

Hexagonal Quantizers are not Optimal for 2-D Data Hiding

Félix Balado and Fernando Pérez-González

University of Vigo

Signal Theory and Communications Department

Lagoas-Marcosende s/n, E-36200 Vigo, Spain

ABSTRACT

Data hiding using quantization has revealed as an effective way of taking into account side information at the encoder. When quantizing more than one host signal samples there are two choices: 1) using the Cartesian product of several one-dimensional quantizers, as made in Scalar Costa Scheme (SCS); or 2) performing vectorial quantization. The second option seems better, as rate-distortion theory affirms that higher dimensional quantizers yield improved performance due to better sphere-packing properties. Although the embedding problem does resemble that of rate-distortion, no attacks or host signal characteristics are usually considered when designing the quantizer in this way. We show that attacks worsen the performance of the a priori optimal lattice quantizer through a counterexample: the comparison under Gaussian distortion of hexagonal lattice quantization against bidimensional Distortion-Compensated Quantized Projection (DC-QP), a data hiding alternative based in quantizing a linear projection of the host signal. Apart from empirical comparisons, theoretical lower bounds on the probability of decoding error of hexagonal lattices under Gaussian host signal and attack are provided and compared to the already analyzed DC-QP method.

Keywords: Data Hiding, Hexagonal Lattice Coding, Projection Quantization, Quantization Index Modulation

1. INTRODUCTION

Quantization lattices are appealing for data hiding applications, for it has been shown¹ that they open one way to approach with reduced complexity the capacity-achieving random codebook for channel coding with side information. There is an inherent compromise in the use of lattices for data hiding: on the one hand, lattice centroids must be packed together as close as possible to keep a certain distortion measure low, maximizing simultaneously the amount of information embedded. On the other hand, they must be placed as far away from each other as possible in order to minimize, under the same distortion restriction, the probability of decoding error caused by further distortions or attacks on the quantized host signal.

The first difficulty can be tackled along source code design guidelines, whose limits are given by rate-distortion theory, while the second one is in fact a channel coding issue with side information at the encoder. The joint consideration of both questions is the key to optimally address the building of practical methods for the data hiding problem, suggesting that, to this end, codes more generic than those lattice-based might be required. Rate-distortion theory chooses, for a given embedding rate, to minimize the distortion caused by modifying the host signal. Lattices are suitable for this kind of design; however, this approach alone might no longer be optimal if additional constraints such as the probability of decoding error are simultaneously imposed to the problem.

The purpose of this paper is to show, by providing a real counterexample, that the optimal bidimensional scheme constructed under the criterion of first designing a lattice source code and afterwards partitioning it into channel codes,² does not perform better than alternative methods such as those based on the quantization of projective transforms. We will be only considering dithered modulation,³ i.e. the quantization centroids for a given symbol will be shifted versions of those of any other symbol in the ensemble used for embedding. The idea of dithered modulation is formally equivalent to that of nested codes (cosets), proposed as a structured implementation of the optimal solution for the Wyner-Ziv problem (dual of channel coding with side information). Additionally, this setting usually leads to tractable analyses.

Further author information:

F. Balado: fiz@tsc.uvigo.es; F.Pérez-González: fperez@tsc.uvigo.es

Finally, no further coding layers are considered in this comparison. It has been demonstrated that the use of coding significantly improves the performance of practical schemes. For instance, iterative decoding⁴ has been used to improve the performance of codes built similarly to² by means of the cubic lattice.

2. TWO-DIMENSIONAL INFORMED DATA HIDING

In this section we present the algorithms that will be used for the comparison, and whose performance will be analyzed in Section 3 and discussed in Section 4. We denote in bold face bidimensional vectors, i.e. $\mathbf{v} = (v[1], v[2])$.

In both methods an additive watermark \mathbf{w} is generated from the host signal \mathbf{x} depending on the information to be embedded, obtaining the watermarked signal as $\mathbf{y} = \mathbf{x} + \mathbf{w}$. The host signal \mathbf{x} is assumed to be Gaussian-distributed with covariance matrix $\Gamma_{\mathbf{x}} = \sigma_x^2 \mathbf{I}$. Finally, detection is made using a noisy version of \mathbf{y} , i.e. $\mathbf{z} = \mathbf{y} + \mathbf{n}$, being \mathbf{n} a zero-mean Gaussian source, with covariance matrix $\Gamma_{\mathbf{n}} = \sigma^2 \mathbf{I}$ and independent of \mathbf{x} .

2.1. Hexagonal Lattice Coding

A certain distortion measurement has to be selected in order to determine an optimal lattice from the rate-distortion point of view. The problems of selecting proper distortion measures are well known in several research areas including data hiding, due to the practical difficulty of finding a measure both tractable and meaningful for the problem in question. Partly because of this, most data hiding approaches have resorted to using the mean-square error (MSE) distortion measurement, even though it has been argued⁵ that it might be not suitable for data hiding purposes.

In this section we will attend to the MSE criterion and disregard more restrictive distortion measurements. It is known that, when using this kind of distortion restriction, the optimal lattices in one and two dimensions are given by the uniform and the hexagonal quantizers respectively,⁶ as long as the quantization error can be taken to be uniform. Moreover, under the latter assumption the hexagonal lattice is also optimal for all norms $\|\cdot\|_r$ with r ranging from 1 to ∞ (MSE is equivalent to $\|\cdot\|_2$). As an example of the influence of the distortion criterion, see that, if for instance pointwise energy restrictions⁵ were used, the optimality of the unidimensional uniform lattice would imply the optimality of the n -dimensional cubic or integer lattice, which is known to be worse performing than the hexagonal one for $n = 2$ (square lattice).

After having justified the use of the hexagonal lattice as a source code we need to define the channel code to be employed. The simplest setting using dithered modulation is a 3-ary scheme like the one depicted in Figure 1. For instance, the use of a simpler binary scheme would imply either that the symbol quantizers were not congruent with each other by means of shifting or that they were not hexagonal for each symbol. Apart from this fact, the hexagonal lattice happens to be the optimal lattice channel code with i.i.d. Gaussian noise with any value of σ under a given distortion constraint.⁷

The ternary alphabet for the hexagonal lattice was also used by Brunk,⁸ who extended the unidimensional DC-QIM approach to higher dimensions using regular dithered quantizers; the hexagonal lattice was chosen in⁸ due to presenting the optimal space-filling polytope. Also, higher alphabet sizes are possible for the hex lattice. For instance, Eggers et al.¹ used 9-ary signalling with distortion compensation in the so-called Hexagonal Costa Scheme (HCS). No details are given about the spatial arrangement used for the symbols, and so we assume that it refers to the extension of the 3-ary scheme depicted in Fig. 1 obtained by subdividing each hexagonal symbol sublattice into three further hexagonal cosets using the same pattern shown. This procedure renders the only 9-ary scheme presenting congruent hexagonal sublattices.

Encoder and decoder structure. We describe next the encoding and decoding stages for the 3-ary method. Each information symbol $b \in \{0, 1, 2\}$ is hidden by using a corresponding bidimensional quantizer $\mathbf{Q}_b(\cdot)$ on the host signal, obtaining the watermark as

$$\mathbf{w} = \mathbf{v} \mathbf{e}, \tag{1}$$

i.e. the bidimensional quantization error $\mathbf{e} \triangleq \mathbf{Q}_b(\mathbf{x}) - \mathbf{x}$ weighted by an optimizable constant ν , $0 < \nu \leq 1$. Using (1) we can put \mathbf{y} as

$$\mathbf{y} = \mathbf{Q}_b(\mathbf{x}) - (1 - \nu)\mathbf{e}. \quad (2)$$

It has to be remarked that the use of the compensation factor ν changes somewhat our discussion above on the optimal lattice when $\nu < 1$. This case has not been studied and needs further research. Nevertheless, observe that the use of distortion compensation *always* diminishes the error rate with respect to the case $\nu = 1$, thus supporting somehow our discussion above on the optimal lattice selection.

Let us define next the symbol quantizers. First, consider the auxiliary rectangular lattice $\Omega = (3\mathbb{Z}, \sqrt{3}\mathbb{Z})\Delta$, that we use to define the basic hexagonal lattice as

$$\Lambda_H = \Omega \cup \left\{ \Omega + (3, \sqrt{3})\Delta/2 \right\}. \quad (3)$$

With (3) we can define the lattices that specify the centroids of the quantizers $\mathbf{Q}_0(\cdot)$, $\mathbf{Q}_1(\cdot)$ and $\mathbf{Q}_2(\cdot)$ as

$$\Lambda_0 = \Lambda_H + \mathbf{d}, \quad (4)$$

$$\Lambda_1 = \Lambda_H + \mathbf{d} + (\Delta, 0), \quad (5)$$

$$\Lambda_2 = \Lambda_H + \mathbf{d} + \frac{1}{2}(\Delta, \sqrt{3}\Delta). \quad (6)$$

The (possibly key-dependant) constant vector \mathbf{d} can be assumed to be $\mathbf{0}$ without loss of generality for analysis purposes. Last, decoding is made through a minimum Euclidean distance detector:

$$\hat{b} = \arg \min_{b \in \{0,1,2\}} \|\mathbf{z} - \mathbf{Q}_b(\mathbf{z})\|. \quad (7)$$

For HCS the encoding and decoding procedures are analogous but using the nine corresponding quantizers/symbols.

2.2. Distortion-Compensated Quantized Projection (DC-QP)

We will summarize in this section the basics of the DC-QP method,⁵ adapting the exposition to the bidimensional case with Gaussian host signal. We recall that in the basic Quantized Projection (QP) case, the method starts by quantizing a linear projection function such as

$$r_x \triangleq \sum_{k=1,2} \frac{x[k]s[k]}{\alpha[k]}, \quad (8)$$

where \mathbf{s} is a zero-mean, unit-variance pseudorandom sequence and α a perceptual mask computed from \mathbf{x} indicating the maximum allowed energy that produces the least noticeable modification for each host signal sample $x[k]$. Notice that this is a pointwise distortion criterion, more restrictive than the MSE one allowed for choosing the optimal hexagonal lattice.

As discussed in⁵ the projection function (8) can be generalized to obtain performance improvements. For projections involving a large number of dimensions r_x can be assumed to be Gaussian-distributed thanks to the Central Limit Theorem (CLT). In general, this assumption does not hold when projecting only two dimensions, but the assumption of a Gaussian host signal \mathbf{x} implies that r_x is also Gaussian. Next, r_x is quantized with one out of two unidimensional lattices

$$\Lambda_b = 2\Delta\mathbb{Z} + b\Delta - \Delta/2, \quad b \in \{0, 1\}, \quad (9)$$

depending on the binary symbol b being embedded. The projected watermark is obtained as the projected quantization error scaled by an optimizable constant $0 < \nu \leq 1$ (distortion-compensation), i.e.

$$r_w = \nu(Q_b(r_x) - r_x), \quad (10)$$

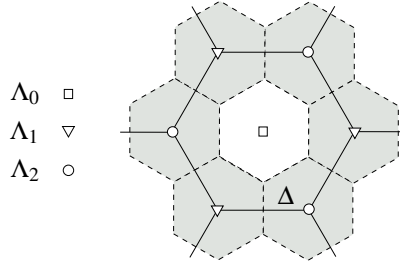


Figure 1. Hexagonal lattice: Voronoi and decision regions (hexagons limited by solid and dashed lines, respectively).

with $Q_b(\cdot)$ a centroid in Λ_b . In order to obtain the unprojected watermark, while at the same time coping with the aforementioned pointwise restriction, the structure $w[k] = \rho \alpha[k] s[k]$ is imposed, what yields $\rho = r_w/2$ with $s[k] \in \{\pm 1\}$ in the bidimensional case.

Detection is carried out by using a minimum distance detector on the projection r_z of received vector \mathbf{z} , i.e.

$$\hat{b} = \arg \min_{b \in \{0,1\}} \|r_z - Q_b(r_z)\|. \quad (11)$$

3. PERFORMANCE ANALYSIS

While in some works⁸¹⁸¹ performance is measured through the achievable rate/capacity using Gaussian channels, as discussed in previous papers by the authors the use of the probability of decoding error is preferred here as the design parameter for measuring the performance of the presented methods.

We assume in the following that $\alpha[1] = \alpha[2] = \alpha$; in this case DC-QP becomes equivalent to Spread Transform Dither Modulation (STDM)³ with distortion compensation (i.e. STSCS¹), but only the performance analysis for DC-QP presented in⁵ is available to our knowledge. Additionally, all symbols are supposed to be equally likely.

While DC-QP makes use of a binary alphabet, a 3-ary symbol constellation is used for the hexagonal lattice. A ternary extension of DC-QP would break the symmetry of the symbols used, thus complicating the analysis. Then, in order to make it possible the performance comparison we will compute for the hexagonal lattice the probability of symbol error (P_e), and afterwards, we will convert P_e to the corresponding bit error probability (P_b).

3.1. Hexagonal Lattice Coding with Distortion-Compensation

We assume that the quantization error \mathbf{e} is independent of \mathbf{x} and uniformly distributed inside a hexagon with edge size Δ that forms the basic Voronoi region (see Figure 1). Assuming without loss of generality that the symbol 0 at the origin is sent, then $\mathbf{z} = \mathbf{v} + \mathbf{n}$ with $\mathbf{v} \triangleq -(1 - \nu)\mathbf{e}$. Therefore, it becomes clear from a glance at Figure 1 that P_e is lower bounded by the probability that \mathbf{z} falls inside the area formed by the union of the six shaded decision hexagons corresponding to the six nearest centroids neighboring the symbol sent. Calling \mathcal{R}_c to the decision region associated to a given centroid \mathbf{c} we can write the lower bound region as

$$\mathcal{R}_l = \{\cup_{\mathbf{c}} \mathcal{R}_c \mid \mathbf{c} \in \{\Lambda_1 \cup \Lambda_2\}, \|\mathbf{c}\| = \Delta\}. \quad (12)$$

Notice that \mathcal{R}_l could be enlarged using further decision regions to get a tighter lower bound, but for the sake of simplicity we prefer to follow this approach while obtaining a usable bound. Now, the lower bound can be put as

$$P_e > P_l \triangleq P\{\mathbf{z} \in \mathcal{R}_l\} = \int_{\mathcal{R}_l} f_{\mathbf{z}}(\mathbf{z}) d\mathbf{z}, \quad (13)$$

with $f_{\mathbf{z}}(\mathbf{z}) = f_{\mathbf{v}}(\mathbf{z}) * f_{\mathbf{n}}(\mathbf{z})$, that is, the bidimensional convolution of the probability distribution functions (pdf's) of \mathbf{v} and \mathbf{n} . In the case that the WNR (see Section 4) is not too low this lower bound is a reasonable approximation to the actual

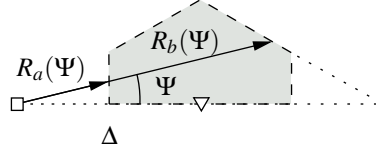


Figure 2. Symmetric area.

probability of error, as the probability of \mathbf{z} falling inside a correct decision region other than the corresponding to the centroid sent becomes negligible.

Taking advantage of the symmetry of the problem we only need to consider the shaded area in Figure 2, and therefore, in a similar way to⁹, we can write (13) in polar coordinates as

$$P_l = 12 \int_0^{\pi/6} \int_{R_a(\Psi)}^{R_b(\Psi)} r f_{\mathbf{z}}(r, \Psi) dr d\Psi, \quad (14)$$

with $R_a(\Psi)$ and $R_b(\Psi)$ the distances at the angle Ψ from the origin to the inner and to the outer border of \mathcal{R}_l , respectively (see Fig. 2). Therefore these distances are

$$R_a(\Psi) = \frac{\Delta}{\sqrt{3}} \frac{\cos(\pi/6)}{\cos \Psi} = \frac{\Delta}{2 \cos \Psi}, \quad (15)$$

$$R_b(\Psi) = \frac{2\Delta}{\sqrt{3}} \frac{\sin(2\pi/3)}{\sin(\pi/6 + \Psi)} = \frac{\Delta}{\sin(\pi/6 + \Psi)}. \quad (16)$$

Notice that, for simplicity, we have let $R_b(\Psi)$ traverse the outer border of \mathcal{R}_l for $0 \leq \Psi < \arctan(\sqrt{3}/3)$; in fact, using this definition of $R_b(\Psi)$ we obtain a tighter lower bound than that defined by (12) because the extra subtended area (the triangle on the right in Fig. 2) still is an error region. Unfortunately, $f_{\mathbf{z}}(r, \Psi)$ has no circular symmetry and so the computation of (14) using (15–16) remains involved, what recommends pursuing a lower bound to P_l . The way to compute this bound in practice is detailed in Appendix A.

Last, observe that the performance analysis done applies exactly the same to the 9-ary scheme HCS, with the sole difference that the Voronoi regions undergo a rotation of $\pi/6$ degrees and a scaling, and, consequently, the quantization error \mathbf{e} has to be taken as uniformly distributed over a rotated hexagon with edge size $\sqrt{3}\Delta$ instead of Δ . The latter value is the only parameter that changes with respect to the 3-ary bound: the decision regions remain the same and the rotation of the Voronoi region is unimportant when following the approach of Appendix A. To conclude, it has to be remarked that the error region \mathcal{R}_l could be further extended in the HCS case to get a tighter lower bound.

Conversion from symbol errors to bit errors. In order to convert P_e to the corresponding bit error rate P_b we use the fact that $2^{11} \approx 3^7$. Let us call N_w to the number of length seven 3-ary codewords at Hamming distance w from the all-zero codeword. For such codewords, let $P_e(w) = w/7$ be the rate of symbols different from zero, and $P_b(w)$ the rate of bits different from zero for all the binary representations with length 11 corresponding to ternary codewords with weight w . Then, the approximate factor of proportionality between symbol errors and bit errors, i.e. $P_b \approx KP_e$, is given by

$$K = \sum_{w=1}^7 \frac{P_b(w)}{P_e(w)} \frac{N_w}{3^7 - 1}, \quad (17)$$

assuming all symbols are equally likely. As in fact $2^{11} < 3^7$ not all the codewords are representable with 11 bits alone, and so we are in fact lower bounding the “true” P_b when considering this binary codeword length. For HCS the same approximation can be done using $2^3 \approx 9^1$.

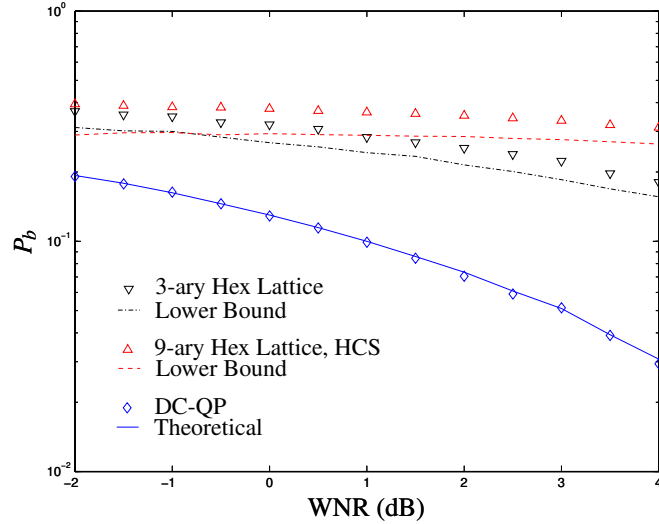


Figure 3. Hexagonal Lattice with DC vs DC-QP, with optimization of ν at each WNR

3.2. DC-QP

The performance analysis of DC-QP was discussed in detail in previous works,⁵ where it was shown that its probability of bit error is approximated (upper bounded) by

$$P_b \approx \sum_{i=-\infty}^{\infty} \frac{\Delta}{\sqrt{2\pi}\sigma_{r_x}} \int_{-1/2}^{3/2} \exp(-\Delta^2(r+2i)^2/2\sigma_{r_x}^2) \cdot \left\{ Q\left(\frac{(1-(1-\nu)(2r-1))}{2\sigma_{r_n}} \Delta\right) + Q\left(\frac{(1+(1-\nu)(2r-1))}{2\sigma_{r_n}} \Delta\right) \right\} dr, \quad (18)$$

with $\sigma_{r_n}^2 = 2\sigma^2/\alpha^2$ and $\sigma_{r_x}^2 = 2\sigma_x^2/\alpha^2$ the variances of the projected noise and host signal, both Gaussian-distributed, and $Q(\cdot)$ the normalized cumulative normal distribution function.

4. COMPARISON OF THE METHODS

In order to perform the comparison at different distortion values we define the watermark-to-noise ratio as $\text{WNR} = 10\log_{10} D_w/D_c$, with D_w and $D_c = \sigma^2$ the watermark energy and channel distortion, respectively. For the hexagonal lattice with distortion compensation we have that⁷

$$D_w = \int_{H_w} \|\mathbf{w}\|^2 f_w(\mathbf{w}) d\mathbf{w} = 6 S_w^{1/3} G(H), \quad (19)$$

with S_w the area of the hexagon H_w with edge size $\nu\Delta$ over which the mark is uniformly distributed, i.e. $f_w(\mathbf{w}) = 1/S_w$ for $\mathbf{w} \in H_w$ (see Sections 2.1 and 3.1), and $G(H) = (\csc(2\pi/6) + \cot(\pi/6))/36$ the dimensionless second moment of a hexagonal polygon. The exact computation of D_w for DC-QP was discussed in,⁵ and can be put as $D_w = \nu^2\tau^2\Delta^2\alpha^2/4$, with τ a certain function bounded as $\sqrt{3} \leq \tau \leq \sqrt{4}$. Also, we define the document-to-watermark ratio as $\text{DWR} = 10\log_{10} D_x/D_w$; this parameter is only relevant for DC-QP, as long as the uniformity assumption on the hexagonal cells holds.

First, in Figure 3 we plot the P_b of the hexagonal lattice with distortion compensation for the 3-ary and 9-ary (HCS) schemes versus that of DC-QP. Numerical minimization of the probability of error on the tunable ν parameter has been performed at each value of the WNR for all three methods; for this reason the DWR varies between 28 and 26 dB along the plotted WNR range for DC-QP. We observe that in this case the performance of the latter method is quite better, recalling that the embedding distortion used for DC-QP is more restrictive. Notice also that the 9-ary method does worse than the

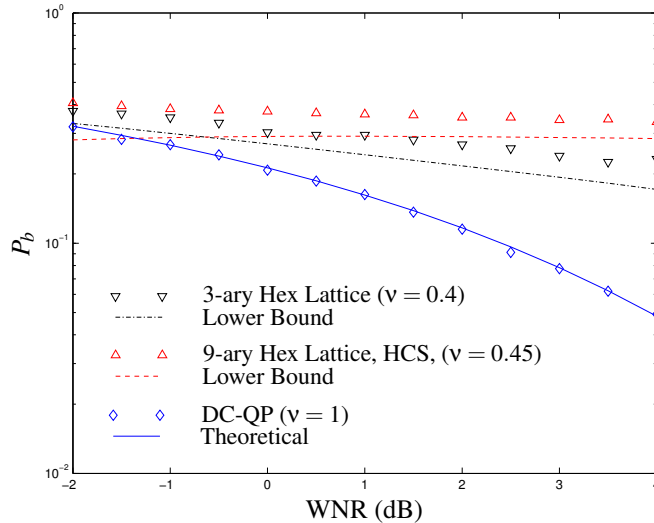


Figure 4. Hexagonal Lattice with DC optimized at WNR = 0 dB vs QP (DWR = 25 dB)

3-ary one. This behavior is logical, because the use of a higher-dimensional constellation for the same allowed embedding distortion will pack the symbols closer, increasing the probability of error. This fact does not contradict the achievable rate analysis done in,¹ as the use of sufficiently powerful coding on top of the 9-ary scheme will eventually approach the predicted performance if WNR values are not too low. Last, for the reasons hinted in Section 3.1 the lower bound is looser for the 9-ary case.

Of course, the case presented in Fig. 3 is ideal because in order to optimize v we need to know *beforehand* the attacking noise power level —i.e. the value of the WNR—, and this is unfeasible most times in practice. Other approaches such as SCS/DC-QIM are also bound to exhibit this weakness for the reason pointed out. In a more realistic scenario we have to content ourselves with undertaking optimization for a given value of the WNR, or alternatively, with no optimization at all, i.e. using $v = 1$. Arguably, if no a priori knowledge of the attacking distortion is available one could for example perform optimization at WNR = 0 dB, which is equivalent to assume that $D_c = D_w$. To illustrate the previous discussion we present in Figure 4 a real case in which the hexagonal methods are optimized at WNR = 0 dB and DC-QP is not optimized, being in fact just QP. Notice that, even in this unfavorable case, DC-QP performs better for the WNR range presented.

As for complexity issues, it is only slightly more involved to implement the hexagonal lattice methods than scalar quantization of a linear projection. This is so because the decomposition (3) into two rectangular lattices makes coding and decoding complexity minimal, as any bidimensional vector can be first easily quantized to each rectangular lattice to select afterwards the nearer centroid resulting from both quantizations.

5. CONCLUSIONS

We have seen throughout this paper that, at least in the two-dimensional case, the use of the optimal quantization lattice does not seem to be the best way to implement an approximation to the optimal random codebook for channel coding with side information. The presented results appear to be even more conclusive if we consider that a more restrictive distortion criterion has been imposed on the alternative method, DC-QP, and are also backed by the fact that its non-optimized version, QP, also performs better than the hex lattice. A likely explanation for this behavior lies in the inability of lattice codes to exploit the host signal features, whereas the projection transformation does improve its performance depending on them.⁵

This result also suggests that the use of the optimal lattices in higher dimensions together with dither modulation might not constitute optimal codebooks either, although further research on this topic is needed. Evidently, this comparison does not tell us that we cannot improve lattice codes through the use of coding, as it was made in,⁴ but coding can also improve

DC-QP performance. Last, the decoding complexity of optimal n -dimensional lattices should not be overlooked.⁷

ACKNOWLEDGMENTS

Work partially supported by the *Xunta de Galicia* under projects PGIDT01 PX132204PM and PGIDT02 PXIC32205PN, and the CYCIT project AMULET, reference TIC2001-3697-C03-01.

APPENDIX A. LOWER BOUND FOR HEXAGONAL LATTICES

First, let us call H_v to the Voronoi region centered at the origin and scaled by $(1-v)$, i.e. the hexagon over which \mathbf{v} is uniformly distributed. The area of H_v is just $S_v = 3/2 \sqrt{3} R_c^2$, with $R_c = (1-v)\Delta$ its circumradius or edge size. Using these data and the inradius $R_i = \frac{\sqrt{3}}{2} R_c$, we construct the function

$$g_v(r, \Psi) \triangleq \begin{cases} \frac{1}{S_v}, & 0 \leq r \leq R_i \\ 0, & r > R_i \end{cases}. \quad (20)$$

Observe that function (20) is no longer a pdf as it integrates to less than 1, but its circular symmetry facilitates the calculation of the bound on P_e . This is so because, from definition (20), it follows that

$$g_v(r, \Psi) \leq f_v(r, \Psi), \quad 0 \leq r < \infty, 0 \leq \Psi < 2\pi, \quad (21)$$

and therefore we have that

$$g_z(\mathbf{z}) \triangleq g_v(\mathbf{z}) * f_n(\mathbf{z}) \leq f_v(\mathbf{z}) * f_n(\mathbf{z}) = f_z(\mathbf{z}). \quad (22)$$

Using (14) and (22) we can lower bound P_l as follows

$$P_l \geq \underline{P}_l = 12 \int_0^{\frac{\pi}{6}} \int_{R_a(\Psi)}^{R_b(\Psi)} r g_z(r, \Psi) dr d\Psi = 12 \int_0^{\frac{\pi}{6}} \left\{ \int_{R_a(\Psi)}^{\infty} r g_z(r, \Psi) dr - \int_{R_b(\Psi)}^{\infty} r g_z(r, \Psi) dr \right\} d\Psi. \quad (23)$$

Next, we will calculate $g_z(\mathbf{z})$. Due the aforementioned symmetry it is enough to compute the left-hand side convolution in (22) for a fixed angle, for instance at those points $\mathbf{z} = (z_1, 0)$ with $z_1 \geq 0$ for which $(r, \Psi) = (z_1, 0)$. In this way we get

$$\begin{aligned} g_z(z_1, 0) &= \frac{1}{2\pi\sigma^2} \iint_{C_i} \exp\left(-\frac{(x-z_1)^2 + y^2}{2\sigma^2}\right) g_v(x, y) dx dy \\ &= \frac{1}{2\pi\sigma^2} \exp\left(-\frac{z_1^2}{2\sigma^2}\right) \iint_{C_i} \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right) \exp\left(\frac{xz_1}{\sigma^2}\right) g_v(x, y) dx dy, \end{aligned} \quad (24)$$

with C_i the circle inscribed in H_v . By transforming (x, y) to polar coordinates (ρ, θ) , we can write

$$\begin{aligned} g_z(z_1, 0) &= \frac{1}{2\pi\sigma^2} \exp\left(-\frac{z_1^2}{2\sigma^2}\right) \int_0^{R_i} \int_0^{2\pi} \rho \exp\left(-\frac{\rho^2}{2\sigma^2}\right) \exp\left(\frac{z_1\rho \cos\theta}{\sigma^2}\right) g_v(\rho, \theta) d\theta d\rho \\ &= \frac{1}{2\pi\sigma^2 S_v} \exp\left(-\frac{z_1^2}{2\sigma^2}\right) \int_0^{R_i} \int_0^{2\pi} \rho \exp\left(-\frac{\rho^2}{2\sigma^2}\right) \exp\left(\frac{z_1\rho \cos\theta}{\sigma^2}\right) d\theta d\rho. \end{aligned} \quad (25)$$

In order to compute the bound (23) we need to solve the integral

$$\begin{aligned} I(R) &\triangleq \int_R^{\infty} r g_z(r, \Psi) dr = \int_R^{\infty} r g_z(r, 0) dr \\ &= \int_R^{\infty} r \left\{ \frac{1}{2\pi\sigma^2 S_v} \exp\left(-\frac{r^2}{2\sigma^2}\right) \int_0^{R_i} \int_0^{2\pi} \rho \exp\left(-\frac{\rho^2}{2\sigma^2}\right) \exp\left(\frac{r\rho \cos\theta}{\sigma^2}\right) d\theta d\rho \right\} dr \\ &= \frac{1}{\sigma^2 S_v} \int_0^{R_i} \rho \int_R^{\infty} r \exp\left(-\frac{r^2 + \rho^2}{2\sigma^2}\right) I_0\left(\frac{r\rho}{\sigma^2}\right) dr d\rho \\ &= \frac{1}{S_v} \int_0^{R_i} \rho Q_1\left(\frac{\rho}{\sigma}, \frac{R}{\sigma}\right) d\rho, \end{aligned} \quad (26)$$

where $Q_1(\cdot, \cdot)$ is the first-order Marcum's Q-function.¹⁰ This function admits the following expansion in exponential series¹⁰:

$$Q_1(\alpha, \beta) = \sum_{n=0}^{\infty} \exp(-\alpha^2/2) \frac{(\alpha^2/2)^n}{n!} \cdot \sum_{k=0}^n \exp(-\beta^2/2) \frac{(\beta^2/2)^k}{k!}. \quad (27)$$

Using this expression in Eq. (26) we can write

$$\begin{aligned} I(R) &= \frac{1}{S_v} \sum_{n=0}^{\infty} \left\{ \int_0^{R_i} \exp\left(-\frac{\rho^2}{2\sigma^2}\right) \frac{\rho^{2n+1}}{n!(2\sigma^2)^n} d\rho \right\} \cdot \sum_{k=0}^n \exp\left(-\frac{R^2}{2\sigma^2}\right) \frac{R^{2k}}{k!(2\sigma^2)^k} \\ &= \frac{\sigma^2}{S_v} \sum_{n=0}^{\infty} \left\{ 1 - \frac{\Gamma(n+1, \frac{R_i^2}{2\sigma^2})}{\Gamma(n+1)} \right\} \cdot \sum_{k=0}^n \exp\left(-\frac{R^2}{2\sigma^2}\right) \frac{R^{2k}}{k!(2\sigma^2)^k}, \end{aligned} \quad (28)$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot, \cdot)$ are the Gamma and the incomplete Gamma functions, respectively. Notice that in practice it is necessary to truncate the series in (28) to a sufficiently high value to retain the lower bound character of expression (23). Now, for a truncation to n terms it suffices to numerically compute $2(n+1)$ integrals having the form

$$\int_0^{\frac{\pi}{6}} \exp\left(-\frac{R(\Psi)^2}{2\sigma^2}\right) \frac{R(\Psi)^{2k}}{k!(2\sigma^2)^k} d\Psi \quad (29)$$

Note that, by using the approach described through this section, we have reduced the problem of computing a four-dimensional integral to calculating an expression based in simple unidimensional integration.

REFERENCES

1. J. J. Eggers, J. K. Su, and B. Girod, "A blind watermarking scheme based on structured codebooks," in *Proc. of IEEE Conf. on Secure Images and Image Authentication*, (London, UK), April 2000.
2. J. Chou, S. Pradhan, L. E. Ghaoui, and K. Ramchandran, "A robust optimization solution to the data hiding problem using distributed coding techniques," in *Proc. SPIE Image, Video Communications & Processing Conference*, **3974**, pp. 301–310, (San José, USA), January 2000.
3. B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Information Theory* **47**, pp. 1423–1443, May 2001.
4. M. Kesal, M. K. Mihçak, R. Koetter, and P. Moulin, "Iteratively decodable codes for watermarking applications," in *Proc. 2nd Symposium on Turbo Codes and Their Applications*, (Brest, France), September 2000.
5. F. Pérez-González, F. Balado, and J. R. Hernández, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. on Signal Processing*, 2003. Accepted for publication in the Special Issue "Signal Processing for Data Hiding in Digital Media & Secure Content Delivery".
6. A. Gersho, "Asymptotically optimal block quantization," *IEEE Trans. on Information Theory* **25**, pp. 373–380, July 1979.
7. J. Conway and N. Sloane, *Sphere Packings, Lattices and Groups*, vol. 290 of *Comprehensive Studies in Mathematics*, Springer, 3rd ed., 1999.
8. H. Brunk, "Quantizer characteristics important for Quantization Index Modulation," in *Security and Watermarking of Multimedia Contents III*, P. W. Wong and E. J. Delp, eds., *Proc. of SPIE* **4314**, pp. 686–694, (San José, USA), January 2001.
9. J. W. Craig, "A new, simple, and exact result for calculating the probability of error for two-dimensional signal constellations," in *Proc. of the IEEE Military Communications Conf. MILCOM '91*, pp. 571–575, (McLean VA, USA), October 1991.
10. M. K. Simon and M.-S. Alouini, *Digital Communications over Fading Channels*, Wiley Series in Telecommunications and Signal Processing, John Wiley & Sons, 2000.

APPENDIX B. ANNEX

For the previously shown comparisons it was required a conversion from probability of symbol error to probability of bit error: the hexagonal schemes presented 3-ary and 9-ary constellations while DC-QP had a binary scheme. There are further considerations to this issue that have been inadvertently omitted in the paper and that we intend to explore in this annex: 1) the conversion from symbol errors to bit errors is not unique, as there are methods other than the one used (there even exists a method that minimizes P_b); 2) also, the comparison of M -ary schemes with different cardinality might be inherently skewed due to the different constellation sizes.

For these reasons we have decided to repeat the simulations for the case in which DC-QP uses a 3-ary constellation in the unidimensional projected domain, thus avoiding the aforementioned conversion step. In the general case, the unidimensional lattice associated to each symbol b in a M -ary constellation is

$$\Lambda_b = M\Delta\mathbb{Z} + b\Delta + d, \quad b \in \{0, \dots, M-1\}. \quad (30)$$

Although a theoretical analysis of DC-QP with these kind of lattices is possible—following the same basic procedure used for the binary lattice case—it turns out to be cumbersome due to the asymmetries between different symbols in a general case. For this reason only empirical simulations are given here.

With this fairer procedure results are less optimistic for DC-QP than in the former comparisons, but in any case they still grant an advantage to this method. In Fig. 5 we can see the results for the 3-ary methods; the cases with $v < 1$ correspond to optimization at WNR = 0 dB. As we can see, the unoptimized version of QP performs now worse than in Fig. 4, where its performance was below the optimized hexagonal lattice results for more negative values of the WNR. Nevertheless, the optimized version at a given WNR performs better than the corresponding hexagonal scheme. In the plot, the offset d in (30) has been chosen to minimize the probability of error, but only very small differences have been found for different values of d .

In spite of these results, it has to be noted that using higher dimensional constellations and bigger values of the WNR the hexagonal lattice will progressively improve its performance over DC-QP and eventually its bit error probability will become smaller. Though, we have seen that, in the low range of WNR and with the constellation sizes used, the hexagonal lattice is not optimal. Note that this result does not mean that the hexagonal lattice is not the optimal channel code for a 3-ary constellation with a power-limited channel, as the problem tackled here is different.

Taking into account the space-filling properties of both methods another interpretation of these results lies in the fact that, although the hexagonal lattice fills very compactly the host signal space, so does the quantization projection

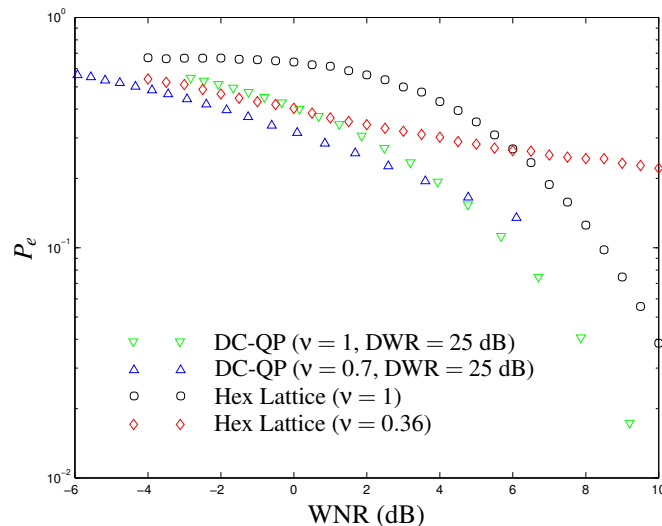


Figure 5. Comparison using 3-ary schemes

method while providing more robust error regions: its Voronoi regions are not closed and so they present certain directions less prone to errors. So, when few symbols are used in the constellation and a low WNR is required (as it happens in many watermarking problems) this type of region shaping seems to be advantageous. An alternative explanation for DC-QP performance is that the projection stage permits to gain enough WNR before quantization, thus improving a merely quantization-based method when WNR is low.

Consequently, the main difference lies in the centroids shape: for whatever lattice, centroids are L -dimensional *points*; for quantized projection methods, centroids are L -dimensional *hyperplanes* (with L the dimensionality considered for embedding). This fact in principle precludes the inclusion of quantization projection methods as a subset of lattices, and therefore results obtained for lattice codes do not apply straightforwardly to DC-QP.