbf{x}, \mathbf{y})$ is the Euclidean distance between $\mathbf{x}$ and $\mathbf{y}$. For an infinite lattice Λ, $P(\lambda, \sigma^2)$ is independent of λ and hence the average probability of decoding error for the lattice $P(\Lambda, \sigma^2)$ is the same as $P(\lambda, \sigma^2)$ for any λ. The volume-to-noise ratio (VNR), $\alpha^2(\Lambda, \sigma^2)$, of an n-dimensional lattice Λ is given by $\alpha^2(\Lambda, \sigma^2) = \frac{V(\Lambda)^{2/n}}{2\pi e \sigma^2}$. Poltyrev in [10] showed that for any VNR > 1 there exists sequence of lattices for which $P(\Lambda, \sigma^2) \to 0$ as $n \to \infty$. We shall call such a sequence of lattices as being Poltyrev-good.

B. Construction D and its Goodness

In this section we briefly describe Construction D lattices [2] [11] and then recall Forney *et al*'s result on the existence of Poltyrev-good lattices based on this construction [5].

For any lattice Λ, a sub-lattice $\Lambda' \subset \Lambda$ induces a coset decomposition (Λ/Λ') of Λ. i.e., it partitions Λ into equivalence groups modulo Λ'. We call this a lattice partition. A multilevel construction of lattices is based on such partition chain and a sequence of nested codes $\{\mathcal{C}_l, 1 \leq l \leq r\}$ where each code $\mathcal{C}_l$ is of length n over $\mathbb{F}_q$, where $\mathbb{F}_q \cong \Lambda_{l-1}/\Lambda_l$. Construction D and Construction D′ are based on such nested sequence of linear codes. For detailed description we refer to [11]. In our work we use one-dimensional lattice partition chain $\Lambda_0/\Lambda_1/\cdots\Lambda_r$, where $\Lambda_i = 2^i\mathbb{Z}$. Then $\Lambda_{i-1}/\Lambda_i \cong \mathbb{F}_2$ for all i. Let $\mathcal{C}_i$ be a (n, k_i) binary code spanned by the set of linearly independent binary n-tuples $\{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_{k_i}\}$ where $k_1 \le k_2 \le \cdots \le k_r$. Using nested binary linear codes $\{\mathcal{C}_j, 1 \le j \le r\}$, a multilevel Construction D type lattice is defined as follows:

$$\Lambda = \bigcup \left\{ 2^r \mathbb{Z}^n + \sum_{1 \le j \le r} \sum_{1 \le i \le k_j} \alpha_{ji} 2^{j-1} \mathbf{g}_i | \alpha_{ji} \in \{0,1\} \right\} \tag{1}$$

where "$+$" denotes addition in $\mathbb{R}^n$. The VNR of a Construction D lattice described above is given by

$$\alpha^2(\Lambda, \sigma^2) = \frac{2^{2(r - \sum_{i=1}^r k_i/n)}}{2\pi e \sigma^2}. \tag{2}$$

Before we describe the multistage decoding used, let $\lambda \in \Lambda$, where Λ is as defined in (1), be transmitted through an AWGN channel and $\mathbf{y} = \lambda + \mathbf{z}$ is received where $\mathbf{z} \sim \mathcal{N}(0, \sigma^2)$. Let $\hat{\mathbf{y}}_0 = \mathbf{y}$.

- **Step 1**: At stage j, $1 \le j \le r$, $\hat{\mathbf{y}}_{j-1} \mod 2$ is decoded to a codeword $\hat{\mathbf{x}}_j \in \mathcal{C}_j$. Also, the corresponding information bits $\{\hat{\alpha}_{j1}, \hat{\alpha}_{j2} \cdots \hat{\alpha}_{jk_j}\} \in \{0,1\}^{k_j}$ that generate $\hat{\mathbf{x}}_j$, are computed.
- **Step 2**: Compute $\hat{\mathbf{y}}_j = \frac{1}{2} \cdot (\hat{\mathbf{y}}_{j-1} - \sum_{1 \le i \le k_j} \hat{\alpha}_{ji} \mathbf{g}_i)$. Repeat **Step 2**.
- **Step 3**: At $(r+1)^{\text{th}}$ stage of decoding, $\hat{\mathbf{y}}_r$ is decoded to the closest $\mathbf{q} \in \mathbb{Z}^n$.
- **Output**: Decoded lattice point $\hat{\lambda} \in \Lambda$ is given by

$$\hat{\lambda} = 2^r \mathbf{q} + \sum_{1 \le j \le r} \sum_{1 \le i \le k_j} \hat{\alpha}_{ji} 2^{j-1} \mathbf{g}_i. \tag{3}$$

At the j^{th} stage of decoding, conditioned on successful decoding in previous stages, the input to the decoder is of the form

$$\begin{aligned} \hat{\mathbf{y}}_{j-1} \bmod 2 &= \frac{1}{2^{j-1}} \left(\mathbf{y} - \sum_{1 \le p < j} \sum_{1 \le i \le k_p} 2^{p-1} \alpha_{pi} \mathbf{g}_i \right) \bmod 2 \\ &= \left(\sum_{i=1}^{k_j} \alpha_{ji} \mathbf{g}_i \right) \bmod 2 + \left(2^{-(j-1)} \mathbf{z} \right) \bmod 2 \\ &= \mathbf{x}_j + 2^{-(j-1)} \mathbf{z} \bmod 2, \end{aligned} \tag{4}$$

where $\mathbf{x}_j \in \mathcal{C}_j$. We call the channel defined in (4) as an additive mod-2 Gaussian noise (AMGN) [5] and denote the capacity for this channel as $C(\mathbb{Z}/2\mathbb{Z}, 2^{-2(j-1)}\sigma^2)$ which is shown to be equal to $C(2^{j-1}\mathbb{Z}/2^j\mathbb{Z}, \sigma^2)$[5].

Theorem 1 (Forney *et al.* [5])**.** For an AWGN channel with noise variance per dimension σ^2, there exists a sequence of construction D lattices Λ based on a chain of two-way one-dimensional lattice partitions and r nested random binary linear codes $\mathcal{C}_1 \subseteq \mathcal{C}_2 \cdots \subseteq \mathcal{C}_r$ that is Poltyrev-good.

Remark 2. Note that in [5], it was shown that if for each level $j \in \{1, \ldots, r\}$, the linear code $\mathcal{C}_j$ at that level achieves the capacity $C(2^{j-1}\mathbb{Z}/2^j\mathbb{Z}, \sigma^2)$ then the Construction D lattice thus constructed is Poltyrev-good.

C. Why not Construction D'

As we know that SC-LDPC codes are based on parity check matrices it raises the question of why not Construction-D' based on nested parity check matrices. Here we try to justify the use of Construction-D over Construction-D'.

Let $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \mathcal{C}_a$ be binary linear codes where $\mathcal{C}_i$ has parameters $[n, k_i]$ for $i = 1, \cdots a$. Let $h_1, h_2, \cdots h_n$ be linearly independent vectors in $\mathbb{F}_2^n$ and code $\mathcal{C}_i, 1 \leq i \leq a$ be defined by the $r_i = n - k_i$ parity-check vectors $h_1, \cdots, h_{r_i}$. Note that $r_1 \geq r_2 \geq \cdots \geq r_a$. For the given nested binary linear codes a lattice based on Construction-D′[12] is given by all vectors $x \in \mathbb{Z}^n$ that satisfy the congruences

$$h_j \cdot x \equiv 0 \pmod{2^i} \quad \text{for all } i \in \{1, 2, \cdots a\}, r_{i+1} + 1 \leq j \leq r_i.$$

One can see that the above congruence relations are equivalent to

$$h_j \cdot x \equiv 0 \pmod{2^i} \quad \text{for all } i \in \{1, 2, \cdots a\}, 1 \leq j \leq r_i. \tag{5}$$

For ease of exposition we consider just two levels i.e., a=2 and in this case the lattice is given by all $x \in \mathbb{Z}^n$ that satisfy

$$\begin{aligned} h_j \cdot x &\equiv 0 \pmod{2} \quad \text{for } 1 \leq j \leq r_1, \\ h_j \cdot x &\equiv 0 \pmod{4} \quad \text{for } 1 \leq j \leq r_2, r_2 \leq r_1. \end{aligned} \tag{6}$$

Every $x \in \mathbb{Z}^n$ can be decomposed into $x = x_1 + 2x_2 + 4\mathbb{Z}^n$ and it can be shown that the congruence equations in (6) are equivalent to

$$\begin{aligned} h_j \cdot x_1 &\equiv 0 \pmod{2} \quad \text{for } 1 \leq j \leq r_1, \\ h_j \cdot (x_1 + 2x_2) &\equiv 0 \pmod{4} \quad \text{for } 1 \leq j \leq r_2. \end{aligned} \tag{7}$$

Let $x = x_1 + 2x_2 + 4\mathbb{Z}^n \in \Lambda$ and from (7) we can see that $x_1 = x \mod 2 \in \mathcal{C}_1$ and hence let $h_j \cdot x_1 = 2d_{1,j}, d_{1,j} \in \mathbb{Z}$ for $1 \leq j \leq r_1$. Then for the second set of equations it can be clearly seen that

$$h_j \cdot 2x_2 = 4d_{2,j} - 2d_{1,j} \text{ for some } d_{2,j} \in \mathbb{Z}$$

thus showing that $x_2 \notin \mathcal{C}_2$. Therefore a lattice point has to be decoded based on a joint decoder rather than a multi-stage decoder resulting in a increase in decoding complexity.

Remark 3. Assuming that the generator vectors and parity-check equations used in both the construciton define the same nested binary linear codes, it is shown in [13] that the lattices thus constructed are not the same. But we can show that volume of the fundamental Voronoi region for both the constructions are same. Let $\mathcal{C}_1 \subseteq \mathcal{C}_2$ be nested binary linear codes with parameters $(n, k_i), 1 \leq i \leq 2$ and $\{\mathbf{g}_1, \cdots, \mathbf{g}_{k_1}\}$, $\{\mathbf{g}_1, \cdots, \mathbf{g}_{k_2}\}$ are the binary vectors that generate $\mathcal{C}_1$, $\mathcal{C}_2$ respectively and similarly $\{\mathbf{h}_1, \cdots, \mathbf{h}_{r_1}\}$, $\{\mathbf{h}_1, \cdots, \mathbf{h}_{r_2}\}$ are the binary parity-check equations that define $\mathcal{C}_1$, $\mathcal{C}_2$ respectively. Note that $k_1 \leq k_2$ and $r_1 \geq r_2$ where $r_i = n - k_i$ for $i = 1, 2$. Volume of the fundamental region of Λ' is given by

$$V(\Lambda') = 2^{r_1 + r_2} = \frac{4^n}{2^{k_1 + k_2}}$$

which can be seen to be equal to that of Λ. For Λ' number of lattice points inside $4\mathbb{Z}^n$ can be computed as $4^{n-r_1} \times 2^{r_1 - r_2}$. If we rewrite the $r_1 - r_2$ set of equations that are to be satisfied $\mod 2$ as parity-check equations

$\mod 2$ then the first term is due to a total of r_1 parity-check equations (and hence $n - r_1$ positions to choose for x) in $\mathbb{Z}_4^n$. The second term can be thought of as correction term since we have 2 choices for the $r_1 - r_2$ equations that are to be satisfied $\mod 2$ giving 2 choices in each equation. Thus the two lattices are not identical but they have the same fundamental voronoi region. Whether these two lattices are isomorphically related (just rotated versions of one another?) need to be undertaken as future work.

III. Proposed SC-LDPC Lattices

Construction of lattices based on Construction D using a SC-LDPC code at each level requires the SC-LDPC codes to be nested. In this section, we first construct such a sequence of nested linear codes based on ensembles of SC-LDPC codes such that each of the code ensembles in the nested construction is capacity achieving. For ease of exposition, we restrict our description to $r = 2$.

A. Construction

Given the rates of $\mathcal{C}_1$ and $\mathcal{C}_2$ as r_1 and r_2, respectively, with $r_1 < r_2$, we construct the nested SC-LDPC code ensemble parameterized by (L, w) where L is the number of independent LDPC systems coupled and w is the coupling width whose design rates tend to r_1 and r_2, respectively, in the limit of $w, L \to \infty$. Choose $d_c \in \mathbb{Z}$ large enough such that there exists $d_v^1, d_v^2 \geq 3 \in \mathbb{Z}$ and

$$1 - \frac{d_v^1}{d_c} > r_1 - \epsilon \text{ and } 1 - \frac{d_v^2}{d_c} > r_2 - \epsilon.$$

Our approach is to first construct a rate r_1 regular LDPC code ensemble and then obtain the r_2 ensemble by removing a fraction of the parity checks and the edges incident on these checks in a way that both the ensembles are regular SC-LDPC code ensembles which are universally capacity achieving. The ensemble described in [14] is not amenable to our approach of deriving the higher rate code, since removing a fraction of the checks from this ensemble does not result in a regular SC-LDPC code ensemble. Therefore, our approach is to use the following multi-edge type construction.

We place Md_c variable nodes at positions $[1, L]$, $L \in \mathbb{N}$ and Md_v^1 check nodes at positions $[1, L + w - 1]$, where $w \in \mathbb{N}$ is the coupling width. At each position divide the Md_v^1 check nodes into d_v^1 groups where each group contains M check nodes. At any position we refer to all check nodes belonging to k^{th} group as of type $\mathcal{T}_k$. Similarly, for each variable node, we classify the d_v^1 edges into types, where k^{th} edge is referred to as type $\mathcal{E}_k$. Therefore there are Md_c edges of each type at each position. For all $i \in \{1, 2, \ldots, L\}$ and $k \in \{1, 2, \ldots, d_v^1\}$, connections for Md_c edges of type $\mathcal{E}_k$ of the variable nodes at position i are chosen uniformly and independently from all type $\mathcal{T}_k$ check nodes in range $\{i, \ldots i + w - 1\}$. This results in a Tanner graph in which every variable node has exactly one edge connected to type $\mathcal{T}_k$ check node for all $k \in \{1, 2, \ldots, d_v^1\}$. We call such graph, a *check-uniform connected graph*.

From such a Tanner graph, removal of all check nodes of a particular type, say $\mathcal{T}_1$, results in variable node degree of $d_v^1 - 1$. One can see that removal of all check nodes of types $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_{d_v^1 - d_v^2}$ from the original

Tanner graph results in a (d_c, d_v^2) SC-LDPC graph that is a sub-graph of the original graph. We call the proposed construction as *check-uniform* SC-LDPC (CU-SC-LDPC) ensemble of codes. One can obtain a sequence of nested linear codes $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \ldots \mathcal{C}_r$ by repeatedly performing the above operation. We refer to such a nested ensemble as $(d_c, d_v^1, \ldots d_v^r)$ CU-SC-LDPC ensemble.

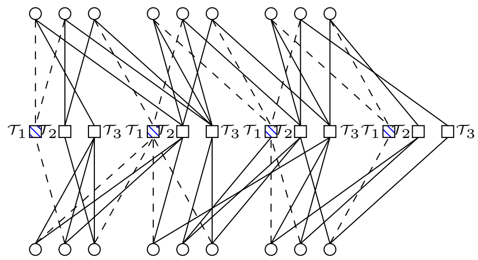

Fig. 1. A protograph for $(3, 6)$, $L = 3$, $w = 2$. Removal of all the type $\mathcal{T}_1$ check nodes i.e the shaded ones, results in a $(2, 6)$ CU-SC-LDPC protograph.

Since Construction D works with generator matrices of nested linear codes, we have to obtain nested generator matrices from the proposed nested CU-SC-LDPC codes. In the following lemma, we show the existence of such nested generator matrices for any set of nested binary linear codes.

Lemma 4. Given nested binary linear codes $\mathcal{C}_1 \subseteq \mathcal{C}_2, \ldots, \subseteq \mathcal{C}_r$ there exists nested generator matrices for these codes.

Proof: It suffices to consider the case having only two levels. For $\mathcal{C}_1$ there exists set of linearly independent binary vectors $\mathbf{G}_1 = \{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_{k_1}\}$ that span $\mathcal{C}_1$ where k_1 =dim$(\mathcal{C}_1)$. Denote $\mathbf{Z}_i = \{\mathbf{G}_1, \mathbf{g}_{k_1+1}, \mathbf{g}_{k_1+2}, \ldots, \mathbf{g}_{k_1+i-1}\}$ and $Y_i = \mathcal{C}_2 \setminus$ span$(\mathbf{Z}_i)$ for $i = 1, 2, \ldots, k_2 - k_1$. Note that for any $\mathbf{x} \in Y_i$, $\mathbf{x}$ is linearly independent with $\mathbf{Z}_i$ and hence $\mathbf{Z}_{i+1} = \{\mathbf{Z}_i, \mathbf{g}_{k_1+i}\}$ forms a linearly independent set where $\mathbf{g}_{k_1+i} = \mathbf{x}$. This recursive procedure gives us a basis $\mathbf{G}_2$ for $\mathcal{C}_2$. Thus the existence of the generator matrices for nested binary linear codes is shown. ∎

From the above Lemma 3, given nested CU-SC-LDPC codes $\mathcal{C}_1 \subset \mathcal{C}_2 \ldots \subset \mathcal{C}_r$, one can find a corresponding sequence of nested sets of generator vectors $\mathbf{G}_1 \subset \mathbf{G}_2 \subset \ldots \subset \mathbf{G}_r$ and hence can use Construction D described in (1) with the proposed CU-SC-LDPC codes. We refer to the lattices thus constructed as the *SC-LDPC lattice*.

B. Poltyrev-Goodness of the Proposed Lattices

We now show the existence of a sequence of SC-LDPC lattices which is Poltyrev-good under BP decoding. In the following lemmas, we show that the proposed CU-SC-LDPC codes achieve the AMGN channel capacity. We then follow the argument by Forney *et al.* described in Remark 2 to show the result.

Lemma 5. For a BMS channel with associated L-density [15] $\mathbf{x}_{\text{BMS}}$, density evolution (DE) equation for a

(d_c, d_v, w, L) CU-SC-LDPC ensemble is given by

$$\mathbf{x}_i^{(l)} = \mathbf{x}_{\text{BMS}} \circledast \left(1 - \frac{1}{w}\sum_{j=0}^{w-1}\left(1 - \frac{1}{w}\sum_{k=0}^{w-1}\mathbf{x}_{i+j-k}^{(l-1)}\right)^{\boxast d_c - 1}\right)^{\circledast d_v - 1}, \tag{8}$$

where $\mathbf{x}_i^{(l)}$ is the average L-density of a variable node at position i in iteration l.

Proof: In the proposed CU-SC-LDPC ensemble, from the perspective of a variable node there are d_v types of edges $\mathcal{E}_1, \mathcal{E}_2, \cdots, \mathcal{E}_{d_v}$. We denote edges of type $\mathcal{E}_k$ that originate from a variable node at position i as $(i, \mathcal{T}_k)$ and the L-density of the message emitted by variable nodes along such edge types as $\mathbf{x}_{ik}^{(l)}$ where l denotes the iteration. But from the perspective of a check node of any type at position i, an edge is randomly connected to one of the variable nodes located at positions $\{i, i-1, ...i-w+1\}$. Hence all the edges connected to check nodes at a certain position are statistically identical and more importantly all check nodes at certain position are statistically identical. The average L-density of the message emitted by a check node at position i in iteration l, denoted by $\mathbf{y}_i^{(l)}$, is given by

$$\mathbf{y}_i^{(l)} = \left(\frac{1}{w}\sum_{j=0}^{w-1}\left(\frac{1}{d_v}\sum_{k=0}^{d_v}\mathbf{x}_{(i-j)k}^{(l-1)}\right)\right)^{\circledast d_c - 1} \tag{9}$$

And a variable node update is given by

$$\mathbf{x}_{ik}^{(l)} = \mathbf{x}_{\text{BMS}} \boxast \left(\frac{1}{w}\sum_{j=0}^{w-1}\mathbf{y}_{i+j}^{(l)}\right)^{\boxast d_v - 1} \tag{10}$$

$$\mathbf{x}_i^{(l)} = \frac{1}{d_v}\sum_{k=0}^{d_v}\mathbf{x}_{ik}^{(l)}$$

where $\mathbf{x}_i^{(l)}$ is the average L-density of the log-likelihood ratio of variable nodes at position i. Combining (9) and (10) and observing that the initialization is $\mathbf{x}_i^{(l)} = \mathbf{x}_{i1}^{(1)} = \mathbf{x}_{i2}^{(1)} = \cdots = \mathbf{x}_{id_v}^{(1)} = \mathbf{x}_{\text{BMS}}$ completes the proof. ■

Note that in (8) we show that the DE equations for the proposed CU-SC-LDPC ensemble are identical to that of SC-LDPC ensemble proposed in [14], [3].

Lemma 6. For any $\epsilon > 0$, there exists a sequence of CU-SC-LDPC Codes parameterized by (d_c, d_v, L, w) such that the rate $R > C_{\text{AMGN}} - \epsilon$ as $L \to \infty$ for which the bit error probability under BP decoding $\to 0$ as $M \to \infty$, where C_{AMGN} is the Shannon capacity of the AMGN channel.

Proof: It has been proved in [3], [4] that over any BMS channel, under BP decoding, any system that satisfies the equation (8) achieve the capacity as $d_c, w, L \to \infty$ (with $\frac{d_v}{d_c}$ fixed). Hence, using Lemma 4, it's enough to show that the AMGN channel described in (4) is indeed a BMS channel. It is clear to see that the AMGN channel has binary input and output lying in an interval of length 2. Let the input alphabet to the channel be $\{0, 1\}$ and without loss of generality let the $\mod 2$ operation produces a output lying in $[-0.5, 1.5]$. Then the conditional PDFs of

$\mathbf{y}$ can be written as

$$f(y|x=0) = \frac{1}{\sqrt{2\pi e\sigma^2}} \sum_{j=-\infty}^{\infty} \exp\left[\frac{-(y+2j)^2}{2\sigma^2}\right] \tag{11}$$

$$f(y|x=1) = \frac{1}{\sqrt{2\pi e\sigma^2}} \sum_{j=-\infty}^{\infty} \exp\left[\frac{-(y+2j-1)^2}{2\sigma^2}\right]. \tag{12}$$

Therefore the PDFs of the output satisfy

$$f(y-0.5|1) = f(0.5-y|0) \quad \text{for all } y \in [-0.5, 1.5].$$

Thus, it belongs to the class of BMS channels. ■

Theorem 7. For any $\epsilon > 0$, there exists a sequence of SC-LDPC lattices with $1 < \alpha^2(\Lambda, \sigma^2) < 1 + \epsilon$ for which the average probability of error approaches zero under multistage BP decoding as $L, M \to \infty$.

Proof: Combining Remark 2 and Lemma 5 completes the proof. ■

Remark 8 (Comparison with LDPC lattices)**.** LDPC codes have been adopted as underlying codes for constructing lattices in [16] where the so-called LDPC lattices have been proposed and analyzed. Our SC-LDPC lattices differ from LDPC lattices in the following ways. Firstly, LDPC lattices are constructed based on Construction D′ [2] in contrast to Construction D adopted here. Secondly, our decoding algorithm is a multistage BP decoding which only works over $\mathbb{F}_2$, on the contrary, since constructed based on Construction D′, LDPC lattices have to considered BP algorithm on the joint Tanner graph [17] (i.e., joint decoding). Last but not least, since there are no analytical evidence that LDPC codes under BP decoding would achieve capacity, LDPC lattices have not been shown Poltyrev-good to the best of our knowledge while for the proposed SC-LDPC lattices, Theorem 6 serves as constructive evidence.

C. Design and Simulation Results

In this subsection, we give a design example of SC-LDPC lattices that approach the Poltyrev limit. Before we explain the design of Poltyrev-good SC-LDPC lattices, we will analyze the average probability of decoding error.

As we use multistage decoding, the average probability of decoding error $p(\Lambda, \sigma^2)$, can be union bounded by the sum of block error probabilities at individual levels. Assuming CU-SC-LDPC code at each level is operating below the BP threshold, the average probability of decoding error of the lattice is dominated by the performance of the last (uncoded) level. Let us denote block error probability for $(r+1)^{\text{th}}$ level by $p(\mathbb{Z}_{2^r}^n, \sigma^2)$. Under minimum distance decoding, $p(\mathbb{Z}_{2^r}^n, \sigma^2)$ is given by

$$\begin{aligned} p(\mathbb{Z}_{2^r}^n, \sigma^2) &\overset{(a)}{\approx} np(\mathbb{Z}_{2^r}, \sigma^2) \\ &= n\left(2Q\left(\frac{0.5}{\sigma_{r+1}}\right)\right) \end{aligned} \tag{13}$$

where the approximation in (a) is for large n and $\sigma_{r+1} \triangleq \sigma/2^r$ is the effective noise observed at the last level.

TABLE I
DE THRESHOLDS AND GAP FROM POLTYREV LIMITS (WITHOUT RATE LOSS FROM TERMINATION) FOR SC-LDPC LATTICE ENSEMBLES FOR VARIOUS DEGREE PROFILES.

(d_c, d_v^1, d_v^2)	(L,w)	σ_{max}	VNR*	$\text{VNR}_{\text{rate-loss}}$
(30,14,3)	(32,4)	0.3184	1.14dB	1.347dB
(60, 27, 3)	(64, 9)	0.3203	0.57dB	0.951
(60, 26, 3)	(72, 12)	0.3200	0.482dB	0.927dB
(60, 42, 3)	(72, 12)	0.3975	0.203dB	—

Let the number of levels required be $r+1$, with r levels using nested SC-LDPC codes and the last level be the $\mathbb{Z}_{2^r}^n$ uncoded lattice. The effective noise seen by i^{th} level is denoted as $\sigma_i \triangleq \sigma/2^{i-1}$. For $n = 2 \times 10^5$ and target block error probability of 10^{-4}, (13) gives us $\sigma_{r+1} = 0.0804$ and moving to the next level, $\sigma_r = 2\sigma_{r+1} = 0.1608$. For the details on capacity of AMGN channel we refer to [5]. The capacity for level r is $C(\mathbb{Z}/2\mathbb{Z}, \sigma_r) = 0.9923$ and similarly proceeding, $\sigma_{r-1} = 2\sigma_r = 0.3217$, $C(\mathbb{Z}/2\mathbb{Z}, \sigma_{r-1}) = 0.5726$, $\sigma_{r-2} = 2\sigma_{r-1} = 0.6434$, $C(\mathbb{Z}/2\mathbb{Z}, \sigma_{r-2}) = 0.0242$. Observe that the capacity for level $r-2$ is almost zero which renders coding for this level unnecessary although this results in a very small increase in VNR (due to rate the loss) of 0.145dB ($= 20\log_{10} 2^{0.0242}$). We use $r = 2$ (i.e., 3 levels) and $(30, 14, 3)$ CU-SC-LDPC ensemble with $L = 32, w = 4$ is used for the first two levels and the uncoded $\mathbb{Z}_4^n$ lattice is used in the last level.

Due to symmetry in the lattice the all-zero lattice point is assumed to be transmitted. Instead of plotting the symbol error rate, we focus on determining the thresholds of the resulting lattice under BP decoding. We estimate the BP threshold by determining the maximum noise variance for which no codeword errors are observed in simulation of 10 consecutive codewords each of length 2×10^5. We calculate the maximum variance for which both levels of the lattice can be decoded, $\sigma_{\text{max}} = \min(\sigma_1^{\text{BP}}, 2\sigma_2^{\text{BP}})$, where σ_1^{BP} and σ_2^{BP} are the respective BP thresholds for the two SC-LDPC codes. The VNR threshold is then calculated for the given rates and σ_{max}. Thus obtained BP thresholds σ_1^{BP}, σ_2^{BP} for the above codes are 0.3142 and 0.2161 respectively which results in a VNR of 1.14dB (1.46dB with rate loss due to termination). The DE predicted values are 0.3184 and 0.21836. We observe that the BP thresholds are very close to DE thresholds. i.e., the parameters are large enough to assume that the BP thresholds can be approximated by DE thresholds. Therefore it is reasonable to calculate the VNR thresholds using the DE thresholds. For various SC-LDPC ensembles Table. I gives the respective DE and VNR thresholds. Note that the Poltyrev limit is zero dB, thus making the VNR threshold and the gap from Poltyrev limit equivalent. The gap to the Poltyrev limit is primarily due to the fact that there is a mismatch between the rates that are obtainable for the proposed ensemble with a fixed d_c and the capacity of the equivalent channel.

In the above design, if we target a bit error probability of 10^{-6} instead, that gives us $\sigma_{r+1} = 0.0999$, capacities for the subsequent levels $C(\mathbb{Z}/2\mathbb{Z}, \sigma_r) = 0.9507$, $C(\mathbb{Z}/2\mathbb{Z}, \sigma_{r-1}) = 0.3223$ and $C(\mathbb{Z}/2\mathbb{Z}, \sigma_{r-2}) = 0.0024$. Pair of nested codes from $(60, 42, 3)$ CU-SC-LDPC ensemble gives us rates 0.3 and 0.95 resulting in better matching of the rates (negligible rate loss). The resulting DE thresholds are within 0.203dB from Poltyrev limit. This is reported in the last row in the table.

IV. Application - Interference Channels

A. Problem Statement

We consider the 3 user Gaussian IC consisting of 3 transmitters, 3 receivers, and 3 independent messages originally considered in [18], where message W_j originates at transmitter j and is intended for receiver j, $\forall j \in \mathcal{J} \triangleq \{1,2,3\}$. The output observed at the receiver j is given by

$$\mathbf{y}_j = \mathbf{x}_j + \sum_{k=1,k\neq j}^{3} h_{jk}\mathbf{x}_k + \mathbf{z}_j, \quad \forall j \in \mathcal{J} \tag{14}$$

where $\mathbf{x}_j$ is the transmitted signal at j^{th} transmitter, h_{jk} are the channel parameters for the cross links, and $\mathbf{z}_j \sim \mathcal{N}(\mathbf{0}, \sigma^2 \cdot \mathbf{I})$ is the AWGN noise. If the channel parameters for all the cross links are equal we refer to such model as symmetric IC. The channel input signals are subjected to the power constraint $\frac{1}{n}\sum_{i=1}^{n} E\left[\|\mathbf{x}_j\|^2\right] \leq P$.

For a 2-user symmetric Gaussian interference channel (IC) it was shown in [19] that, in the very strong interference regime, the capacity region for the IC is as if there is no interference at all. For this symmetric model, a simple extension of the very strong interference condition for the 2 user IC to the 3 user one is given by [18]

$$\beta^2 \geq \frac{\left((1+P)^2 - 1\right)(1+P)}{2P}. \tag{15}$$

Sridharan *et al.* in [18] introduce the idea of lattice alignment where each user uses a lattice code and each receiver first decodes the total interference (aligned due to lattice structure) observed and then decodes the desired message. For this case, they derived a tighter condition on β in order for the interference to be decoded first. This is based on lattice coding, independent of the number of users, and is given by

$$\beta^2(\sigma) \geq {\beta^*}^2(\sigma) \triangleq \frac{(P+\sigma^2)^2}{P\sigma^2} \tag{16}$$

If (16) is satisfied, each user can achieve a capacity [18] of $\frac{1}{2}\log(1+\frac{P}{\sigma^2})$. Equivalently, for a given rate R, maximum noise variance under which the rate can be achieved is given by

$$\sigma^2_{\max} = \frac{P}{2^{2R}-1}. \tag{17}$$

B. Applying the Proposed Lattices

Encouraged by the Poltyrev-limit achieving property of the proposed lattice ensembles under BP decoding, we use SC-LDPC lattice codes for the symmetric Gaussian IC in the very strong interference region. Let Λ_{SC} be the SC-LDPC lattice defined in (1) with $r = 2$. We define the SC-LDPC lattice code $\mathcal{C}_{SCL}$ based on Λ_{SC} using hypercube shaping:

$$\mathcal{C}_{SCL} = \{\lambda \mod \mathbb{Z}_4^n : \lambda \in \Lambda\} \tag{18}$$

where n is the dimension of Λ_{SC}. Let codeword $\mathbf{c}_j \in \mathcal{C}_{SCL}$ at transmitter j be

$$\mathbf{c}_j = \sum_{i=1}^{k_1} \alpha_{ji}\mathbf{g}_i + 2\sum_{i=1}^{k_2} \beta_{ji}\mathbf{g}_i \mod \mathbb{Z}_4^n \qquad \alpha_{ji}, \beta_{ji} \in \{0,1\} \tag{19}$$

$$= \sum_{i=1}^{k_1} \alpha_{ji}\mathbf{g}_i + 2\sum_{i=1}^{k_2} \beta_{ji}\mathbf{g}_i - 4\mathbf{k}_j, \text{ for some } \mathbf{k}_j \in \mathbb{Z}^n \tag{20}$$

where "+" denotes addition in $\mathbb{R}^n$. Each codeword $\mathbf{c}_j \in \mathcal{C}_{SCL} \subset \{0,1,2,3\}^n$ is modulated to $\tilde{\mathbf{x}}_j \triangleq 1.5^n - \mathbf{c}_j$ such that $\tilde{\mathbf{x}}_j \in \mathcal{A} \triangleq \{-1.5, -0.5, +0.5, +1.5\}^n$. At transmitter j, a dither vector $\mathbf{d}_j$ uniformly distributed among $\mathcal{B} \triangleq [-2, 2)$ is added to obtain the transmitted signal $\mathbf{x}_j$ given by

$$\mathbf{x}_j = \tilde{\mathbf{x}}_j + \mathbf{d}_j \mod \mathbb{Z}_4^n, \tag{21}$$

where the mod operation is over $\mathcal{B}$ instead of $[0,4)$. The dither vector achieves the purpose of randomizing the interference and helps in treating the undesired components of the received signal as additive uncorrelated noise. From (**??**) it can be seen that $\mathbf{x}_j$ is uniformly distributed over $\mathcal{B}$ and the average power of the transmitted signal at each transmitter is 1.33.

C. Decoding

Before looking at the general case let us consider the symmetric Gaussian IC i.e $h_{12} = h_{13}$. Without loss of generality let us consider receiver 1. The system flow from the perspective of receiver 1 is given in Fig. 2. The input to the multistage decoder at receiver 1 is given by

$$\begin{aligned}\tilde{\mathbf{y}}_1 &\triangleq \frac{\mathbf{y}_1}{h_{12}} - \mathbf{d}_2 - \mathbf{d}_3 + 1.5^n + 1.5^n \\ &= \mathbf{c}_2 + \mathbf{c}_3 + \frac{1}{h_{12}}\left(\mathbf{x}_1 + \mathbf{z}_1\right).\end{aligned}$$

The key here is that $\mathbf{c}_2, \mathbf{c}_3 \in \mathcal{C}_{SCL} \subset \Lambda$ and hence $\mathbf{c}_2 + \mathbf{c}_3 \in \Lambda$.

$$\begin{aligned}\mathbf{c}_2 + \mathbf{c}_3 &= \sum_{i=1}^{k_1}\left(\alpha_{2i} + \alpha_{3i}\right)\mathbf{g}_i + 2\sum_{i=1}^{k_2}\left(\beta_{2i} + \beta_{3i}\right)\mathbf{g}_i + 4\mathbf{k}_2 + 4\mathbf{k}_3 \\ &= \sum_{i=1}^{k_1}\left(\alpha_{2i} \oplus \alpha_{3i}\right)\mathbf{g}_i + 2\sum_{i=1}^{k_2}\left(c_{1i} \oplus \beta_{2i} \oplus \beta_{3i}\right)\mathbf{g}_i + 4\mathbf{k}_{23}\end{aligned}$$

where $c_{1i} = 0.5\left(\alpha_{2i} + \alpha_{3i} - \alpha_{2i} \oplus \alpha_{3i}\right)$, $c_{2i} = 0.5\left(c_{1i} + \beta_{2i} + \beta_{3i} - c_{1i} \oplus \beta_{2i} \oplus \beta_{3i}\right)$ are carryovers from first and second levels respectively and $\mathbf{k}_{23} = \mathbf{k}_2 + \mathbf{k}_3 + \sum_1^{k_2} c_{2i}\mathbf{g}_i \in \mathbb{Z}^n$. The key point is that $c_{1i}, c_{2i} \in \{0,1\}$. Using multi-stage decoder described in Section III, one can directly decode the lattice point $\mathbf{x}_2 + \mathbf{x}_3$(interference), subtract it and decode the desired signal.

The decoding scheme above extends to the case when one channel gain is an integer multiple of the other. For example, let $h_{13} = Kh_{12}$ where $K = \sum_0^{l-1} a_i 2^i \in \mathbb{Z}, a_i \in \{0,1\}$. In this case, input to the multi-stage decoder is

$$\begin{aligned}\tilde{\mathbf{y}}_1 &\triangleq \frac{\mathbf{y}_1}{h_{12}} - \mathbf{d}_2 - K\mathbf{d}_3 + 1.5^n + K1.5^n \\ &= \mathbf{c}_2 + K\mathbf{c}_3 + \frac{1}{h_{12}}\left(\mathbf{x}_1 + \mathbf{z}_1\right).\end{aligned}$$

where $\mathbf{c}_2 + K\mathbf{c}_3$ is a lattice point and is given by

$$\sum_{i=1}^{k_1} (\alpha_{2i} \oplus a_0\alpha_{3i})\, \mathbf{g}_i + 2\sum_{i=1}^{k_2} (c_{1i} \oplus \beta_{2i} \oplus a_0\beta_{3i} \oplus a_1\alpha_3)\, \mathbf{g}_i + 4\mathbf{k}$$

for some $\mathbf{k} \in \mathbb{Z}^n$.

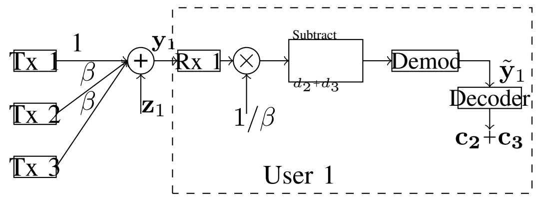

Fig. 2. System flow for the 3-user Symmetric Gaussian Interference channel at receiver 1.

D. Simulation Results for Symmetric IC

In this section we present simulation results for the symmetric Gaussian IC and compare them with the bounds given in [18]. We choose a pair of nested codes from the $(30, 18, 3)$ CU-SC-LDPC ensemble with spatial-coupling parameters $(L, w) = (32, 4)$. We fix $\sigma = \sigma_{\text{max}}$ (such that in absence of interference, desired signal can be decoded successfully) and we analyze the bit error probability in decoding the interference versus the channel gain β. We observe that within 0.396dB of the very strong interference regime given by (16) we are able to decode the interference with a bit error probability of less than 10^{-6}. Note that the main bottle neck in error performance in decoding the interference is the last i.e., the uncoded level whereas in decoding the desired signal (after the interference is decoded and subtracted), within σ_{max}, arbitrarily small error rates can be achieved since no uncoded level needs to be decoded.

In Fig. 3, we plot the achievable rate as a function of P/σ^2 for the desired user for $r = 4$. It can be seen that the achievable rate with the lattice code has a gap of roughly 1.53 dB from the corresponding Shannon limit at high rates. This is the shaping loss due to hypercube shaping. The DE thresholds with the proposed SC-LDPC codes is also shown in the plot and it can be seen that the DE thresholds are very close to the achievable rates.

References

[1] U. Erez, S. Litsyn, and R. Zamir, “Lattices which are good for (almost) everything,” *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, 2005.

[2] E. Barnes and N. Sloane, “New lattice packings of spheres,” *Canad. J. Math*, vol. 35, pp. 117–130, 1983.

[3] S. Kudekar, T. J. Richardson, and R. Urbanke, “Spatially coupled ensembles universally achieve capacity under belief propagation,” in *Proc. IEEE ISIT*, pp. 453–457, 2012.

[4] S. Kumar, A. J. Young, N. Macris, and H. D. Pfister, “A proof of threshold saturation for spatially-coupled LDPC codes on BMS channels,” in *Proc. 50th Annual Allerton Conf. on Commun., Control, and Comp*, 2012.

[5] G. D. Forney Jr, M. D. Trott, and S.-Y. Chung, “Sphere-bound-achieving coset codes and multilevel coset codes,” *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 820–850, 2000.

[6] Y. Yan, C. Ling, and X. Wu, “Polar lattices: where Arıkan meets Forney,” in *Proc. IEEE ISIT*, pp. 1292–1296, 2013.

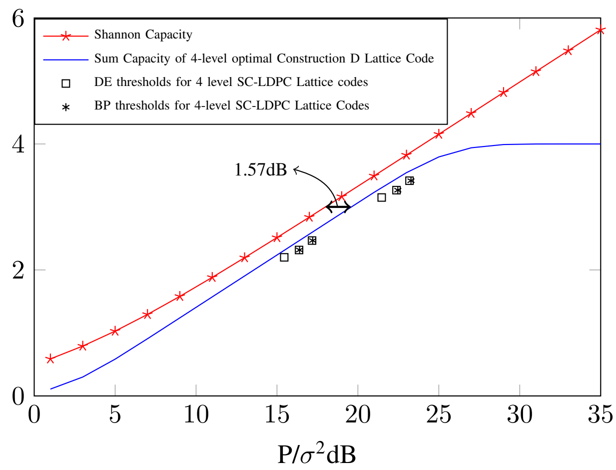

Fig. 3. Gap between the Shannon capacity and the sum-capacity of a 4-level Construction D lattice code(hypercube shaping) under multi-stage decoding. The DE thresholds for various SC-LDPC lattice codes with a maximum check node degree of 60 are also given.

[7] S. A. Jafar and S. Vishwanath, "Generalized degrees of freedom of the symmetric Gaussian k-user interference channel," *arXiv preprint arXiv:0804.4489*, 2008.

[8] M. C. Estela, C. Ling, and J.-C. Belfiore, "Barnes-wall lattices for the symmetric interference channel," in *Proc. IEEE ISIT*, pp. 2239–2243, 2013.

[9] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.

[10] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 409–417, 1994.

[11] N. J. Sloane, J. Conway, *et al.*, *Sphere packings, lattices and groups*, vol. 290. Springer, 1999.

[12] N. J. Sloane, J. Conway, *et al.*, *Sphere packings, lattices and groups*, vol. 290. Springer, 1999.

[13] W. Kositwattanarerk and F. Oggier, "Connections between construction d and related constructions of lattices," *arXiv preprint arXiv:1308.6175*, 2013.

[14] S. Kudekar, T. J. Richardson, and R. L. Urbanke, "Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803–834, 2011.

[15] T. J. Richardson and R. L. Urbanke, *Modern coding theory*. Cambridge University Press, 2008.

[16] M.-R. Sadeghi, A. H. Banihashemi, and D. Panario, "Low-density parity-check lattices: construction and decoding analysis," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4481–4495, 2006.

[17] A. H. Banihashemi and F. R. Kschischang, "Tanner graphs for group block codes and lattices: construction and complexity," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 822–834, 2001.

[18] S. Sridharan, A. Jafarian, S. Vishwanath, and S. A. Jafar, "Capacity of symmetric k-user Gaussian very strong interference channels," in *Global Telecommunications Conference, 2008.*, pp. 1–5, IEEE, 2008.

[19] A. Carleial, "Interference channels," *IEEE Trans. Inf. Theory*, vol. 24, no. 1, pp. 60–70, 1978.