A CAPACITY THEOREM FOR LATTICE CODES ON GAUSSIAN CHANNELS

H. Magalhães de Oliveira and G. Battail

Ecole Nationale Supérieure des Télécommunications
TELECOM-PARIS : Département Communications
46, rue Barrault 75.634 Paris CEDEX 13 France

ABSTRACT

A capacity theorem for lattice codes signaling is presented which is based on an upper bound on the error probability introduced by R. de Buda. It is shown that lattice codes can be used to achieve the channel capacity for any signal-to-noise ratio (positive statement) and the negative statement of the capacity theorem is also proved. The sphere hardening is shown to result from the weak law of large numbers. The proof allows a better understanding of the application of dense lattices as an efficient signaling alphabet. An expression of the reliability function $E(R,C)$ for lattices in AWGN channels is also presented.

I. INTRODUCTION

A LONG TIME PASSED since Shannon's work [1] before the transmission at rates close to the channel capacity (near the cut-off rate) becomes a reality. The conventional coding techniques introduced during three decades were shown to be usefull only for channels in the power-limited region. It was thought that coding had very little to offer to channels in the band-limited region [2]. A breakpoint was finally introduced in Ungerboeck's famous paper on set-partition coding [3]. A new research area in coding theory namely, coded-modulation, was created which has met tremendous interest and immediate practical applications, specially in digital MODEMs [4].

Although dense lattices have long been suggested as efficient codes in Gaussian channels [5,6,7] it seems they became attractive after an excellent paper by Calderbank and Sloane [8]. Since then, coding theorists had increased attention to lattices and cosets. These are an alternative way to represent the coded modulation systems: coset codes (lattice codes) are a powerful and attractive representation of trellis-coded (block-coded) modulation. The main fundamentals on cosets and lattices as a coding technique were recently introduced by Forney [9,10]. The interest in lattice codes stemmed from the work of de Buda [11] who showed that high dimensional lattices can be used in order to reduce the error probability in the presence of Gaussian noise and that such a code asymptotically achieves the channel capacity at high signal-to-noise ratio. In the present paper, we show that lattice codes can achieve the capacity at any signal-to-noise ratio and we also prove the negative statement of the capacity theorem. These results confirm those discussed by de Buda in a more recent paper [12], but in a simpler way which moreover relies on the same tools as he used in his earlier work.

The paper is organized as follows. Section II introduces upper and lower bounds on the worst case error probability which are a slight modification of those presented by de Buda [11]. Sphere hardening theorems are presented in section III and they are used, in section IV, to prove a capacity theorem for lattice codes over the Gaussian channel. Finally, a reliability function for AWGN channels is introduced in section V assuming that coding is made by means of a lattice code.

II. BOUNDS ON THE ERROR PROBABILITY

Some bounds introduced here are essentially a modified version of those presented by R. de Buda. Let $J_n(r)$ denote the volume of a hypersphere of center $\underline{x}$ and radius r, $\{ B_n(\underline{x},r) = \underline{x}' \in R^n \mid |\underline{x}'-\underline{x}| \le r \}$, which is given by

$$J_n(r) = V_n\, r^n \tag{1}$$

where $V_n = \pi^{n/2}/\Gamma(\frac{n}{2}+1)$ is the volume of a normalized n-sphere.

Let us suppose now that the n-dimensional bandlimited noise is AWGN with average power N, so that

$$\underline{r} = (n_1, n_2, \ldots, n_n) \tag{2}$$

where $\{n_i\}$ are independent identically distributed (i.i.d.) Gaussian random variables of zero mean and variance N_n (denoted by $n_i \propto N(0,N_n)$). Here, N_n denotes the variance (average power) of the noise in each dimension. Of course, since the n-dimensional noise is isotropic, one has $N_n = N/n$.

Let r be the magnitude of the noise vector. Then

$$r^2 = n_1^2 + n_2^2 + \cdots + n_n^2 = |\underline{r}|^2. \tag{3}$$

The n-variate probability density of $\underline{r}$ is given by

$$P_n(\underline{r}) = (2\pi N_n)^{-n/2} \exp(-r^2/N_n) \tag{4}$$

and the corresponding normalized probability density is

$$Z_n(\underline{r}) = (2\pi)^{-n/2}\exp(-r^2/2)\,. \tag{5}$$

The n-variate chi-square distribution $Q(\chi^2|n)$ is the probability that the sum of n squared normalized Gaussian random variables exceeds χ^2. It is convenient to express $Q(\chi^2|n)$ as:

$$Q(\chi^2|n) = \int_{\chi}^{\infty} Z_n(r)\, dJ_n(r)\,. \tag{6}$$

It is well known that maximum likelihood decoding (MLD) in AWGN is equivalent to choose the signal point closest to the received signal. Thus, the decision region of each lattice point $\underline{x}_k$ coincides with its Voronoi region $V(\underline{x}_k)$. Given that a lattice point $\underline{x} = \underline{x}_k$ was transmitted, the conditional error probability is

$$P_E(\underline{x}) = P\,(\text{outside}\ \ V(\underline{x}_k)|\underline{x}_k) = 1 - \int_{V(\underline{x}_k)} P_n(\underline{x}_k+\underline{r})\, dV\,. \tag{7}$$

In an unbounded lattice, because of both the lattice symmetry and the additiveness of the noise, it follows that

$$P_E(\underline{x}) = 1 - \int_{V(\underline{0})} P_n(\underline{r})\, dV = P_E(\underline{0})\,. \tag{8}$$

Then the probability that the noise alone is outside the Voronoi region surrounding the origin is the error probability P_E of any lattice point, that is, $(\forall \underline{x} \in \Lambda)\ \ P_E(\underline{x}) = P_E$. If the signaling set Ω (coded constellation) is given by all the points of a lattice contained in a bounded region, the outmost signal points have Voronoi regions which are larger than $V(\underline{0})$ so they have an error probability less than P_E. Thus, P_E is the worst case error probability. It can be bounded as follows.

CH 2901-7/90/0000-0005 $1.00 © 1990 IEEE

Lower Bound

Let $\{ \underline{x}_k \}$ be points of a lattice Λ, and let us consider n-dimensional spheres of radius a, $A(\underline{x}_k) = B_n(\underline{x}_k, a)$, having the same volume as a Voronoi region namely, $V(\underline{x}_k) = V(\underline{0}) = \det \Lambda$, that is, such that

$$J_n(a) = \det \Lambda \,. \tag{9}$$

Since $P_n(\underline{r})$ is a monotonically decreasing function of r, it follows that

$$P(\text{inside } A(\underline{0})|\underline{0}) = \int_{A(\underline{0})} P_n(\underline{r})\, dV \geq P(\text{inside } V(\underline{0})|\underline{0}) = \int_{V(\underline{0})} P_n(\underline{r})\, dV \tag{10}$$

A simple bound on P_E can be obtained by taking the complementary event in R^n, i.e., P (outside $A(\underline{0})|\underline{0}) \leq P$ (outside $V(\underline{0})|\underline{0})$, so that

$$\int_a^{\infty} P_n(r)\, dJ_n(r) \leq P_E \tag{11}$$

or, after changing the variable of integration

$$P_E \geq \int_{a/\sqrt{N_n}}^{\infty} Z_n(r')\, dJ_n(r') = Q(a^2/N_n \mid n) \,. \tag{12}$$

Upper Bounds

A simple upper bound on P_E can be obtained by taking a hypersphere $B(\underline{0}) = B_n(\underline{0},\rho)$ with center at the origin and radius $\rho = d_{\min}/2$, where $d_{\min}$ is the minimum distance between the lattice points. Let $B^c(\underline{0})$ be the complementary set of such a hypersphere. Obviously, P (outside $V(\underline{0})|\underline{0}) \leq P$ (outside $B(\underline{0})|\underline{0})$ or

$$P_E \leq \int_{B^c(\underline{0})} P_n(\underline{r})\, dV = \int_{\rho}^{\infty} P_n(r)\, dJ_n(r) \,. \tag{13}$$

Finally, we obtain

$$P_E \leq \int_{\rho/\sqrt{N_n}}^{\infty} Z_n(r')\, dJ_n(r') = Q(\rho^2/N_n \mid n) \,. \tag{14}$$

From (9) and the definition of the lattice density Δ [13], the relationship between ρ^2 and a^2 can be easily be shown to be $\rho^2 = \Delta^{2/n} a^2$, so (14) may be rewritten as

$$P_E \leq Q(\Delta^{2/n} a^2/N_n \mid n) \,. \tag{15}$$

At this point, it is worthwhile to mention that (14) may be interpreted in a very interesting way. The signaling set Ω (coded constellation) is given by all points in a bounded lattice with average power $P(\Omega)$. Then

$$P_E \leq Q\left(\frac{\rho^2}{P(\Omega)} \frac{P(\Omega)}{N}\, n \mid n\right) = Q\left(\frac{\rho^2}{P(\Omega)} \gamma_{av}\, n \mid n\right) \,. \tag{16}$$

A figure of merit of the coded constellation is given by $FM(\Omega)$, where

$$FM(\Omega) \overset{\Delta}{=} \frac{\rho^2}{P(\Omega)} = \frac{(d_{\min}^2/2)}{P(\Omega)} \,. \tag{17}$$

Let us now suppose that decoding is effected by taking hyperspheres $B(\underline{x}_k) = B_n(\underline{x}_k, b)$ with center at the lattice points $\underline{x}_k$ as decision regions. The radius $r = b < a$ of these spheres will be selected latter. Two types of error can occur with probabilities $P_E I$ and $P_E II$, respectively. First, when the received signal is outside the correct decision sphere. Secondly, since the decision sphere overlap, when a signal from a wrong lattice point is found inside the decision sphere, such an ambiguous decision will be counted as an error of type II.

The type I error probability $P_E I$ can easily be determined by

$$P_E I = \int_r^{\infty} P_n(r)\, dJ_n(r) = Q(r^2/N_n \mid n) \,. \tag{18}$$

The type II error probability is bounded in a more complicated way, according to de Buda's bound. Let $f: \Lambda \to R$ be a Riemann integrable function and let us denote by

$$f(\Lambda) = \sum_{\substack{\underline{x} \in \Lambda \\ \underline{x} \neq \underline{0}}} f(\underline{x}) \tag{19}$$

the sum of $f(\underline{x})$ over all lattice points except the origin. For a lattice point $\underline{x} \neq \underline{0}$, the type II error probability is

$$P_E II(\underline{x}) = \int_{|\underline{r}| < r} P_n(\underline{x}-\underline{r})\, dV(\underline{r}) = f(\underline{x}) \tag{20}$$

so that

$$P_E II(\underline{x}) = f(\Lambda) \,. \tag{21}$$

In order to obtain a bound over $P_E II$, it is intended to use the following theorem of the geometry of numbers [11]:

THEOREM 1 (Minkowsky-Hlawka-de Buda): With $f(\Lambda)$ defined as above, given $\varepsilon > 0$, there exists a lattice with $\det\Lambda = \varepsilon$ such that $\det\Lambda \,.\, f(\Lambda) \leq \int_{(\underline{x})} f(\underline{x})\, dV(\underline{x})$

The first step for determining the bound on $P_E II$ is the evaluation of the integral

$$I = \int_{(\underline{x})} f(\underline{x})\, dV(\underline{x}) \tag{22}$$

where f is given by (20). Substituting (20) in (22) and interchanching the order of the integration (which is possible due the steep decrease of $P_n(.)$), we have

$$I = \int_{|\underline{r}| < r} \int_{(\underline{x})} P_n(\underline{x}-\underline{r})\, dV(\underline{x})\, dV(\underline{r}) \,. \tag{23}$$

Since $P_n(.)$ is a probability density, the inner integral is unity, so

$$I = \int_{|\underline{r}| < r} dV(\underline{r}) = J_n(r) \,. \tag{24}$$

The application of (22),(24) and Theorem 1 implies that a lattice exists which verifies

$$f(\Lambda) \,.\, J_n(a) \leq J_n(r) \,. \tag{25}$$

We can now apply the union bound and (21) so P_E is upper bounded by

$$P_E \leq P_E I + P_E II = Q(r^2/N_n \mid n) + J_n(r)/J_n(a) \,. \tag{26}$$

The parameter r (radius of a decision region) will be given the value b such that the tightest bound is obtained. It is a solution of

$$\frac{d(P_E I + P_E II)}{dJ_n(r\sqrt{N_n})} = -Z_n(r\sqrt{N_n}) + 1/J_n(a\sqrt{N_n}) = 0 \,. \tag{27}$$

This equation has a single real positive root $r = b$, namely:

$$b = \sqrt{N_n (2\ln J_n(a\sqrt{N_n}) - n\ln(2\pi)} \,. \tag{28}$$

The tightest upper bound is thus

$$P_E \leq Q(b^2/N_n \mid n) + Z_n(b\sqrt{N_n}) \,.\, J_n(b) = Q(b^2/N_n \mid n+2) \tag{29}$$

where equality results from integration by part (see also Abramowitz-Stegun [14]). Substituting the volume of a normalized n-sphere and rearranging, we obtain

$$b^2/N_n = n \ln\left(\frac{n/2}{\Gamma^{2/n}(\frac{n}{2}+1)} \frac{a^2}{N}\right) \,. \tag{30}$$

III. SPHERE HARDENING THEOREMS

We are now interested in the behaviour of $Q(\chi^2|n)$ for n very large, where $\chi^2 = r^2$ is given by (3). Let us consider the following random variable transformations:

r.v.	distribution	probability density
r	χ_n	$P_r(\xi;n) = \dfrac{\xi^{n-1}\exp-\xi^2/2}{2^{\frac{n}{2}-1}\,\Gamma(\frac{n}{2})}$
r^2	χ_n^2	$P_{r^2}(\xi;n) = \dfrac{\xi^{\frac{n}{2}-1}\exp(-\xi/2)}{2^{n/2}\,\Gamma(\frac{n}{2})}$
r^2/n	χ_n^2/n	$P_{r^2/n}(\xi;n) = \dfrac{(n/2)^{n/2}}{\Gamma(n/2)}\ \xi^{\frac{n}{2}-1}\ \exp(-\dfrac{n}{2}\xi)$

where

$$P_{r^2/n}(\xi;n) = P_r(\sqrt{n\xi}\ ;\ n)\frac{\sqrt{n}}{2\sqrt{\xi}} = P_{r^2}(n\xi\ ;\ n)\ .\ n\ . \qquad (31)$$

Thus, $Q(\chi^2|n)$ may be expressed alternatively by:

$$Q(\chi^2|n) = \int_{\chi^2}^{\infty} P_{r^2}(\xi;n)\ d\xi = \int_{\chi^2/n}^{\infty} P_{r^2/n}(\xi;n)\ d\xi\ . \qquad (32)$$

THEOREM 2: For any real λ^2, the chi-square function verifies

$$\lim_{n\to\infty} Q(\lambda^2\ n\ |n) = I_{(-\infty,1)}(\lambda^2) \overset{\Delta}{=} \begin{cases} 0 & \text{if } \lambda^2 > 1, \\ 1 & \text{otherwise.} \end{cases}$$

The proof is based on a few results which allow a better understanding of the sphere hardening phenomenon and will be discussed later.

THEOREM 3 (Weak law theorem): Let $\{X_i\}$ be i.i.d. random variables with $X_i \propto N(0,\sigma^2)$ and $W = 1/n\sum_1^n X_i^2$. Then the limit in probability of W is σ^2.

proof. The mean and variance of such a distribution can be shown to be $E(W) = \sigma^2$ and $Var(W) = 2(\sigma^2)^2/n$. By the Chebyshev inequality it follows that $P(|W-\sigma^2| > \varepsilon) \le 2(\sigma^2)^2/(n\varepsilon^2) \to 0$ as $n\to\infty$ **Q.E.D.** ■

The Theorem above can be used to show that $P_{r^2/n}(\xi;n)$ defines a generalized function as we see by the following

THEOREM 4: The sequence of functions $\{\ P_{r^2/n}(\xi;n)\ \}$ defines the Dirac distribution $\delta(\xi-1)$.

proof. We know that

$$\int_{-\infty}^{\infty} P_{r^2/n}(\xi\ ;\ n)\ d\xi = 1 \qquad (33)$$

because $P_{r^2/n}(.;n)$ is a pdf. On the other hand, from Theorem 3:

$$1 \ge \int_{1-\epsilon}^{1+\epsilon} P_{r^2/n}(\xi\ ;\ n)\ d\xi\ = 1 - P(|W-1| > \varepsilon) \ge 1 - 2/(n\varepsilon^2)\ .$$

Taking the limit (when n increases indefinitely) in the expression above,

$$\lim_{n\to\infty} \int_{1-\epsilon}^{1+\epsilon} P_{r^2/n}(\xi\ ;\ n)\ d\xi = 1\ . \qquad (34)$$

Then $\lim_{n\to\infty} P_{r^2/n}(\xi;n) = \delta(\xi-1)$ follows from (33) and (34). **Q.E.D.** ■

proof of Theorem 2:

Writing $Q(\lambda^2 n\ |\ n)$ in terms of the density of the r.v. r^2/n (31), we have

$$Q(\lambda^2 n\ |n) = \int_{\lambda^2}^{\infty} P_{r^2/n}(\xi\ ;\ n)\ d\xi \qquad \text{or}$$

$$\lim_{n\to\infty} Q(\lambda^2\ |n) = \lim_{n\to\infty} \int_{\lambda^2}^{\infty} P_{r^2/n}(\xi\ ;\ n)\ d\xi\ . \qquad (35)$$

The application of Theorem 4 yields:

$\lim_{n\to\infty} Q(\lambda^2 n\ |n) = \int_{\lambda^2}^{\infty} \delta(\xi-1)\ d\xi$ and the result follows. **Q.E.D.** ■

LEMMA 5 : For any integer ν, $\lim_{n\to\infty} Q(\lambda^2 n\ |n+\nu) = I_{(-\infty,1)}(\lambda^2)$

proof. Once again, we write $Q(\chi^2|n)$ in terms of $P_{r^2/n}(.;n)$

$$\lim_{n\to\infty} Q(\lambda^2\ |n+\nu) = \lim_{n\to\infty} \int_{\lambda^2}^{\infty} P_{r^2/n}(\xi\ ;n+\nu\ )\ d\xi \qquad (36)$$

$$\text{but}\quad P_{r^2/n}(\xi\ ;\ n+\nu) = P_{r^2}(n\xi\ ;\ n+\nu)\ .\ n\ . \qquad (37)$$

When n grows, $P_{r^2}(\ \cdot\ ;n) \to P_{r^2}(\ \cdot\ ;n+\nu)$, so that $\lim_{n\to\infty} P_{r^2/n}(\ \cdot\ ;n+\nu) = \lim_{n\to\infty} P_{r^2/n}(\ \cdot\ ;n)$ and the proof follows from Theorem 2. **Q.E.D.** ■

IV. CAPACITY THEOREM FOR LATTICE CODES

The bounds introduced in section II depend on two parameters a and b, so we must find the relationship between these parameters and the transmission rate R. This can be done with the aid of a geometrical representation of signals and noise as shown in Figure 2.

The volume of a Voronoi region is $V(0) = \det\Lambda$ and we took spheres with same volume as $V(0)$ according to (9). If the transmission rate is R *bits/dim*, then the total number of such n-spheres (or signal points) is 2^{nR}. The total volume occupied by all the Voronoi regions is $2^{nR}\ .\ \det\Lambda = 2^{nR}\ .\ J_n(a)$. Suppose that the code consists of all lattice points inside a hypersphere of radius $\sqrt{a^2+S}$ (see Fig. 2), so the available volume is $J_n(\sqrt{a^2+S})$. Then $V_n\ (\sqrt{a^2+S})^n = 2^{nR}\ V_n a^n$, so that

$$R = \frac{1}{2}\ \log_2((a^2+S)/a^2)\ . \qquad (38)$$

THEOREM 6: Given a lattice Λ, if the rate R is less than the channel capacity C then $a^2/N \ge 2^{2(C-R)}$. In contrast, if the rate R exceeds the capacity C, then $a^2/N \le 2^{2(C-R)}$.

proof. The relationship between the lattice parameter a and the transmission rate R is given by (38) which implies $a^2 = S\,(2^{2R}-1)^{-1}$. On the other hand, Shannon's capacity formula leads to $S/N = (2^{2C}-1)$. Thus,

$$a^2/N = (2^{2C}-1)\ (2^{2R}-1)^{-1}\ . \qquad (39)$$

This relation can be rewritten as

$$\frac{a^2}{N} = \frac{2^{2C}-1}{2^{2C}\ 2^{2(R-C)}-1} = 2^{2(R-C)}\ \frac{2^{2C}-1}{2^{2C}-2^{2(C-R)}}\ . \qquad (40)$$

The proof is completed by comparing the second term of the right side of (40) with unity. **Q.E.D.** ■

Recollecting the bounds obtained in section II,

$$Q(a^2/N_n\ |n) \le P_E \le Q(b^2/N_n\ |n+2)\ . \qquad (41)$$

The proof of the capacity theorem is based on new bounds derived from these ones and theorem 6 as follows.

THEOREM 7 (Capacity Theorem)

Positive statement: If the rate R in *bits/dim* is less than C, some lattice code exists such that the decoder error probability tends to zero as n grows.

Negative statement: Conversely, if R exceeds C, any lattice code has error probability near one.

proof.

(negative Statement) Any lattice code with $R > C$ verifies the inequality $a^2/N\ n \le 2^{2(C-R)}n \overset{\Delta}{=} \alpha^2/N\ n$ which is an immediate consequence of Theorem 6. Then the worst case error probability for a lattice code obeys

the following lower bounds:

$$P_E \geq Q(a^2/N_n \mid n) \geq Q(\alpha^2/N_n \mid n) . \qquad (42)$$

By hypothesis, $R > C$, so that $R = C + \varepsilon/2$ for some $\varepsilon > 0$. Applying the lower bound (42), any lattice code must verify $P_E \geq Q(2^{2(C-R)}n \mid n) = Q(2^{-\varepsilon}n \mid n)$. When the dimensionality increases without limit, then $\lim P_E \geq \lim_{n\to\infty} Q(2^{-\varepsilon}n \mid n) = 1$ (from theorem 2).

(Positive statement) Analogically, the application of Theorem 6 to the lattice code with rate $R < C$ yields the following inequality:

$$b^2/N_n \geq 2n\ln 2\left[C - R - \frac{1}{2}\log_2 \frac{\Gamma^{2/n}(\frac{n}{2}+1)}{n/2}\right] \stackrel{\Delta}{=} \beta^2/N_n \qquad (43)$$

so that the worst case error probability verifies the upper bounds: $P_E \leq Q(b^2/N\ n \mid n+2) \leq Q(\beta^2/N\ n \mid n+2)$.

Let us now examine the condition $\beta^2/N > 1$. From (43) this implies

$$C - \frac{1}{2}\log_2 \frac{e\Gamma^{2/n}(\frac{n}{2}+1)}{n/2} - R > 0 . \qquad (44)$$

Let us define

$$\bar{C}(n) \stackrel{\Delta}{=} C - \frac{1}{2}\log_2 \frac{e\Gamma^{2/n}(\frac{n}{2}+1)}{n/2} . \qquad (45)$$

Then $C(n) = C + \phi(n)$, where $\phi(n)$ is a function which approaches zero when n increases indefinitely, as we shall see by

LEMMA 8 : $C(n)$ approaches the channel capacity C when $n\to\infty$, i.e., $\lim C(n) = C$ *bits/dim.*

proof. By the Stirling approximation, $\Gamma(\frac{n}{2}+1) \approx \sqrt{\pi n}(n/2e)^{n/2}$ so that

$$\frac{e\Gamma^{2/n}(\frac{n}{2}+1)}{n/2} \approx (\pi n)^{1/n} , \quad n \text{ large} .$$

Therefore, $\phi(n) \approx \frac{1}{n}\log_2(\pi n)$ goes to zero as $n\to\infty$, and the proof follows directly from the definition of $C(n)$. **Q.E.D.** ■

Rewritting the upper bound on P_E,

$$P_E \leq Q(\beta^2/N\ n \mid n+2) = Q((2\ln 2(C(n)-R)+1)\ n \mid n+2) . \qquad (46)$$

The rate is less than C, so $R = C - \varepsilon$ for some $\varepsilon > 0$. From Theorem 1, a lattice code exists such that:

$$\beta^2/N = 2\ln 2\ (\varepsilon - \phi(n)) + 1 \quad \text{and} \quad \lim \beta^2/N = 2\varepsilon\ln 2 + 1 .$$

Applying the upper bound (46) when $n\to\infty$ gives

$$\lim P_E \leq \lim_{n\to\infty} Q(\beta^2/N_n \mid n+2) = \lim_{n\to\infty} Q[(1+2\varepsilon\ln 2)\ n \mid n+2] \to 0$$

(from Lemma 5) **Q.E.D.** ■

This result has a well known geometrical interpretation. If $a^2 \to N$, then $R \to C$ follows from (38). Futhermore, $\beta^2 \to b^2$ and $\alpha^2 \to a^2$ follows from (40) and (43). If $a^2 \to N$, then $b \to a$ when $n\to\infty$ and the upper and lower bounds in (41) agree. For high dimensionality, the noise becomes concentrated on the surface of a hypersphere of radius equal to the average power of the noise (consequence of Theorem 4). Each lattice point is the center of a hypersphere of radius b ($b \to a$). If the signal plus noise is in the n-sphere around a lattice point $\underline{x}$, it will be decoded as $\underline{x}$. Then if $a^2 > N$ ($b^2 \to a^2 > N$), the received signal will be at the surface of the hypersphere around the transmitted lattice point as $n\to\infty$ and no decoding errors will occur. In contrast, if $a^2 < N$, then $b^2 \to a^2 < N$ and the signal plus noise points will be almost surely decoded in a wrong way. To summarize, if $a^2 > N$ then $P_E \to 0$ as n grows, otherwise $P_E \to 1$.

The use of dense lattice codes is explained as follows. Let us suppose that the n-dimensional lattice was obtained by rescaling [13] a lattice Λ^*, i.e., $\Lambda = (\rho/\rho^*)\Lambda^*$.

We can rewrite equation (9) as $a^2 = (\det\Lambda/V_n)^{2/n}$ so that $a^2 > N$ implies

$$(\det\Lambda/V_n)^{2/n} > N . \qquad (47)$$

But $\det\Lambda = (\rho/\rho^*)^n \det\Lambda^*$, hence the above equation yields

$$\rho^2 (\Delta^*)^{-2/n} > N . \qquad (48)$$

Then we must take a compact lattice Λ^* and use a rescaled version Λ so that the minimal distance 2ρ between lattice points obeys (48)

V. PERFORMANCE OF LATTICE CODES OVER THE AWGN CHANNEL

A reliability function for the AWGN channel can also be obtained by

THEOREM 9 : If $R < C$ *bits/dim*, then a lattice code exists such that

$$P_E < \frac{1}{2}\exp(-nE(R,C))$$

as $n\to\infty$, where $E(R,C) = E(R-C) = (\sqrt{1+2\ln 2\ (C-R)} - 1)^2$.

proof. For $\chi^2 > n+2$, n large, the following approximation of the chi-square distribution can be used:

$$Q(\chi^2 \mid n+2) \approx \frac{1}{2}\operatorname{erfc}(\sqrt{\chi^2} - \sqrt{n+1.5}) < \frac{1}{2}\exp-(\sqrt{\chi^2} - \sqrt{n+1.5})^2 .$$

Let $\chi^2 = (2\ln 2.(C(n) - R) + 1)n$. We find it convenient to express χ^2 as

$$\chi^2 = (1 + 2\ln 2\ .\ (C - R - \phi(n) - \frac{1}{n}\log_2 e))n + 2 .$$

If $R < C$, there is $\varepsilon > 0$ such that $C - R = \varepsilon$. For a lattice with a large enough dimension n, $\varepsilon > \phi(n) + \frac{1}{n}\log_2 e$, so that $\chi^2 > n + 2$. In that case, the chi-square approximation gives

$$P_E \leq \frac{1}{2}\exp[-n(\sqrt{2\ln 2\ .\ (C(n)-R)+1} - \sqrt{1+1.5/n})^2] . \qquad (49)$$

Let us consider the function $E_n(R,C)$ defined as

$$E_n(R,C) \stackrel{\Delta}{=} (\sqrt{2\ln 2\ .\ (C(n)-R)+1} - \sqrt{1+1.5/n})^2 .$$

When n grows, this results in

$$\lim E_n(R,C) = (\sqrt{1+2\ln 2\ (C-R)} - 1)^2 \quad \text{as} \quad n\to\infty . \qquad (50)$$

If we define the reliability function $E(R,C)$ as the above limit, it follows that a lattice exists for which the error probability is bounded as proposed. **Q.E.D.** ■

It is interesting to note that even for relatively small n, the approximation $E_n(C-R) \approx E(C-R)$ is remarkably tight. We present in Figure 3 the $E(R,C)$ function for an AWGN channel with SNR = 27.1 dB as an example. We have used as a bound $P_E < \frac{1}{2}\,2^{-nE_2(R,C)}$ instead of $\frac{1}{2}\exp[-nE(R,C)]$, where $E_2(R,C) = E(R,C)/\ln(2)$.

It is now well established [15,16] that the Leech lattice can be used on telephone channels (B = 2742.86 Hz, SNR = 27 dB) for transmitting at R = 3.5 *bits/dim* (or 7 *(bits/s)/Hz*) with an acceptable error probability, which yields a 19,200 bits/s digital MODEM. It can be seen that lattices are powerful coding tools to allow reliable transmission at high rates (near to the cut-off rate R_0 = 4.0 *bits/dim*, at present). Some bounds presented here have been applied to the Leech lattice at rate R = 7 *bits/2dim*. These results show that in spite of the very high number of neighbours, P_E may be quite acceptable. Both near and above the cut-off rate, the union bound is useless.

VI. CONCLUSIONS

The Minkowski-Hlawka theorem of the geometry of numbers was used by R. de Buda in place of the random coding argument to show that lattice codes are close to the optimal codes at high signal-to-noise ratios. This result was modified here to prove a capacity theorem for the Gaussian channel (negative and positive statements) when high-dimensional lattices are used as signal constellations. This approach allows a better understanding of the sphere hardening and the use of lattice codes to achieve the channel capacity for any SNR. Error bounds are also presented, including an $E(R,C)$ reliability function for lattice coded AWGN channels.

REFERENCES

[1] C.E. Shannon, Probability of error for optimal codes in a Gaussian channel, *Bell Syst. Tech. J.*, **38**, 1959, pp. 611-656

[2] G.D. Forney Jr., Coding and its application in space communications, *IEEE Spectrum*, **7**, Jun., 1970, pp. 47-58

[3] G. Ungerboeck, Channel coding with multilevel/phase signals, *IEEE Trans. Info. Theory*, **IT-28**, n.1, Jan., 1982, pp. 56-67

[4] A.R. Calderbank, The mathematics of MODEMs, *Math. Intell.*, to appear

[5] I.F. Blake, The Leech lattice as a code for the Gaussian channel, *Infor. Contr.*, **19**, 1971, pp. 66-74

[6] J. Leech and N.J.A. Sloane, Sphere packings and error correcting codes, *Canad. J. Math.*, **23**, 1971, pp. 71-745

[7] N.J.A. Sloane, Tables of sphere packings and spherical codes, *IEEE Trans. Info. Theory*, **IT-27**, n.3, May, 1981, pp. 327-338

[8] A.R. Calderbank and N.J.A. Sloane, New trellis codes based on lattices and cosets, *IEEE Trans. Info. Theory*, **IT-33**, n.2, Mar., 1987, pp. 177-195

[9] G.D. Forney Jr., Coset codes. part I: Introduction and geometrical classification, *IEEE Trans. Info. Theory*, **IT-34**, n.5, Sept., 1988, pp. 1123-1151

[10] G.D. Forney Jr., Coset codes. part II: Binary lattices and related codes, *IEEE Trans. Info. Theory*, **IT-34**, n.5, Sept., 1988, pp. 1152-1187

[11] R. de Buda, The upper error bound of a near-optimal code, *IEEE Trans. Info. Theory*, **IT-21**, n.4, July, 1975, pp. 441-445

[12] R. de Buda, Some optimal codes have structure, *IEEE J. Select. Areas Comm.*, **SAC-7**, n.6, Aug., 1989, pp. 893-899

[13] J.H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, NY:Springer, 1988

[14] M. Abramowitz and I.A. Stegun Eds., Handbook of mathematical functions, Washington, DC:National Bureau of Standards, 1972

[15] G.R. Lang and F.M. Longstaff, A Leech lattice MODEM, *IEEE J. Select. Areas Comm.*, **SAC-7**, n.6, Aug., 1989, pp. 968-973

[16] Y. Be'ery, B. Shahar and J. Snyders, Fast decoding of the Leech lattice, *IEEE J. Select. Areas Comm.*, **SAC-7**, n.6, Aug., 1989, pp. 959-967

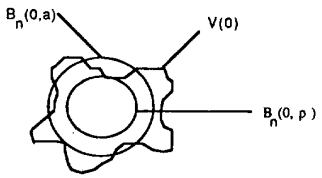

Figure 1
Regions concerning the bounds

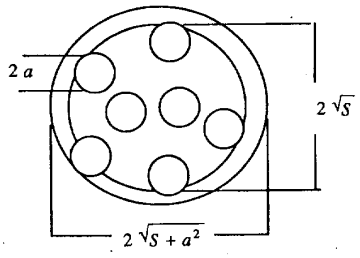

Figure 2
Sphere packing representation of lattice points

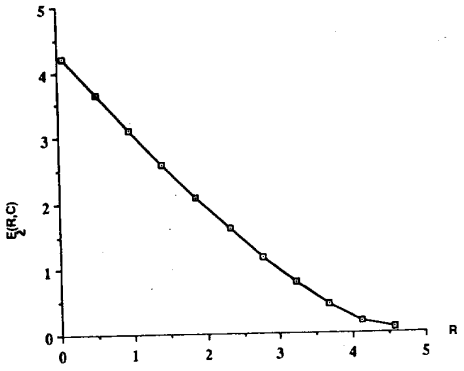

Figure 3
Reliability function $E_2(R,C)$ for a Gaussian channel (SNR = 27.1 dB)