Regular LDPC Lattices are Capacity-Achieving

Mohammad-Reza Sadeghi, and Amin Sakzad,

Abstract—The concept and existence of sphere-bound-achieving and capacity-achieving lattices has been explained on the AWGN channels by Forney [4]. In this paper we focus on regular LDPC lattices [7]. We introduce and investigate an ensemble of LDPC lattices with known properties. It is shown that these lattices are sphere-bound-achieving and capacity-achieving.

Index Terms—Low Density Parity Check (LDPC) Lattice, Volume to Noise Ratio (VNR), Coding Gain.

I. INTRODUCTION

Forney [4] proved the existence of sphere-bound-achieving lattices via Construction D lattices theoretically. He also defined volume-to-noise ratio as a parameter for measuring the goodness of lattices. Afterwards, the search for sphere-bound-achieving and capacity-achieving lattices and lattice codes has been started [7]. LDPC lattices, which were introduced first by Sadeghi et al. in [7], motivate us that LDPC lattices can achieve sphere-bound on the AWGN channels when the level of construction increases. In the present work, mathematically we explain how regular LDPC lattices can achieve sphere-bound on the AWGN channel by the definition of Forney.

Regular LDPC lattices have some special characteristics which can help us in determining the minimum distance, volume, coding gain, kissing number and also an upper bound on the probability of error of such lattices in communication on an AWGN channel. These types of lattices are constructed based on a well-known structure which converts a set of nested codes to a lattice named construction $D'$. By an extended version of PEG algorithm, so called E-PEG algorithm [7] we construct the Tanner graph of regular LDPC lattices. Such construction provides us with some information about cycle-free properties of the Tanner graph of these lattices. It is known that presence of short cycles can hurt the decoding algorithms which use Tanner graph as their underlying structure for decoding process.

Polytrev [6] suggested employing coding without restriction on the AWGN channel for lattices. That is a communication which has no power constraint. In such a communication system the coding rate will be a meaningless parameter. Instead, he introduced two new concepts: Normalized Logarithmic Density (NLD) and generalized capacity ($C_\infty$). He also proved the existence of ensembles of lattices which can achieve generalized capacity on the AWGN channel without restriction. Therefore generalized capacity for lattices means that, there exists a lattice of high enough dimension $n$ that enables transmission with arbitrary small error probability if and only if the constellation density NLD is less than $C_\infty$.

However, Forney [4] restated the above concept by use of VNR. He defined VNR of a communication on an AWGN channel with noise variance $\sigma^2$, where NLD = $C_\infty$ implies that VNR = 1 and vice versa. Then a lattice is called capacity-achieving when VNR = 1 and its probability of error in an AWGN channel with noise variance $\sigma^2$ tends to zero. It can be shown that if there exist generalized capacity achieving lattices, then by selecting proper shaping region we can construct capacity-achieving lattice codes.

In this work we derive special types of high enough dimension, regular LDPC lattices which have been previously introduced by Sadeghi et al. in [7]. Then we compute the basic parameters of these lattices for example minimum distance, coding gain and kissing number. Finally we explain how such lattices are sphere-bound-achieving and capacity-achieving.

The rest of our paper is organized as follow: backgrounds will appear in Section 2. Regular LDPC lattices will be explained in Section 3. We introduce a type of sphere-bound-achieving and capacity-achieving LDPC lattices in Section 4. Discussion about concluding remarks, showing simulation results, open problems and further research topics are in Section 5.

II. PRELIMINARIES

A. Lattices

A discrete, additive subgroup $\Lambda$ of the $m$-dimensional real space $\mathbb{R}^m$ is called a lattice. The notation $d_{\min}(\Lambda)$ is used to denote the length of the shortest nonzero vector of the lattice $\Lambda$. In fact $d_{\min}(\Lambda)$ refers to the minimum distance between lattice points. The coding gain of a lattice $\Lambda$ is defined as:

$$\gamma(\Lambda) = \frac{d_{\min}^2(\Lambda)}{(\det(\Lambda))^{\frac{2}{m}}} \quad (1)$$

where the $\det(\Lambda)$ is the volume of $\Lambda$.

The normalized volume [4] of an $n$-dimensional lattice $\Lambda$ is defined as $d_{\min}(\Lambda)^{\frac{2}{n}}$. This volume may be regarded as the volume of $\Lambda$ per two dimensions. Define the kissing number of a sphere packing in any dimension to be the number of spheres that touch one sphere and denote it by $\tau$. The volume-to-noise ratio (VNR) of an $n$-dimensional lattice $\Lambda$ is defined as

$$\text{VNR} = \frac{\det(\Lambda)^{\frac{2}{n}}}{2\pi^e\sigma^2}. \quad (2)$$

For large $n$, the VNR is the ratio of the normalized volume of $\Lambda$ to the normalized volume of a noise sphere of squared radius $n\sigma^2$ which is defined as SNR in [7] and $\alpha^2$ in [4]. In
the rest of this paper we use \( \alpha^2 \) to represent VNR.

Let the vector \( \mathbf{e} \in \Lambda \) be transmitted on the AWGN channel, then the received vector \( \mathbf{r} \) can be written as \( \mathbf{r} = \mathbf{e} + \mathbf{e} \) where \( \mathbf{e} = (e_1, \ldots, e_n) \) is in the Euclidean space and its components are independently and identically distributed random variables with zero mean and variance \( \sigma^2 \). It is well known that the capacity of this channel is

\[
C = \frac{1}{2} \log_2 \left( 1 + \frac{P}{\sigma^2} \right)
\]

where \( \sigma^2 \) is the variance of the i.i.d Gaussian noise. Thus the probability of error is given by

\[
P_e = \int_{\nu(c)} \frac{1}{\sqrt{2\pi}} e^{-\frac{|x|^2}{2\sigma^2}} dx
\]

where \( \nu(c) \) is the Voronoi cell of \( c \) and \( |x| \) is Euclidean norm of \( x \).

Due to the geometric uniformity of lattices, we can assume \( 0 \) is transmitted and \( \mathbf{r} \) is the received vector. Then the components of \( \mathbf{r} \) are Gaussian distributed random variables with zero mean and variance \( \sigma^2 \). Using union bound \( [3] \) we have

\[
P_e \leq \sum_i \frac{1}{2} \text{erfc} \left( \frac{|x|}{\sqrt{2\sigma}} \right)
\]

where \( \text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt \).

In general, evaluation of this bound is very difficult.

### B. Construction \( D' \) Lattice

Construction \( D' \) \([3]\) converts a set of parity checks defined by a family of nested codes into congruences for a lattice. This construction is a good tool for lattice construction based on LDPC codes. Let \( \alpha = 1 \) or \( 2 \) and let \( C_0 \subseteq C_1 \subseteq \cdots \subseteq C_n \) be a family of nested linear codes, where \( C_l \) has parameter \([n, k, d_{c_{\text{min}}}^l] \) such that \( h_1, \ldots, h_n \) be linearly independent vectors in \( \mathbb{F}_2^n \) for \( 0 \leq l \leq a \) where the code \( C_l \) is defined by the \( r_l = n - k_l \) parity check vectors \( h_1, \ldots, h_l \) and \( r_{l-1} = 0 \).

Consider \( v \) as a vector in \( \mathbb{R}^n \), with component \( 0 \) or \( 1 \). Define the new lattice \( \Lambda \) consisting of those \( x \in \mathbb{Z}^n \) that satisfy the congruences \( h_j \cdot x \equiv 0 \pmod{2^{l+1}} \) for \( 0 \leq l \leq a \) and \( r_{l-1} = 0 \).

By multiplying \( [3] \) the modular equations by appropriate powers of \( 2 \), we can restate Construction \( D' \). Indeed, \( x \in \Lambda \) if \( Hx^T = 0 \pmod{2^{a+1}} \) where

\[
H = [h_1, \ldots, h_{r_0}, \ldots, 2^ah_{r_{a-1}+1}, \ldots, 2^ah_n]^T.
\]

\( H \) is the parity check matrix of \( \Lambda \).

For any \( 0 \leq l \leq a \), \( d_{s_j}^l \) denotes the degree of the symbol node \( s_j \) in the parity check matrix of \( C_l \). We put \( d_{s_j}^l = d_{s_j}^{l+1} \), \( 1 \leq j \leq n \) and use \( d_{c_i}^l \), \( 1 \leq i \leq m \) to denote the degree of the check node \( c_i \).

**Definition 1:** A lattice \( \Lambda \) constructed based on Construction \( D' \) is called LDPC lattice if its parity check matrix \( H \) is a sparse matrix.

It is trivial that if the underlying nested codes \( C_l \) are LDPC codes then the corresponding lattice is a LDPC lattice and vice versa.

**Theorem 2:** Let \( \Lambda \) be a lattice constructed using Construction \( D' \), then the volume of \( \Lambda \) is

\[
\Lambda(\Lambda) = 2^{\sum_{i=0}^{a} r_i}.
\]

Also the minimum distance of \( \Lambda \) satisfies the following bounds

\[
\min_{0 \leq l \leq a} \{d_{c_{\text{min}}}^{l-1} \leq d_{c_{\text{min}}}^l \leq 2^a \}. \quad (6)
\]

**Proof:** The proof is given in \([7]\).

### C. Extended Progressive Edge Growth Algorithm

The Extended Progressive Edge Growth Algorithm (E-PEG) was introduced in \([7]\) and used to construct regular bipartite graph.

**Definition 3:** An \((a+1)\)-level Tanner graph is called \((d_x, d_c; \alpha+1)\) regular \([7]\) if:

1. for each \( 0 \leq l \leq a \) there is a constant \( d_s^l \) such that \( d_{s_j}^l = d_s^l \) for every \( 1 \leq j \leq n \) and \( d_s^l = d_s^0 \);
2. \( d_{c_i}^l = d_{c_i}^0 \) for \( 1 \leq i \leq m \).

As we can see if the input parameters of the E-PEG are selected appropriately, then a class of regular Tanner graphs and consequently a class of regular lattices may be constructed.

**Definition 4:** A lattice is called regular if its parity check matrix \( H \), or the corresponding Tanner graph, is \((d_x, d_c)\) regular, i.e., the number of nonzero elements in all columns and all rows are the same and are respectively equal to \( d_x \) and \( d_c \).

Suppose that for \( 0 \leq l \leq a \)

\[
d_s^l = d_s^0 \quad 1 \leq j \leq n
\]

and select a divisor \( d_c \) of \( n \) such that \( d_c > d_x \). Also let \( r_l \) be such that

\[
d_s^l = r_l d_c \quad 0 \leq l \leq a. \quad (7)
\]

Now, use the E-PEG algorithm to construct a regular Tanner graph. The corresponding lattice which can be made by this regular Tanner graph is also regular.

### III. Regular LDPC Lattice

Let \( d_c = 2^{a+1} \) and \( d_s^l = l + 2 \) for \( 0 \leq l \leq a \). Using equation \( (7) \) to compute \( r_l \)'s, we get

\[
r_l = \frac{l + 2}{2^{a+1}}
\]

for every \( 0 \leq l \leq a \). E-PEG algorithm with above initial parameters constructs an \((a + 2, 2^{a+1}; a + 1)\) level Tanner graph. Let \( H \) be the \((a + 1)\)-level incidence matrix of this Tanner graph and \( \Lambda \) be its corresponding lattice. Then \( \Lambda \) is an \((a + 2, 2^{a+1}; a + 1)\) level lattice. These classes of lattices are denoted by \( L_{a+1}^{a+1} \). These types of lattices are the same as the lattices in \([7]\).

We note that \( H \) is an \((a + 1)\)-level matrix constructed using E-PEG. Denote the \( l \)'th level of \( H \) by \( H_l \) which is an \( r_l \times n \) matrix. Every row of \( H_l \) has \( d_c = 2^{a+1} \) one and every column...
of $H_l$ has $d_i^l = l + 2$ one and all other elements are zero. So we have $n(l + 2) = r_i(2^{a+1})$.

Let’s do an example to reveal the notations that we introduced so far.

**Example 5:** Consider the $(3, 4; 2)$ regular lattice

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 2
\end{bmatrix}
\]

Here $a = 2, d_e = 4$ for $1 \leq i \leq 12$, $d_i^2 = 2$ and $d_i^3 = 3$.

In the rest of this section we want to compute the coding gain and the kissing number of regular LDPC lattices regarding $a + 1$ and $n$. Here we mention a strong theorem concerning minimum distance of codes which their corresponding Tanner graphs have regular from [10].

**Theorem 6:** If $G$ is a regular connected graph with bit nodes of uniform degree $i$, $r$ parity nodes of uniform degree $j$ and incidence matrix $H$, the minimum distance of the code satisfies

\[
d \geq \frac{n(2i - \mu_2)}{ij - \mu_2}
\]

where $ij = \mu_1 \geq \mu_2$ are the largest eigenvalues of the matrix $H^tH$.

Let $C_l$ be the corresponding Tanner graph of $H_l$, the $l^{th}$ level of the parity check matrix of the regular lattice $\Lambda$, then $d_i^l = l + 2$ and $d_e = 2^{a+1}$ play the roles of $i$ and $j$ in [5] respectively. Hence we have

\[
d_{\min}^l \geq \frac{n(2(l + 2) - \mu_2)}{(l + 2)2^{a+1} - \mu_2} \geq \frac{n}{(l + 2)2^{a+1}}
\]

for $0 \leq l \leq a$.

**Theorem 7:** If $L_{n}^{a+1}$ is an $(a + 2, 2^{a+1}; a + 1)$ regular $n$-dimensional lattice with $n \geq (a + 2)8^{a+1}$ then

\[
d_{\min}^{a+1}(L_{n}^{a+1}) = 4^{a+1},
\]

and

\[
\gamma(\Lambda) = 4^{a+1} - \frac{(a + 1)(a + 2) + 2(a + 1)}{2^{a+2}}.
\]

**Proof:** By Theorem 2 the volume of a regular LDPC lattice can be computed by $\det(L_{n}^{a+1}) = 2^{\sum_{i=0}^{r} r_i}$. Hence,

\[
\frac{2}{n} \sum_{l=0}^{a} r_i l = \frac{2}{n} \sum_{l=0}^{a} \frac{l + 2}{2^{a+1}n}
\]

\[
= \frac{2}{n} \left( \frac{n}{2^{a+1}} \sum_{l=0}^{a} (l + 2) \right)
\]

\[
= \frac{1}{2^a} \left( 2 + 3 + \cdots + (a + 2) \right)
\]

\[
= \frac{1}{2^a} \left( \frac{(a + 1)(a + 2) + (a + 1)}{2} \right)
\]

\[
= \frac{(a + 1)(a + 2) + 2(a + 1)}{2^{a+1}}.
\]

So,

\[
(\det(L_{n}^{a+1}))^\frac{1}{a} = 2^{\frac{(a + 1)(a + 2) + 2(a + 1)}{2^{a+1}}}. \tag{11}
\]

In addition, since $d_{\min}^{a+1} \geq \frac{n}{(l + 2)2^{a+1}}$, for $0 \leq l \leq a$, the minimum distance of $L_{n}^{a+1}$ satisfies the following inequalities

\[
d_{\min}^{a+1}(L_{n}^{a+1}) \geq \min_{0 \leq l \leq a} \left\{ \frac{4^{n}}{(a + 2 - l)2^{a+1}, 4^{a+1}} \right\}.
\]

So,

\[
d_{\min}^{a+1}(L_{n}^{a+1}) > \min \left\{ 4^{a+1}, \frac{n}{(a + 2)2^{a+1}} \right\}. \tag{12}
\]

Since $n \geq (a + 2)8^{a+1}$ then the right hand side of (12) is equal to $4^{a+1}$. Now because $d_{\min}^{a+1}(L_{n}^{a+1}) \leq 4^{a+1}$, so $d_{\min}^{a+1}(L_{n}^{a+1}) = 4^{a+1}$. Replacing (11) and $d_{\min}^{a+1}(L_{n}^{a+1}) = 4^{a+1}$ in the definition of coding gain, turns out that we have

\[
\gamma(L_{n}^{a+1}) = 4^{a+1} - \frac{(a + 1)(a + 2) + 2(a + 1)}{2^{a+2}}.
\]

**Theorem 8:** If $L_{n}^{a+1}$ is an $(a + 2, 2^{a+1}; a + 1)$ regular $n$-dimensional lattice with $n \geq (a + 2)8^{a+1}$, then the kissing number of $L_{n}^{a+1}$ is $2n$.

**Proof:** Based on Theorem 7 we have $d_{\min}^{a+1}(L_{n}^{a+1}) = 4^{a+1}$.

The only points in $L_{n}^{a+1}$ that achieve $d_{\min}^{a+1}(L_{n}^{a+1})$ are $2n$ points $\pm 2^{a+1}e_i$ for $1 \leq i \leq n$ where $e_i$ is the $i^{th}$ unit vector plus those points in $C_l$’s which satisfy inequality (6) by equality. The later points must be in $C_l$’s with weight $d_{\min}^{a+1}$ such that $4^{a+1} - d_{\min}^{a+1} = 4^{a+1}$. This means that the kissing number of $L_{n}^{a+1}$ for $n \geq (a + 2)8^{a+1}$ is bounded above by

\[
2n + \sum_{1 \leq l \leq a} 2^{d_{\min}^{a+1}} A_{d_{\min}^{a+1}} \tag{13}
\]

where $A_{d_{\min}^{a+1}}$ denotes the number of codewords in $C_l$ with weight $d_{\min}^{a+1}$. Since $L_{n}^{a+1}$ is an $(a + 2, 2^{a+1}; a + 1)$ regular lattice, then the equation (10) implies that

\[
d_{\min}^{a+1} \geq \frac{n}{(j + 2)2^{a+1}} \geq \frac{(a + 2)8^{a+1}}{(j + 2)2^{a+1}} > 4^{a+1}.
\]

This means that in (13) there exist no terms in summation and the kissing number of $L_{n}^{a+1}$ is $2n$. ■
IV. Ensemble of Capacity-Achieving Lattices

By means of multilevel coding and using Construction D lattices Forney et al. [3] has proven, in the following Theorem, the existence of binary lattices which can achieve sphere-bound on the AWGN channels:

Theorem 9: (Sphere Bound): For large n, the probability of error $P_e$ of a minimum-distance decoder for an n-dimensional lattice on an AWGN channel with noise variance $\sigma^2$ per dimension cannot be small unless $\alpha^2 > 1$. Moreover, if $\alpha^2 = 1$, then $P_e$ cannot be small unless n is large. Therefore, we have the following definitions.

Definition 10: A lattice $\Lambda$ is said to be sphere-bound-achieving if

$$P_e(\Lambda, \alpha^2) \to 0$$

whenever $\alpha^2 > 1$.

Definition 11: A class of packings of Euclidean n-space is capacity-achieving for the AWGN channel [5] with noise variance $\sigma^2$ per dimension if there exists lattice $\Lambda$ in the class with $\alpha^2 = 1$ (NLD = $C_\infty$) and $P_e(\Lambda, \alpha^2) \to 0$.

Here for the AWGN channel with noise variance $\sigma^2$ per dimension and an n-dimensional lattice $\Lambda$ we have

$$\mathrm{NLD} = \frac{1}{n} \ln \left( \frac{1}{\det(\Lambda)} \right)$$

and

$$C_\infty = \frac{1}{2} \ln \left( \frac{1}{2\pi e \sigma^2} \right).$$

Therefore NLD = $C_\infty$, implies $\det(\Lambda)^{\frac{1}{n}} \geq 1$ which is equivalent to $\alpha^2 = 1$.

So by the definition a class of packings of Euclidean n-space is capacity-achieving for the AWGN channel with noise variance $\sigma^2$ per dimension if there exists lattice $\Lambda$ in the class with $\alpha^2 = 1$ and $P_e(\Lambda, \alpha^2) \to 0$.

When $\sigma$ is small, a simple estimation of the $P_e(\Lambda, \alpha^2)$ in [3] and [4] for a minimum distance decoder is given by Conway et al. in [3],

$$P_e(\Lambda, \alpha^2) \lesssim \frac{1}{2} \text{erfc} \left( \frac{\rho}{\sqrt{2\sigma}} \right)$$

where $\rho = \frac{d_{\text{mp}}}{2}$ is the packing radius of $\Lambda$ and $\tau$ is the average number of code points at distance $2\rho$ from a code point.

If we use the formula of coding gain and $\alpha^2$, then we have:

$$P_e(\Lambda, \alpha^2) \lesssim \frac{\tau}{2} \left( \frac{\sqrt{\pi e}}{4} \gamma(\Lambda) \alpha^2 \right)$$

for a maximum likelihood decoder where $\tau$ is the kissing number of lattice $\Lambda$. That is a key observation of our paper.

Theorem 12: For AWGN channel with noise variance $\sigma^2$ per dimension, $L_n^{a+1}$ is sphere-bound-achieving and capacity-achieving for $n = (a+2)8^{a+1}$ and $a \geq 2$.

Proof: Theorems [7] and [8] and equation (15) turn out that

$$P_e(L_n^{a+1}, \alpha^2) \lesssim n \text{erfc} \left( \sqrt{\frac{\pi e \gamma(\Lambda) \alpha^2}{4}} \right)$$

where $\text{erfc}(w) \leq e^{-w^2}$ for every $w \geq 0$ explains (16). Also (17) is true since

$$\lim_{a \to \infty} (a + 2)8^{a+1} e^{-\pi \sigma(4^{a-2})\alpha^2} = 0.$$

By the definition of limit for every arbitrary $\varepsilon = 10^{-\nu}$, there exist an $N$ such that for every $a \geq N \geq 2$, we have

$$(a + 2)8^{a+1} e^{-\pi \sigma(4^{a-2})\alpha^2} \leq 10^{-\nu}.$$  

This means that selecting $a$ and $n$ properly, would be resulted in the decreasing of $P_e(L_n^{a+1}, \alpha^2)$ dramatically. So $L_n^{a+1}$ are sphere-bound-achieving for $a \geq 2$. Now, the above discussion is true whenever $\alpha^2 = 1$. This means that $(a+1)$-level regular LDPC lattices of dimension $n = (a+2)8^{a+1}$ are capacity-achieving.

V. Simulation and Concluding Remarks

Here we simulate upper bound [15] on the performance analysis of regular LDPC lattices. For a fixed $n = (a+2)8^{a+1}$, it can be seen that increasing the number of level of construction up to $a$, can result in gaining reliable communication. It is shown in Fig. 1 that increasing the level of construction for a 2048-dimensional regular LDPC lattices from 1 to 3 would be resulted in more and more coding gain. In practice, it is sufficient for us to have $P_e(\Lambda, \alpha^2) \leq 10^{-6}$. It seems that $(a+1)$-level regular LDPC lattices with dimension $n = (a+2)8^{a+1}$ and $a \geq 2$ are capacity-achieving. Lattices decoding is generally an NP-hard problem, however it is important to note that there exist some iterative algorithms like generalized min-sum algorithm [7] and also max-product [2] algorithm which can run properly and test the goodness of such regular LDPC lattices. On the other hand, finding low complexity decoding algorithms for lattices in general case would be of interest.

REFERENCES


