Fifty-first Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 2 - 3, 2013

On the Capacity of the Modulo Lattice Channels

Hamed Mirghasemi and Jean-Claude Belfiore

***Abstract*—The modulo lattice channel is a key ingredient in the study of lattice encoding and decoding for the AWGN channel. In this paper, the capacity of the modulo lattice channels is investigated.**

I. Introduction

Since de Buda's theorem [1] which demonstrates that the spherical lattice codes can achieve the capacity of the AWGN channel, a great deal of effort has been made to design practical coding schemes for the AWGN channel. One of the long-standing problem in the application of lattice codes for the AWGN channel was if lattice decoding (rather than ML decoding) can achieve the capacity of the AWGN channel. In [2], Erez and Zamir showed that nested lattice codes with lattice decoding can achieve the capacity of the AWGN channel. A key ingredient in their work was to transform the AWGN channel to the modulo lattice channel which allows to incorporate nested lattice coding. While this channel transformation is not information preserving, they showed that if lattice is "good for quantization", the modulo lattice channel is asymptotically (in lattice dimension) the same as the AWGN channel at any noise variance. AWGN channel transformation to modulo lattice channel were also used in [9] to prove that the structured binning can achieve the Costa's dirty-paper channel capacity, and in [3] to show that there exists a class of coset codes that can achieve the Plotyrev's capacity [6].

To evaluate the capacity of the modulo lattice channel, we need to evaluate an integration over the Voronoi region which would be a tedious task even for small dimensions. In [3], the asymptotic behavior of modulo lattice channel capacity has been studied and for two different volume-to-noise ratio (VNR) regimes, two channel capacity estimates have been provided. In this paper, we provide lower and upper bounds on the capacity of the modulo lattice channel. These bounded are provided for two different regimes, small VNR regime and large VNR regime, and in each regime, the proposed capacity bounds are asymptotically tight. In Sections II and III, our proposed capacity bounds are stated and their asymptotic behavior and numerical results have been studied and finally, Section IV contains the poof of our main results.

This work was supported in part by FP7 PHYLAWS. Hamed Mirghasemi and Jean-Claude Belfiore are with the Communications and Electronics Department, Telecom ParisTech, 75634 Paris Cedex 13. Emails: {mirghasemi,belfiore@telecom-paristech.fr}.

A. Preliminaries on lattices

An n-dimensional lattice Λ is a discrete subgroup of the Euclidean space $\mathbb{R}^n$ and is defined by

$$\Lambda = \{A\mathbf{z} \ : \mathbf{z} \in \mathbb{Z}^n\}$$

where the columns of the basis matrix $A = [\mathbf{a}_1, \cdots, \mathbf{a}_n]$ are linearly independent. Given Λ, the nearest-neighbor quantizer function: $\mathbb{R}^n \to \Lambda$ is defined by

$$Q_\Lambda(\mathbf{x}) = \arg\min_{\lambda\in\Lambda} \|\mathbf{x}-\lambda\|\,, \quad \forall \mathbf{x} \in \mathbb{R}^n\,.$$

The fundamental Voronoi region $\mathcal{V}(\Lambda)$ of Λ is the set of points in $\mathbb{R}^n$ whose nearest lattice point is origin, i.e. $\mathcal{V}(\Lambda) = \{\mathbf{x}|\, Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$. The volume of Λ is defined as the volume of $\mathcal{V}(\Lambda)$ and is given by $V(\Lambda) = \int_{\mathcal{V}(\Lambda)} \mathrm{d}\mathbf{z}$. For any $\mathbf{x} \in \mathbb{R}^n$, the mod-$\Lambda$ function: $\mathbb{R}^n \to \mathcal{V}(\Lambda)$ is given by

$$\mathbf{x} \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x})\,.$$

For any given lattice Λ, the radius $r_p(\Lambda)$ of the largest sphere centered on the origin and entirely contained in $\mathcal{V}(\Lambda)$ is the packing radius. The smallest $r_c(\Lambda)$ for which the sphere with radius $r_c(\Lambda)$ centered on the origin covers $\mathcal{V}(\Lambda)$ is the covering radius. The minimum distance between lattice points and the number of lattice points with minimum distance to the origin (i.e. kissing number) are denoted respectively by $d_{\min}(\Lambda)$ and $K(\Lambda)$. The Theta series of a lattice is also given by $\Theta_\Lambda(q) \overset{\text{def}}{=} \sum_{\lambda\in\Lambda} e^{-\pi q\|\lambda\|^2}$. For any full rank lattice Λ, its dual lattice is defined as $\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n | \forall\lambda \in \Lambda, <\lambda, \mathbf{y}> \in \mathbb{Z}\}$.

B. The mod-Λ channel

Given an n-dimensional lattice Λ, the mod-Λ channel is an additive channel whose:

- input ($\mathbf{x}$) is restricted to the Voronoi cell $\mathcal{V}(\Lambda)$.
- input is transmitted over an AWGN channel with the noise variance σ^2

$$\mathbf{y}' = \mathbf{x} + \mathbf{N} \ , \mathbf{N} \sim g_{\sigma^2}(\mathbf{w}) = \frac{1}{(\sqrt{2\pi\sigma^2})^n} e^{-\|\mathbf{w}\|^2/2\sigma^2}\,.$$

- output $\mathbf{y}$ is mapped to $\mathcal{V}(\Lambda)$ by the mod-Λ function

$$\mathbf{y} = \mathbf{y}' \bmod \Lambda\,.$$

The capacity of the mod-Λ channel is given by [1] [3]

$$C(\Lambda, \sigma^2) = \log V(\Lambda) - h(\Lambda, \sigma^2)\,, \tag{1}$$

where $h(\Lambda, \sigma^2)$ is the differential entropy of the Λ-aliased Gaussian noise $\mathbf{N}' = \mathbf{N} \bmod \Lambda$ whose probability density function is given by

$$\begin{aligned} f_{\Lambda,\sigma^2}(\mathbf{z}) &= \sum_{\lambda \in \Lambda} g_{\sigma^2}(\mathbf{z} + \lambda) \\ &= \frac{1}{(\sqrt{2\pi\sigma^2})^n} \sum_{\lambda} e^{-\|\mathbf{z}+\lambda\|^2/2\sigma^2}\,. \end{aligned}$$

and

$$h(\Lambda, \sigma^2) = -\int_{\mathcal{V}(\Lambda)} f_{\Lambda,\sigma^2}(\mathbf{z}) \log f_{\Lambda,\sigma^2}(\mathbf{z})\, d\mathbf{z}\,. \tag{2}$$

Let's denote the volume-to-noise (VNR) ratio of Λ by $\alpha(\Lambda, \sigma^2)$

$$\alpha(\Lambda, \sigma^2) = \frac{V(\Lambda)^{2/n}}{2\pi e \sigma^2}\,.$$

The following theorem provides the first-order estimates of the mod-Λ channel capacity [3, Theorems 20 and 21] in bits per n dimensions.

Theorem 1. • *For large* $\alpha(\Lambda, \sigma^2)$

$$C(\Lambda, \sigma^2) \approx \frac{n}{2} \log \alpha(\Lambda, \sigma^2) + \pi P_e(\Lambda, \sigma^2) \log e\,. \tag{3}$$

where $P_e(\Lambda, \sigma^2)$ *is the error probability of lattice decoding*

$$P_e(\Lambda, \sigma^2) = 1 - \int_{\mathcal{V}(\Lambda)} g_{\sigma^2}(\mathbf{z})\, d\mathbf{z}\,.$$

- *For small* $\alpha(\Lambda, \sigma^2)$

$$C(\Lambda, \sigma^2) \approx \frac{K(\Lambda^*)}{2} e^{-4\pi^2\sigma^2 d^2_{min}(\Lambda^*)} \log e\,, \tag{4}$$

where $K(\Lambda^*)$ *and* $d_{min}(\Lambda^*)$ *are respectively the kissing number and the minimum distance of* Λ^*.

II. Small VNR regime

We first consider the small VNR regime where the Λ-aliased Gaussian distribution approaches the uniform distribution over $\mathcal{V}(\Lambda)$. In [4], the flatness factor is defined as

$$\epsilon(\Lambda, \sigma^2) \stackrel{\text{def}}{=} V(\Lambda) \times \max_{\mathbf{z} \in \mathcal{V}(\Lambda)} |f_{\Lambda,\sigma^2}(\mathbf{z}) - 1/V(\Lambda)|\,, \tag{5}$$

[1]Logarithms are taken to the base 2 throughout the paper.

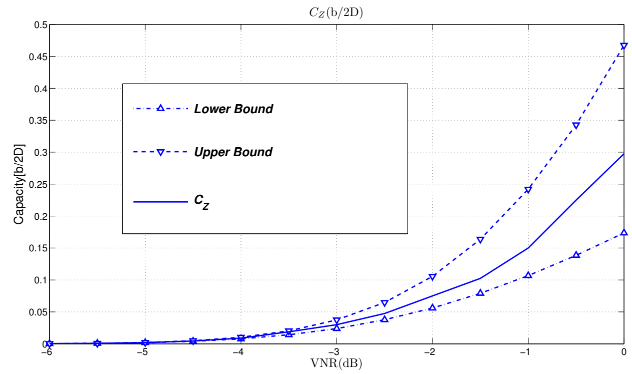

Fig. 1. Normalized capacity curves $C(\mathbb{Z})$ in b/2D for VNR smaller than $0\,dB$.

and it is shown that, for any lattice Λ and noise variance σ^2, we have

$$\epsilon(\Lambda, \sigma^2) = \Theta_{\Lambda^*}(2\pi\sigma^2) - 1\,. \tag{6}$$

As $\sigma^2 \to \infty$, $\epsilon_{\Lambda,\sigma^2} = O(e^{-2\pi d(\Lambda^*)\sigma^2})$ and therefore, in small VNR regime, this parameter provides a tight bound on the maximum difference between f_{Λ,σ^2} and $1/V(\Lambda)$. The capacity bounds for small VNR regime are stated in the following theorem.

Theorem 2. *For any lattice* Λ *and noise variance* σ^2*, we have*

$$\begin{aligned} \beta(\Lambda, \sigma^2)(\Theta_{\Lambda^*}(4\pi\sigma^2) - 1) &\le C(\Lambda, \sigma^2) \\ &\le \gamma(\Lambda, \sigma^2)(\Theta_{\Lambda^*}(4\pi\sigma^2) - 1)\,, \end{aligned} \tag{7}$$

where

$$\begin{aligned} \beta(\Lambda, \sigma^2) &\stackrel{def}{=} \frac{\log e}{2(1 + \epsilon(\Lambda, \sigma^2))} \\ \gamma(\Lambda, \sigma^2) &\stackrel{def}{=} \log e (1 - \frac{1}{2(1 + \epsilon(\Lambda, \sigma^2))^2})\,. \end{aligned}$$

We note that our theorem recovers the asymptotic behavior analysis of $C(\Lambda, \sigma^2)$ (cf. (4)) in [3, Theorem20] since as $\sigma^2 \to \infty$, we have

$$\Theta_{\Lambda^*}(4\pi\sigma^2) - 1 \approx K(\Lambda^*) e^{-4\pi\sigma^2 d^2(\Lambda^*)}\,.$$

and $\beta(\Lambda, \sigma^2) \approx \gamma(\Lambda, \sigma^2) \approx 0.5 \log e$.

Corollary 1. *When* $\sigma^2 \to \infty$*, we have*

$$C(\Lambda, \sigma^2) = O(e^{-4\pi\sigma^2 d^2(\Lambda^*)})\,.$$

Figs. 1 and 2 show the capacity curves of mod-Λ channels for $\mathbb{Z}$, and the hexagonal lattice A_2. We can see that these bounds are fairly close for a wide range of VNR. For instance, their difference at VNR lower than $-1.5\,dB$ is about 0.1 bits per two dimensions.

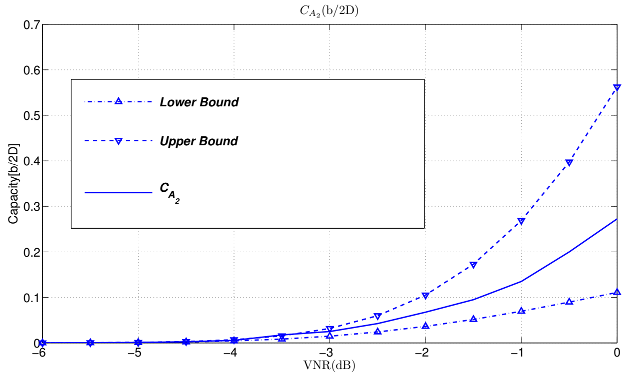

Fig. 2. Normalized capacity curves $C(A_2)$ in b/2D for VNR smaller than $0\,dB$.

III. Large VNR regime

Rearranging the terms in (2) yields

$$C(\Lambda,\sigma^2)=\frac{n}{2}\log(\alpha(\Lambda,\sigma^2))+\log e\times \Big(D_{\text{KL}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))-D_{\text{var}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))\Big)\,, \tag{8}$$

where $D_{\text{KL}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))$ is the KL divergence between $f_{\Lambda,\sigma^2}(\mathbf{z})$ and $g_{\sigma^2}(\mathbf{z})$, defined by

$$D_{\text{KL}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))\overset{\text{def}}{=}\int_{\mathcal{V}(\Lambda)} f_{\Lambda,\sigma^2}(\mathbf{z})\ln(f_{\Lambda,\sigma^2}(\mathbf{z})/g_{\sigma^2}(\mathbf{z}))\,\mathrm{d}\mathbf{z} \tag{9}$$

and $D_{\text{var}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))$ is the variance distance between $f_{\Lambda,\sigma^2}(\mathbf{z})$ and $g_{\sigma^2}(\mathbf{z})$, defined by

$$D_{\text{var}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))\overset{\text{def}}{=}\frac{1}{2\sigma^2}\Big(\int_{\mathcal{V}(\Lambda)}\|\mathbf{z}\|^2 f_{\Lambda,\sigma^2}(\mathbf{z})\mathrm{d}\mathbf{z}-\int_{\mathbb{R}^n}\|\mathbf{z}\|^2 g_{\sigma^2}(\mathbf{z})\mathrm{d}\mathbf{z}\Big)\,. \tag{10}$$

We note that the first term in (8) is the asymptotic capacity of Λ-mod channel (bits per n dimensions) in large VNR regime. Thus, the capacity of mod-Λ channel would approach its limit in large VNR regime if and if:

- The KL divergence between the Λ-aliased density $f_{\Lambda,\sigma^2}(\mathbf{z})$ and the Gaussian density $g_{\sigma^2}(\mathbf{z})$ goes to zero;
- and the variance distance between the Λ-aliased density and the Gaussian density approaches zero.

A. The KL distance

First, we deal with $D_{\text{KL}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))$. For any given lattice Λ and noise variance σ^2, we define the ratio function as

$$r_{\Lambda,\sigma^2}(\mathbf{z})\overset{\text{def}}{=}\frac{f_{\Lambda,\sigma^2}(\mathbf{z})}{g_{\sigma^2}(\mathbf{z})} =1+\sum_{\lambda\in\Lambda\setminus\{0\}} e^{-\|\lambda\|^2/2\sigma^2}e^{-<\lambda,\mathbf{z}>/\sigma^2}\ ,\forall\mathbf{z}\in\mathcal{V}(\Lambda)\,. \tag{11}$$

In Lemmas 6 and 7, we show that for any $\mathbf{z}\in\mathcal{V}(\Lambda)$, we have

$$\Theta_\Lambda(1/2\pi\sigma^2)\le r_{\Lambda,\sigma^2}\le r_m(\Lambda,\sigma^2)\,,$$

where $r_m(\Lambda,\sigma^2)$ is the "Gaussianity factor" and is defined by

$$r_{\text{M}}(\Lambda,\sigma^2)\overset{\text{def}}{=}e^{r_c^2(\Lambda)/2\sigma^2}\max_{\mathbf{z}^*\in\mathcal{Z}^*}\Theta_{\Lambda+\mathbf{z}^*}(1/2\pi\sigma^2)\,, \tag{12}$$

where $\mathcal{Z}^*$ is set of Voronoi region vertices and

$$\Theta_{\Lambda+\mathbf{z}^*}(1/2\pi\sigma^2)=\sum_{\lambda\in\Lambda}e^{-\|\mathbf{z}^*+\lambda\|^2/2\sigma^2} \tag{13}$$

is the Theta series of the shifted lattice to a vertex $\mathbf{z}^*$ of Voronoi region. The following theorem provides a lower and upper bounds on $D_{\text{KL}}(f,g)$ in the terms of $P_e(\Lambda,\sigma^2)$.

Theorem 3. *For any given lattice Λ and noise variance σ^2, we have*

$$2\,P_e^2(\Lambda,\sigma^2)\le D_{KL}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z})) \le(1+ln(r_M(\Lambda,\sigma^2)))P_e(\Lambda,\sigma^2)\,. \tag{14}$$

Now, we turn to analyze the asymptotic behavior of our proposed bounds on $D_{\text{KL}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))$. Lemma 5 in Section IV implies that r_M is bounded as σ^2 goes to zero and hence, the proposed upper bound is equal to $O(P_e(\Lambda,\sigma^2))$ as $\sigma^2\to 0$. Therefore, the decline rate of $D_{\text{KL}}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))$ is between $O(P_e(\Lambda,\sigma^2))$ and $O(P_e^2(\Lambda,\sigma^2))$ as $\sigma^2\to 0$. Figs. 3 and 4 show the upper and lower bounds on the KL distance for $\Lambda=\mathbb{Z}$ and $\Lambda=A_2$, respectively. Numerical results suggest that our proposed upper bound is closer to D_{KL} than the upper bound. Also we can see that these bounds are fairly close for a wide range of VNR. For instance, the maximum gap between our lower and upper bounds is about 0.05 bits per two dimensions for VNR$=1\,dB$.

B. The variance distance

Now we state our proposed bounds on $D_{\text{var}}(f(\mathbf{z}),g(\mathbf{z}))$. For any integer n and any $r\ge 0$, we define functions $S(n,r,\sigma^2)$ and $P_e(n,r,\sigma^2)$ as follows:

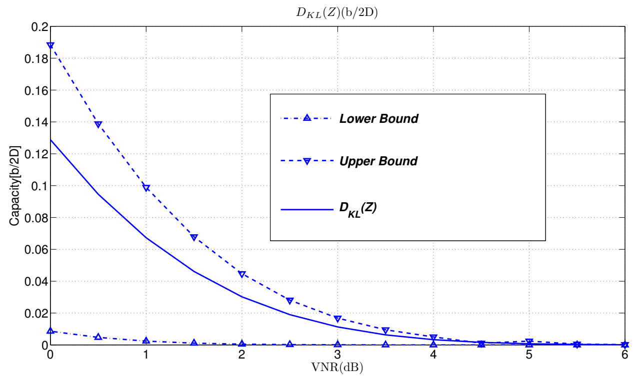

Fig. 3. Normalized bounds on $D_{\rm KL}(Z)$ in b/2D for VNR larger than $0\,dB$.

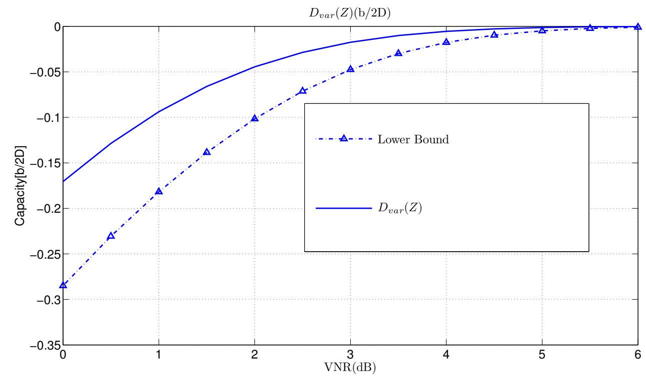

Fig. 5. Normalized bounds on $D_{\rm var}(Z)$ in b/2D for VNR larger than $0\,dB$.

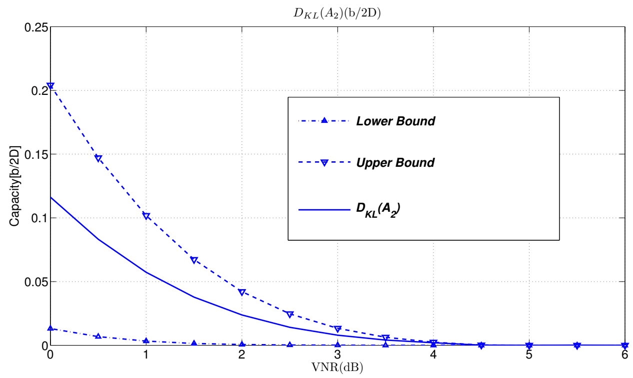

Fig. 4. Normalized bounds on $D_{\rm KL}(A_2)$ in b/2D for VNR larger than $0\,dB$.

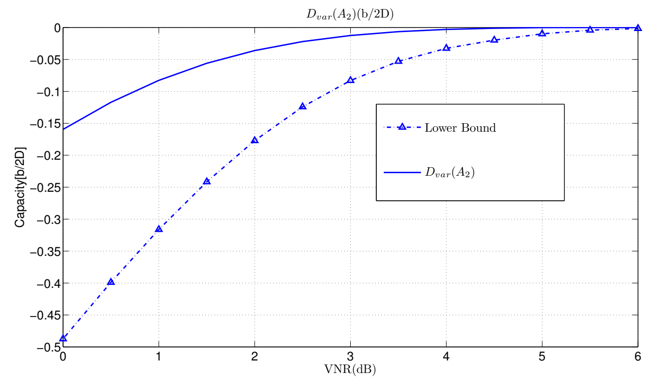

Fig. 6. Normalized bounds on $D_{\rm var}(A_2)$ in b/2D for VNR larger than $0\,dB$.

- If n is an even integer

$$S(n,r,\sigma^2) \stackrel{\text{def}}{=} \frac{n}{2}(1-e^{-y}\sum_{k=0}^{n/2} y^k/k!)$$

$$P_e(n,r,\sigma^2) \stackrel{\text{def}}{=} e^{-y}\sum_{k=0}^{n/2-1} y^k/k!\,;$$

- If n is an odd integer

$$S(n,r,\sigma^2) \stackrel{\text{def}}{=} \frac{n}{2}\Big(1-\text{erfc}(y^{1/2})- e^{-y}\sum_{k=0}^{(n-1)/2}\frac{y^k}{(k+1/2)!}\Big)$$

$$P_e(n,r,\sigma^2) \stackrel{\text{def}}{=} \text{erfc}(y^{1/2})+e^{-y}\sum_{k=0}^{(n-1)/2-1}\frac{y^k}{(k+1/2)!}\,,$$

where $y = r^2/(2\sigma^2)$ and

$$\text{erfc(y)} \stackrel{\text{def}}{=} \frac{2}{\sqrt{\pi}}\int_0^y e^{-t^2}\,\text{dt}\,.$$

In [7], it is shown that $P_e(n,r,\sigma^2)$ is the probability of decoding error when the decoding region is the n-dimensional sphere of radius r centered at the origin. Similarly, in Lemma 9 in Section IV, we prove that $S(n,r,\sigma^2)$ is equal to $1/2\sigma^2\int_{\mathcal{S}(n,r)}\|\mathbf{z}\|^2 g_{\sigma^2}(\mathbf{z})\text{d}\mathbf{z}$, where $\mathcal{S}(n,r)$ is the n-dimensional sphere of radius r centered at the origin.

Theorem 4. *For any given lattice Λ and noise variance σ^2, we have*

$$y_p\times(P_e(\Lambda,\sigma^2)-P_e(n,r_p,\sigma^2))+S(n,r_p,\sigma^2)-n/2\leq D_{var}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))\leq 0\,.$$

where $y_p = r_p^2(\Lambda)/2\sigma^2$.

From [7], we know that for any finite dimensional lattice, the decline rate of $P_e(\Lambda,\sigma^2)$ is between $O(\frac{1}{\sigma^{n-2}}e^{\frac{-r_e^2(\Lambda)}{2\sigma^2}})$ and $O(\frac{1}{\sigma^{n-2}}e^{\frac{-r_p^2(\Lambda)}{2\sigma^2}})$ where $r_e(\Lambda)$ is the equivalent radius of lattice Λ. Therefore, we can easily conclude that for any finite dimension n, the decline rate of our proposed bounds on $D_{\rm var}(f_{\Lambda,\sigma^2}(\mathbf{z}),g_{\sigma^2}(\mathbf{z}))$ is at least equal to $O(\frac{1}{\sigma^n}e^{\frac{-r_p^2(\Lambda)}{2\sigma^2}})$ as $\sigma^2\to 0$. Figs. 5 and 6 illustrate the numerical evaluations of our proposed lower bound on the $D_{\rm var}(f_{\Lambda,\sigma^2}(\mathbf{z}),g(\mathbf{z}))$ for lattices $\mathbb{Z}$ and A_2. As we can see, as VNR increases, the gap between the lower bound and the actual value deceases. Also, we can see that the lower bound has better performance for lattice $\mathbb{Z}$ than for lattice A_2. For instance, in $VNR = 2\,dB$, the gap between our proposed lower and upper bound is about 0.05(b/2D)

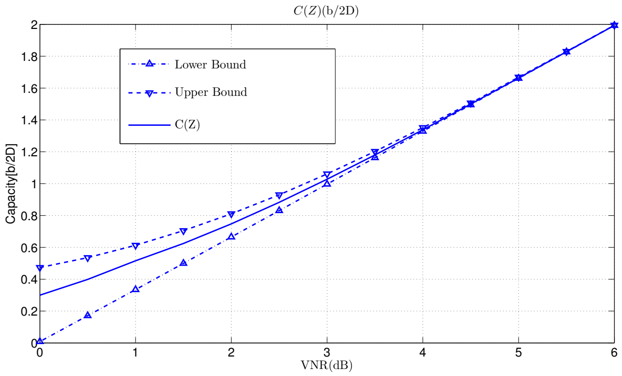

Fig. 7. Normalized capacity curves on $C(\mathbb{Z})$ in b/2D for VNR larger than $0\,dB$.

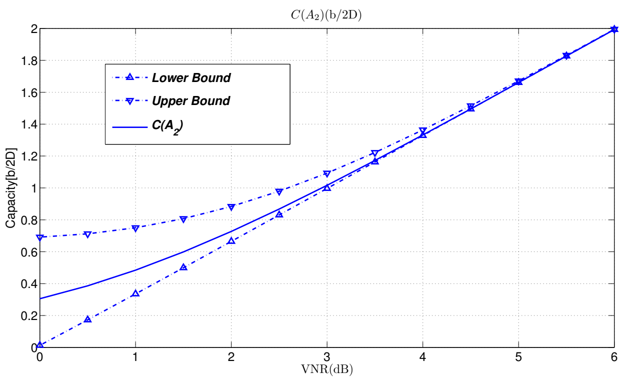

Fig. 8. Normalized capacity curves on $C(A_2)$ in b/2D for VNR larger than $0\,dB$.

while for lattice A_2 this gap is about 0.15(b/2D).

C. Capacity Bounds

Combination of Theorems 3 and 4 provides a lower and upper bound on the mod-Λ channel capacity in large VNR regime. In Figures 7 and 8, the numerical performance of these capacity bounds are plotted for two lattices $\mathbb{Z}$ and A_2. As we can see, the gap between capacity bounds approaches zero as $\sigma^2 \to 0$.

IV. Proof

In this chapter, $f_{\Lambda,\sigma^2}(\mathbf{z})$, $g_{\sigma^2}(\mathbf{z})$ and $\mathcal{V}(\Lambda)$ are abbreviated by $f(\mathbf{z})$, $g(\mathbf{z})$ and $\mathcal{V}$, respectively.

A. Proof of Theorem 2

In order to prove Theorem 2, we need the following lemmas.

Lemma 1. *For any given Λ and any two Λ-periodic functions $f(\mathbf{x})$ and $g(\mathbf{x})$ with Fourier coefficients $\hat{f}(\mathbf{y})$ and $\hat{g}(\mathbf{y})$, Fourier coefficients of $h(\mathbf{x}) = f(\mathbf{x})g(\mathbf{x})$ are given by*

$$\hat{h}(\mathbf{y}) = \sum_{\mathbf{z}\in\Lambda^*} \hat{f}(\mathbf{z})\hat{g}(\mathbf{y}-\mathbf{z}), \quad \forall\, \mathbf{y} \in \Lambda^* . \tag{15}$$

Lemma 1: For any $\mathbf{y} \in \Lambda^*$, the Fourier coefficients of the product function is

$$\begin{aligned}
\hat{h}(\mathbf{y}) &= \frac{1}{V(\Lambda)} \int_{\mathcal{V}} f(\mathbf{x})g(\mathbf{x})\, e^{-2\pi i<\mathbf{y},\mathbf{x}>}\, d\mathbf{x} \\
&= \frac{1}{V(\Lambda)} \int_{\mathcal{V}} \Big(\sum_{\mathbf{s}\in\Lambda^*} \hat{f}(\mathbf{s})\, e^{2\pi i<\mathbf{s},\mathbf{z}>} \Big) \\
&\qquad \Big(\sum_{\mathbf{t}\in\Lambda^*} \hat{g}(\mathbf{t})\, e^{2\pi i<\mathbf{t},\mathbf{z}>} \Big)\, e^{-2\pi i<\mathbf{y},\mathbf{x}>}\, d\mathbf{x} \\
&= \frac{1}{V(\Lambda)} \sum_{\mathbf{s}} \sum_{\mathbf{t}} \hat{f}(\mathbf{s})\hat{g}(\mathbf{t}) \int_{\mathcal{V}} e^{2\pi i<\mathbf{s}+\mathbf{t}-\mathbf{y},\mathbf{z}>}\, d\mathbf{x} \\
&\overset{(a)}{=} \sum_{\mathbf{s}} \hat{f}(\mathbf{s})\hat{g}(\mathbf{y}-\mathbf{s}),
\end{aligned}$$

where (a) follows from the fact that for any $\mathbf{y} \in \Lambda^*$, we have

$$\frac{1}{V(\Lambda)} \int_{\mathcal{V}(\Lambda)} e^{-2\pi i<\mathbf{z},\mathbf{y}>}\, d\mathbf{z} = \delta_{\mathbf{y}} .$$

■

Lemma 2. *For any $\epsilon \geq 0$ and $-1 < x \leq \epsilon$, we have*

$$\frac{1}{1+x}\Big(x + \frac{x^2}{2(1+\epsilon)}\Big) \leq ln(1+x) \leq x - \frac{x^2}{2(1+\epsilon)^2} . \tag{16}$$

Lemma 2: Let us define $s(x) \overset{\text{def}}{=} (1+x)\ln(1+x) - x - \beta x^2$ where $\beta \overset{\text{def}}{=} 1/(2(1+\epsilon))$. It can be easily shown that $s(0) = s'(0) = 0$, and for any $x \in (-1,\epsilon]$, we have $s''(x) > 0$. Therefore, we can conclude that $s(x) \geq 0$ for any $x \in (-1,\epsilon]$. The other side of the inequality can be similarly shown. ■

From the Fourier expansion of $f(\mathbf{z})$ ([3, 5]), we have

$$f(\mathbf{z}) = \frac{1}{V(\Lambda)} \sum_{\mathbf{y}\in\Lambda^*} \hat{f}(\mathbf{y}) e^{2\pi i<\mathbf{y},\mathbf{z}>} , \tag{17}$$

where the discrete Fourier coefficients of $f(\mathbf{z})$ is

$$\hat{f}(\mathbf{y}) = e^{-2\pi^2\sigma^2\|\mathbf{y}\|^2} . \tag{18}$$

We define $n(z) \overset{\text{def}}{=} V(\Lambda)f(z) - 1$. Substituting equation (18) in $h(\Lambda,\sigma^2)$ yields

$$h(\Lambda,\sigma^2) = \ln(V(\Lambda)) - \int_{\mathcal{V}(\Lambda)} f(\mathbf{z})\ln(1+n(\mathbf{z}))\, d\mathbf{z} .$$

The above inequalities provide us lower and upper bounds on $h(\Lambda,\sigma^2)$ as follows. Let us define $\beta = \frac{1}{2(1+\epsilon(\Lambda,\sigma^2))}$ and $\gamma = \frac{1}{2(1+\epsilon(\Lambda,\sigma^2))^2}$. From the RHS of

(16) we have

$$\begin{aligned}
h(\Lambda,\sigma^2) &\leq \ln(V(\Lambda)) - \int_{\mathcal{V}} \frac{f(\mathbf{z})}{1+n(\mathbf{z})}(n(\mathbf{z})+\beta n^2(\mathbf{z}))\,\mathrm{d}\mathbf{z} \\
&= \ln V(\Lambda) - \frac{1}{V}\int_{\mathcal{V}} (n(z)+\beta n^2(\mathbf{z}))\,\mathrm{d}\mathbf{z} \\
&= \ln(V(\Lambda)) - \frac{\beta}{V}\int_{\mathcal{V}} n^2(\mathbf{z})\mathrm{d}\mathbf{z} \\
&= \ln V(\Lambda) - \beta V \int_{\mathcal{V}} f^2(\mathbf{z})\mathrm{d}\mathbf{z} + \beta \\
&\overset{(a)}{=} \ln(V(\Lambda)) + \beta - \beta V^2(\Lambda)\sum_{\mathbf{y}\in\Lambda^*} \hat{f}(\mathbf{y})\hat{f}(-\mathbf{y}) \\
&\overset{(b)}{=} \ln(V(\Lambda)) + \beta(1-\sum_{\mathbf{y}\in\Lambda^*} e^{-4\pi\sigma^2\|\mathbf{y}\|^2}) \\
&= \ln(V(\Lambda)) + \beta(1-\Theta_{\Lambda^*}(4\pi\sigma^2)),
\end{aligned}$$

where (a) and (b) are respectively due to Lemma 1 and (18). Thus

$$C(\Lambda,\sigma^2) \geq \frac{\Theta_{\Lambda^*}(4\pi\sigma^2)-1}{2(1+\epsilon(\Lambda,\sigma^2))}$$

nats per n dimensions. The upper bound can be proved as follows:

$$\begin{aligned}
C(\Lambda,\sigma^2) &\leq \int_{\mathcal{V}} f(\mathbf{z})\ln(1+n(\mathbf{z}))\mathrm{d}\mathbf{z} \\
&\leq \frac{1}{V(\Lambda)}\int_{\mathcal{V}} (n(\mathbf{z})+1)(n(\mathbf{z})-\gamma n^2(\mathbf{z}))\mathrm{d}\mathbf{z} \\
&\leq \frac{1-\gamma}{V(\Lambda)}\int_{\mathcal{V}} n^2(\mathbf{z})\mathrm{d}\mathbf{z} + \frac{1}{V}\int_{\mathcal{V}} (n(\mathbf{z})\mathrm{d}\mathbf{z} \\
&= (1-\frac{1}{2(1+\epsilon(\Lambda,\sigma^2))})(\Theta_{\Lambda^*}(4\pi\sigma^2)-1).
\end{aligned}$$

B. *Poof of Theorem 3*

The following lemma provides a lower bound on the KL divergence between $f(\mathbf{z})$ and $g(\mathbf{z})$ in the terms of probability of error decoding $P_e(\Lambda,\sigma^2)$.

Lemma 3.

$$D_{KL}(f(\mathbf{z}),g(\mathbf{z})) \geq 2P_e^2(\Lambda,\sigma^2). \tag{19}$$

Proof of Lemma 3: Pinsker's inequality gives a lower bound on the KL divergence in terms of the total variation distance [8]

$$D_{\mathrm{KL}}(f(\mathbf{z}),g(\mathbf{z})) \geq \frac{1}{2}D^2_{\mathrm{TV}}(f(\mathbf{z}),g(\mathbf{z})),$$

where the total variation distance is given by

$$D_{\mathrm{TV}}(f(\mathbf{z}),g(\mathbf{z})) = \int_{\mathbb{R}^n} |f(\mathbf{z})-g(\mathbf{z})|\,\mathrm{d}z.$$

To prove the Lemma, we need to relate $D_{\mathrm{TV}}(f(\mathbf{z}),g(\mathbf{z}))$ to $P_e(\Lambda,\sigma^2)$. We note that in $\mathcal{V}(\Lambda)$, we have $f(\mathbf{z}) > g(\mathbf{z})$ and in $\mathbb{R}^n\setminus\mathcal{V}(\Lambda)$, we have $f(\mathbf{z})=0$. Thus

$$\begin{aligned}
D_{\mathrm{TV}}(f(\mathbf{z}),g(\mathbf{z})) &= \int_{\mathcal{V}} (f(\mathbf{z})-g(\mathbf{z}))\,\mathrm{d}\mathbf{z} + P_e(\Lambda,\sigma^2) \\
&= \int_{\mathcal{V}} \sum_{\lambda\setminus\{0\}} g(\mathbf{z}+\lambda)\,\mathrm{d}\mathbf{z} + P_e(\Lambda,\sigma^2) \\
&= \sum_{\lambda\setminus\{0\}} \int_{\mathcal{V}+\lambda} g(\mathbf{z})\,\mathrm{d}\mathbf{z} + P_e(\Lambda,\sigma^2) \\
&= 2\,P_e(\Lambda,\sigma^2),
\end{aligned}$$

where the last equality is due to $\cup_{\lambda\setminus\{0\}}\mathcal{V}(\Lambda)+\lambda = \mathbb{R}^n\setminus\mathcal{V}(\Lambda)$. ■

Now we will prove some important properties of the ratio function defined in equation (11). The first lemma guarantees that $r(\mathbf{z})$ is well defined for all $\mathbf{z}\in\mathcal{V}(\Lambda)$.

Lemma 4. *For any $z\in\mathcal{V}(\Lambda)$, the value of $r_{\Lambda,\sigma^2}(\mathbf{z})$ is finite.*

Proof of Lemma 4: Since the generator matrix A of the lattice is positive definite, there exists an $a>0$ such that $A^TA \geq aI_n$, where I_n is the $n\times n$ Identity matrix. Let's define $y=A^T\mathbf{z}$. For any given y, there exists an b such that $\max_{1\leq i\leq n}|y_i| < b$. Consider a given lattice point $\lambda = A\gtrdot$ where A is the generator matrix and $\gtrdot\in\mathbb{Z}^n$. Subsequently

$$\begin{aligned}
e^{-\|\lambda\|^2/2\sigma^2}e^{-<\lambda,\mathbf{z}>/\sigma^2} &\leq e^{-\frac{a}{2\sigma^2}\sum_{i=1}^n m_i^2+\frac{b}{\sigma^2}\sum_{i=1}^n|m_i|} \\
&= \prod_{i=1}^n e^{-\frac{a}{2\sigma^2}m_i^2+\frac{b}{\sigma^2}|m_i|}.
\end{aligned}$$

Taking the summation of the both sides on the above inequality over all $\lambda\in\Lambda\setminus$ yields

$$\begin{aligned}
&\sum_{\lambda} e^{-\|\lambda\|^2/2\sigma^2}e^{-<\lambda,\mathbf{z}>/\sigma^2} \\
&\leq \left(\sum_{m\geq 0} e^{-\frac{a}{2\sigma^2}m^2+\frac{b}{\sigma^2}m}\right)^n \\
&= e^{\frac{b^2n}{2a\sigma^2}} \times \left(\sum_{m\geq 0} e^{-\frac{1}{2\sigma^2}(m-b/a)^2}\right)^n.
\end{aligned}$$

The proof concludes by observing that the last series is convergent. ■

The following lemma shows that as $\sigma^2\to 0$, the value of $r_{\Lambda,\sigma^2}(\mathbf{z})$ is bounded.

Lemma 5. *For any $\mathbf{z}\in\mathcal{V}(\Lambda)$, $\lim_{\sigma^2\to 0} r_{\Lambda,\sigma^2}(\mathbf{z})$ is finite.*

Proof of Lemma 5: We note that for any finite value of $1/\sigma^2$, lemma 4 states that r_{Λ,σ^2} is bounded. Thus, we need to check that for any $\mathbf{z}\in\mathcal{V}(\Lambda)$ and any $\lambda\in\Lambda$, $\|\lambda\|^2+2<\mathbf{z},\lambda>$ can not be less than zero:

$$\|\lambda\|^2+2<\mathbf{z},\lambda> = \|\lambda+\mathbf{z}\|^2-\|\mathbf{z}\|^2 \geq 0,$$

where the last equality follows from the definition of $\mathcal{V}(\Lambda)$. ∎

The following Lemma states that $r_{\Lambda,\sigma^2}(\mathbf{z})$ attains its minimum at $\mathbf{z}=0$.

Lemma 6.

$$\min_{\mathbf{z}\in\mathcal{V}(\Lambda)} r_{\Lambda,\sigma^2}(\mathbf{z}) = \Theta_\Lambda(1/2\pi\sigma^2)\,. \tag{20}$$

Proof of Lemma 6: According to Mean-value theorem for multivariate functions, for any $\mathbf{z}\in\mathcal{V}(\Lambda)$, there exists a $0\le c\le 1$, such that

$$\begin{aligned} r(\mathbf{z}) &= r(0) + \nabla r((1-c)\mathbf{z}).\mathbf{z} \\ &= r(0) + \sum_{\lambda\setminus\{0\}} -\frac{<\lambda,\mathbf{z}>}{\sigma^2} e^{-<\lambda,\mathbf{z}>/\sigma^2} e^{-\|\lambda\|^2/2\sigma^2}\,. \end{aligned}$$

For any given $\mathbf{z}\in\mathcal{V}(\Lambda)$, we define $\Lambda_z \stackrel{\text{def}}{=} \{\lambda\in\Lambda| <\mathbf{z},\lambda>\ge 0\}$. We note that if $\lambda\in\Lambda_z$, then $-\lambda\in\Lambda\setminus\Lambda_z$ and $<\lambda,(1-c)\mathbf{z}>\ge 0$, $\forall c\in[0,1]$. Thus

$$\begin{aligned} r(\mathbf{z}) &= r(0) + \sum_{\lambda\in\Lambda_z} \frac{e^{-\|\lambda\|^2/2\sigma^2}}{\sigma^2} <\lambda,\mathbf{z}> \\ &\qquad \times (e^{<\lambda,(1-c)\mathbf{z}>/\sigma^2} - e^{-<\lambda,(1-c)\mathbf{z}>/\sigma^2}) \\ &\stackrel{(a)}{\ge} r(0) = \Theta_\Lambda(1/2\pi\sigma^2)\,, \end{aligned}$$

where (a) follows from the fact that each summand in the last sum is positive. ∎

The following Lemma provides an upper bound on $r_{\Lambda,\sigma^2}(\mathbf{z})$.

Lemma 7. *For any lattice Λ and noise variance σ^2, $r_{\Lambda,\sigma^2}(\mathbf{z})$ attains its maximum at the vertices of Voroni region.*

Proof: First, we show that $r(\mathbf{z})$ attains its maximum at the boundaries of $\mathcal{V}(\Lambda)$. We consider a given ray going out from the origin and we choose two points $\mathbf{z}_1$ and $\mathbf{z}_2$ in this ray. We denote the polar ordinates of $\mathbf{z}_1$ and $\mathbf{z}_2$ by $\mathbf{z}_1=(r_1,\theta_1,\cdots,\theta_n)$ and $\mathbf{z}_2=(r_2,\theta_1,\cdots,\theta_n)$, respectively. It can be easily shown that if $r_1\ge r_2$, then we have $r(\mathbf{z}_1)\ge r(\mathbf{z}_2)$. Therefore, if we move from the origin, $r_{\Lambda,\sigma^2}(\mathbf{z})$ increases and therefore, $r(\mathbf{z})$ attains its maximum at the boundaries of $\mathcal{V}(\Lambda)$. Now assume that $r(\mathbf{z})$ attains its maximum at the facet $\mathcal{V}_{\lambda^*}$ (the facet $\mathcal{V}_{\lambda^*}=\{\mathbf{z}:\|\mathbf{z}\|^2=\|\mathbf{z}-\lambda^*\|^2\}$). The value of $r(\mathbf{z})$ over this facet is

$$r(\mathbf{z}) = 2 + e^{\frac{-\|\lambda^*\|^2}{\sigma^2}} + \sum_{\lambda\setminus\{\pm\lambda^*\}} e^{-\frac{\|\lambda\|^2}{2\sigma^2}} e^{-\frac{<\mathbf{z},\lambda>}{2\sigma^2}}\,.$$

The above argument can be repeated for infinite constellation $\Lambda\setminus\{\pm\lambda^*\}$ and its associated ratio function. ∎

Now, we prove our proposed upper bound on $D_{\text{KL}}(f(\mathbf{z}),g(\mathbf{z}))$.

Lemma 8. *For any given Λ and σ^2, we have*

$$D_{KL}(f(\mathbf{z}),g(\mathbf{z})) \le (1+ln(r_M))P_e(\Lambda,\sigma^2)\,, \tag{21}$$

where r_M is given in Lemma 7.

Proof of Lemma 8: Recall that $r(\mathbf{z})=f(\mathbf{z})/g(\mathbf{z})$. Let's define $h(t)\stackrel{\text{def}}{=} t\ln(t)$. Thus

$$\begin{aligned} D_{\text{KL}}(f(\mathbf{z})\, g(\mathbf{z})) &= \int_{\mathcal{V}} g(\mathbf{z}) r(\mathbf{z}) \ln(r(\mathbf{z}))\, \mathrm{d}\mathbf{z} \\ &= \int_{\mathcal{V}} g(\mathbf{z}) h(r(\mathbf{z}))\, \mathrm{d}\mathbf{z}\,. \end{aligned}$$

Since $h(t)$ is a Lipschitzian continuous function on the interval $[r(0),r_M]$, i.e. the range of $r(\mathbf{z})$, we have

$$\begin{aligned} |h(r(\mathbf{z}))-h(1)| &\le |r(\mathbf{z})-1| \max_{r(\mathbf{z})\in[r(0),r_M]} (1+\ln(r(\mathbf{z})) \\ &= (1+\ln(r_M))|r(\mathbf{z})-1|\,, \end{aligned}$$

where the last equality follows from the fact that $r(0)>1$. So we have

$$\begin{aligned} D_{\text{KL}}(f(\mathbf{z}),g(\mathbf{z})) &\le (1+\ln(r_M)) \int_{\mathcal{V}} |f(\mathbf{z})/g(\mathbf{z})-1| \mathrm{d}\mathbf{z} \\ &= (1+\ln(r_M)) P_e(\Lambda,\sigma^2)\,. \end{aligned}$$

∎

Combination of lemmas 3 and 8 completes the proof.

C. Proof of Theorem 4

Our proposed bounds are obtained by bounding the following integration

$$I(\mathcal{V}(\Lambda),\sigma^2) = \frac{1}{2\sigma^2}\int_{\mathcal{V}(\Lambda)} \mathbf{z}^2 g(\mathbf{z})\, \mathrm{d}\mathbf{z}\,.$$

In the following lemma, we show that $S(n,r,\sigma^2)=I(\mathcal{S}(n,r),\sigma^2)$ where $S(n,r,\sigma^2)$ is defined in III.

Lemma 9. *For any $r\ge 0$, σ^2 and any integer n, we have $I(\mathcal{S}(n,r),\sigma^2)=S(n,r,\sigma^2)$.*

Proof of Lemma 9: Similar to [7], coordinate transformation from Cartesian coordinates to spherical coordinates yields

$$S(n,r,\sigma^2) = \frac{nV(n,1)}{2^{n/2+1}\pi^{n/2}} \int_0^{r/\sigma} u^{n+1} e^{-u^2/2}\, \mathrm{d}u\,,$$

where $V(n,1)$ is the volume of n-dimensional sphere of radius 1, given by

$$V(n,1) = \frac{\pi^{n/2}}{\Gamma(n/2+1)}\,.$$

The integration by parts provides the following recursive formula

$$S(n,r,\sigma^2) = \frac{n}{n-2} S(n-2,r,\sigma^2) - \frac{nV(n,1)}{2\pi^{n/2}} e^{-y} y^{\frac{n}{2}}\,. \tag{22}$$

For the special cases $n = 1$ and $n = 2$, we have

$$S(1, r, \sigma^2) = \frac{1}{2}(1 - \text{erfc}(y^{1/2}) - 2\sqrt{\frac{y}{\pi}}e^{-y})$$
$$S(2, r, \sigma^2) = 1 - (1 + y)e^{-y}\,, \tag{23}$$

where erfc(y) $\stackrel{\text{def}}{=} \frac{2}{\sqrt{\pi}} \int_0 ye^{-t^2}\,\mathrm{d}t$. Combination of eqs. (22) and (23) completes the proof. ■

Now we are ready to prove our proposed lower bound on $D_{\text{var}}(f(\mathbf{z}), g(\mathbf{z}))$. For any $\mathbf{z} \in \mathcal{V}(\Lambda)$, we have $f(\mathbf{z}) \geq g(\mathbf{z})$. Thus

$$\begin{aligned} &D_{\text{var}}(f(\mathbf{z}), g(\mathbf{z})) \\ &\geq \frac{1}{2\sigma^2}\Big(\int_{\mathcal{V}} \|\mathbf{z}\|^2 g(\mathbf{z})\,\mathrm{d}\mathbf{z} + \int_{\mathcal{V}\setminus\mathcal{S}(n,r_p)} \|\mathbf{z}\|^2 g(\mathbf{z})\mathrm{d}\mathbf{z}\Big) - \frac{n}{2} \\ &\stackrel{(a)}{\geq} y_p \times \Big(P_e(\Lambda, \sigma^2) - P_e(\mathcal{S}(n, r_p), \sigma^2)\Big) \\ &\qquad\qquad + S(n, r_p, \sigma^2) - \frac{n}{2}\,. \end{aligned}$$

where (a) follows from the fact that $\|\mathbf{z}\|^2 g(\mathbf{z})$ is a positive function and $\mathcal{S}(n, r_p) \subseteq \mathcal{V}(\Lambda)$.

Now we turn to our proposed upper bound in Theorem 4. We have

$$\begin{aligned} &D_{\text{var}}(f(\mathbf{z}), g(\mathbf{z})) \\ &\quad= \frac{1}{2\sigma^2}\Big(\int_{\mathcal{V}} \|\mathbf{z}\|^2 f(\mathbf{z})\,\mathrm{d}\mathbf{z} - \frac{1}{2\sigma^2}\int_{\mathbb{R}^n} \|\mathbf{z}\|^2 g(\mathbf{z})\,\mathrm{d}\mathbf{z}\Big) \\ &\quad= \frac{1}{2\sigma^2}\sum_{\lambda}\int_{\mathcal{V}} (\|\mathbf{z}\|^2 - \|\mathbf{z}+\lambda\|^2) g(\mathbf{z}+\lambda)\,\mathrm{d}\mathbf{z}\,, \end{aligned}$$

and since for any $\mathbf{z} \in \mathcal{V}(\Lambda)$ and any $\lambda \in \Lambda\backslash\{0\}$ we have $\|\mathbf{z}\|^2 \leq \|\mathbf{z}+\lambda\|^2$, the value of above integral is negative.

V. Conclusion

In this paper, the capacity of the modulo lattice channel in two different VNR regimes is investigated. In small VNR, the capacity is bounded in terms of the flatness factor and we can establish that as $\sigma^2 \to \infty$, the capacity is equal to $O(\epsilon(\Lambda, 2\sigma^2))$. In large VNR regime, we provide bounds on two distances (the KL distance and the variance distance) between Λ-aliased Gaussian noise and WGN. Our bounds suggest that the KL distance and the variance distance decline at a rate at least as $O(P_e(\Lambda, \sigma^2))$ and $O(\frac{1}{\sigma^n}e^{-r_p^2(\Lambda)/2\sigma^2})$, respectively and hence, we can conclude that as $\sigma^2 \to 0$, the decline rate of $C(\Lambda, \sigma^2) - \frac{n}{2}\log\alpha(\Lambda, \sigma^2)$ is at least $O(\frac{1}{\sigma^n}e^{-r_p^2(\Lambda)/2\sigma^2})$. Our future work would be investigating the statistical distances between the Λ-aliased Gaussian, the white Gaussian and the uniform distributions at finite values of VNR in high dimensional lattices.

Acknowledgment

We would like to thank C. Ling for interesting and fruitful discussions.

References

[1] R. De Buda. Some optimal codes have structure. *Selected Areas in Communications, IEEE Journal on*, 7(6):893–899, 1989.

[2] U. Erez and R. Zamir. Achieving 1/2 log (1+snr) on the awgn channel with lattice encoding and decoding. *Information Theory, IEEE Transactions on*, 50(10):2293–2314, 2004.

[3] Jr. Forney, G.D., M.D. Trott, and S. Y. Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *Information Theory, IEEE Transactions on*, 46(3):820 –850, may 2000.

[4] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé. Semantically secure lattice codes for the gaussian wiretap channel. *CoRR*, abs/1210.6673, 2012.

[5] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, April 2007.

[6] G. Poltyrev. On coding without restrictions for the awgn channel. *Information Theory, IEEE Transactions on*, 40(2):409–417, 1994.

[7] V. Tarokh, A. Vardy, and K. Zeger. Universal bound on the performance of lattice codes. *Information Theory, IEEE Transactions on*, 45(2):670–681, 1999.

[8] F. Topsoe. Some inequalities for information divergence and related measures of discrimination. *Information Theory, IEEE Transactions on*, 46(4):1602–1609, 2000.

[9] R. Zamir, S. Shamai, and U. Erez. Nested linear/lattice codes for structured multiterminal binning. *Information Theory, IEEE Transactions on*, 48(6):1250–1276, 2002.