PROGRAM

Thursday, October 29, 1991

9-10 a.m. Invited Lecture: On discrete log authentication and signature schemes.
C. SCHNORR (Frankfurt, Germany) .................................. 112

10-10.30 a.m.
Coffee Break

Cryptography I

10.30-11 a.m. An asymptotic theorem for substitution-resistant authentication codes.
S. MAEST, A. SCAIRO (Trieste, Italy) ......................... 113

11-11.30 a.m.
On randomized cipher systems.
F. PESARIN, F. DI NIZZIO (Padova, Italy) .................. 116

11.30-12 m.
Rational interval maps and cryptography.
S. HARKARI, L. LARIONOV (Moscov, Russia) .... 120

12 m.-12.30 p.m.
On the unconditional performance of authentication and integrity encoding.
G. KABATHANNK, L. LARIONOV (Moscov, Russia) ... 124

Coding Performance I

10.30-11 a.m. Soft decision decoding of Reed-Solomon codes.
P. SWEENY, S.K. SHIM (Surrey, England) ............. 126

11-11.30 a.m.
Bounds on the decoding error probability of binary linear codes via their spectrum.
G. POLYBER (Tel-Aviv, Israel) .......................... 128

11.30-12 m.
Asymptotic performance of lattice codes over the gaussian channel.
H. MAGALHãES, F. OLIVEIRA, G. BATTAIL (Paris, France) ............................. 130

Thursday, October 29, 1991

Boolean functions

2.30-3 p.m.
Boolean functions, differential equations over finite fields of characteristic 2 in coding theory.
C. CARLET (Amiens, France) ....................... 134

3-3.30 p.m.
On generalized bent functions.
P. LANGEVIN (Toulon, France) .................. 138

3.30-4 p.m.
Coffee Break

Coding Performance II

2.30-3 p.m.
Decoding beyond the BCH bound for Reed-Solomon codes
J. MIKRA, P. SWEENY (Surrey, England) ............. 142

3-3.30 p.m.
VLSI Implementation of a fractal image coding algorithm.
R. CREUTZBURG, W. GEISELMANN, H. HIL (Karlsruhe, Germany) .... 147

Cryptography II

4-4.30 p.m.
Pseudoprimes: A survey of recent results.
F. MORAIN (INRIA-Neuquencourt, France) .......... 152

4.30-5 p.m.
Asymptotic analysis of algorithms for finding short codewords.
F. CHABAUD (Paris, France) .................. 154

5-5.30 p.m.
One-time identification with low memory.
S. VAUPENAY (Paris, France) .................. 158

Block Coding VI

4.30-5 p.m.
Bound for trace equation and application to coding theory.
V. GILLOT (Toulon, France) ................ 162

5-5.30
Algebraic geometric codes on surfaces.
Y. AUBRY (Luminy, France) ................ 166

8 p.m.
Banquet
ASYMPTOTIC PERFORMANCE OF LATTICE CODES OVER THE GAUSSIAN CHANNEL

H. Megaílhes de Oliveira (1) and O. Battaïli (2)

II. INTRODUCTION

There is a renewed interest in signaling schemes using finite-dimensional constellations (e.g., lattices) [1-6], especially since solid bases of their theory were laid by Forney [7]. It has been recently reported that lattice codes exist which can achieve the capacity over the additive white Gaussian noise (AWGN) channel [8,9], showing that this technique is quite powerful. We consider here finite-dimensional signaling schemes based on lattices and we intend to clarify the trade-off between signal-to-noise ratio and rate for such schemes.

II. DEFINITION AND BASIC PROPERTIES OF LATTICE CODES

A lattice code $\Omega$ (i.e., an $n$-dimensional signal set or constellation), consists of all the points of a lattice $\Lambda$, or a translate of it, which belong to a given region $R$ of the Euclidean space $\mathbb{R}^n$. Its rate is

$$ R = \left(\frac{1}{n}\right) \log_2 |\Omega| $$

binary units (bits) per dimension, where $|\Omega|$ denotes the cardinality of $\Omega$. We assume here that $n$ is even and we consider the Cartesian product of some quadrature amplitude modulation (QAM) constellation $C$, to be referred to as the constituent constellation, $n/2$ times itself, thus obtaining an $n$-dimensional constellation. Among the points of this constellation, we choose only those which belong to some lattice $\Lambda$ or a translate of it.

Let us recall that, given a set of $m$ linearly independent vectors (points) $y_1, y_2, \cdots, y_m$ of $\mathbb{R}^n$, $m \leq n$, a lattice $\Lambda$ is the (finite, non-countable) set of points $\{x\} = \{y_1, y_2, \cdots, y_m\}$, where $\theta_1, \theta_2, \cdots, \theta_m$ are arbitrary algebraic integers. Therefore, $\Lambda$ is a group under the ordinary vector addition in $\mathbb{R}^n$. The set of vectors (row-vectors) $[y_1, y_2, \cdots, y_m]$ is referred to as the basis of $\Lambda$, and the corresponding generator matrix is defined as the matrix $M$ whose rows are $y_1, y_2, \cdots, y_m$. The Gram matrix is defined as $G = MM^T$, where $T$ denotes transposition and $\times$ denotes equal by definition. Then $V(\Lambda) = \det(G)$ is the volume of the fundamental parallelepiped in $\mathbb{R}^n$, of the set of points $y$ of $\mathbb{R}^n$ such that $y = \alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_m y_m$, $0 \leq \alpha_i < 1$, to be referred to as the fundamental volume of $\Lambda$.

The lattice codes resemble the linear codes of conventional coding theory: all the elements of a lattice are defined as linear combinations of the comparatively few elements of its basis, and the other ones do not depend on the chosen point. However, we consider here the Euclidean space instead of a vector space over some finite field. A lattice code is defined by both the chosen lattice $\Lambda$ and the region $R$, so it will be denoted by $C(\Lambda, R)$, and its rate depends on both according to (1).

Let us recall that the maximum likelihood rule (ML) for the AWGN channel consists of choosing the signal point closest to the received one. Now consider the set of points $R'$ which are closer to a given lattice point $y_i$, then to any other one, which is clearly the decision region associated with the ML rule. It is referred to as the Voronoi region of the lattice. Its shape is the same for all points, and its volume equals the fundamental volume $V(\Lambda)$.

The radius $r$ of the largest sphere centered on the origin and entirely contained in the Voronoi region is called the packing radius. It is the largest possible radius of identical disjoint spheres centered on the lattice points. Clearly, $r = d_{\min}/2$, where $d_{\min}$ is the minimum distance between any two points of the lattice. The radius $r$ of the smallest sphere centered on the origin which entirely contains its Voronoi region is called the lattice covering radius. It is the smallest possible radius of identical spheres centered on the lattice points which cover the whole space.

The density $\Delta$ of the lattice is the ratio of the volume of the largest packing sphere to that of the fundamental volume $V(\Lambda)$:

$$ V_{\pi} = \pi^{n/2} \left(\frac{n}{2}\right) = 1 $$

$$ \Delta = \frac{V_{\pi}}{V(\Lambda)} $$

denotes the volume of an $n$-dimensional sphere of radius 1. $\Gamma(n)$ denotes Euler's factorial function. Similarly, the thickness $\Theta$ of the lattice is the ratio of the volume of the smallest covering sphere to $V(\Lambda)$, i.e., $\Theta = \frac{V_{\pi}}{V(\Lambda)}$.

The center density $\delta$ of the lattice is the number of its points per volume unit i.e., $\delta = \delta V_{\pi} = \pi^n V(\Lambda)$, and its normalized thickness $\Theta$ is similarly defined as $\Theta = \Theta V_{\pi} = \pi^n V(\Lambda)$.

Bounds on these parameters are known for large $n$, some of which being also valid for non-lattice packings or coverings [10]. From the Minkowski lower bound and the upper bound of Kneser, Levitzki, and Sidel'nikov on the largest possible density, (2) and Stirling's approximation result in:

(1) Department of Electronics and System - Communication Research Group CODEC, Universidade Federal de Paranaiba, Curitiba.
(2) Universidade Federal do Paraná, Brazil.
(3) Universidade Federal de Minas Gerais, Belo Horizonte.
(4) Centre National d'Etudes des Télécommunications, Département Communications, France.
\[
\frac{1}{\text{lim}_{n \to \infty}} \leq \lim_{n \to \infty} \frac{S_{n}}{n} \leq \frac{1}{2 \text{lim}_{n \to \infty} n}
\]

(3)

clearly, the limit of the normalized thickness is shown to be for the thinnest covering:

\[
\lim_{n \to \infty} \frac{S_{n}}{n} = \frac{1}{2n}.
\]

(4)

the average normalized power of the constituent constellation, a dimensionless quantity, is defined as the average squared norm of its points and denoted by \( P(C) \). This quantity is obviously additive in the average squared norm of the lattice code points is \( P(\Omega) = \frac{N}{2} P(C) \).

Let the signal associated with the constituent constellation be \( s(t) = a_{1} \cos(2\pi f_{c} t) + a_{2} \sin(2\pi f_{c} t) \) where \( a_{1} \) and \( a_{2} \) are the coordinates of a point \( f_{c} \) is the carrier frequency and \( u(t) \) is some pulse of finite energy \( E_{u} \). Then the average physical energy per constituent constellation is \( E_{C} = P(C) E_{u}/2 \). The signal-to-noise ratio per constituent constellation is \( P(C) E_{u}/2N_{0} \). Both the signal and noise energies are additive, so it is also the overall signal-to-noise ratio \( \gamma = E_{u}/N_{0} \).

III. BOUNDS ON THE \( n \)-DIMENSIONAL ERROR PROBABILITY

We have now the following bounds on the error probability of lattice codes over the AWGN channel:

THEOREM 1. The error probability of lattice codes over the additive white Gaussian noise channel is bounded as

\[
Q(\text{FM}(p, \Omega)) \leq P_{e}(n) \leq Q(\text{FM}(p, \Omega)) + \gamma n/n_{0}.
\]

(5)

\[
Q(\chi^{2}) = \frac{1}{\sigma^{2} \Gamma(\alpha/2)} \int_{0}^{\frac{\alpha^{2}}{2}} e^{-\frac{x}{2\alpha}} dx = \frac{1}{\alpha} \frac{\Gamma(\frac{\alpha}{2})}{\Gamma(\alpha/2)} \exp\left(-\frac{\alpha}{2}\right) d\alpha/2.
\]

\[\sum_{i=1}^{n} X_{i}^{2} \text{ is the sum of } n \text{ independent } \chi^{2} \text{ random variables with mean zero and unit variance.}
\]

\[\sum_{i=1}^{n} X_{i}^{2} \text{ is the sum of } n \text{ independent } \chi^{2} \text{ random variables with mean zero and unit variance.}
\]

\[\text{FM}(p, \Omega) = p^{n} P(C) = 2^{n} \text{ EnP(}C\text{)} \text{.}
\]

(6)

The bounds (5) are easily derived if we remember that the inner ML decision regions in the presence of AWGN are identical to the Voronoi regions. Then a noise vector whose \( n \) components are i.i.d. Gaussian variables, each of mean zero and variance \( \sum_{i=2}^{n} \), is added to the signal. The squared norm of this noise vector thus obeys the \( \chi^{2} \) law with \( n \) degrees of freedom. As soon as its norm exceeds \( p \), this vector may be outside the Voronoi region, hence the upper bound. On the other hand, it is certainly outside this region if its norm is larger than \( p \) and the lower bound results.

IV. LATTICE POINTS CONFINED IN BOUNDED REGIONS

Forney and Wei [11] showed that the normalized power, \( P(C) \), is approximately equal to \( 2 \alpha \) times the average power \( P(R) \) of a continuous distribution that is uniform within \( R \) and zero elsewhere, resulting in:

\[
P(C) = 2G(R) V^{n}(R).
\]

(7)

Where \( V(R) = \int_{R}^{n} \text{ is the volume of } R \text{ and } G(R) = \|r\|^{n} v^{n-1}(R) \text{ where } r \text{ is a vector of } R \text{ and } \|r\| \text{ is its norm (in the } n \text{ dimensional space) of } R \text{ which measures the effect of its shape on the average signal power.}
\]

They also proposed the approximation

\[
Q = V(R) V(\Lambda).
\]

(8)

The normalized power \( P(C) \) is thus replaced by (7) and (8) to both the ratio (1) and the fundamental volume \( V(\Lambda) \).

However, the argument used by Forney and Wei in [11] for deriving (8) does not take into account the boundary points. In order to include points on the border of \( R \), we introduce

PROPOSITION 1. The size \( |Q| \) of any constellation consisting of the points of a lattice \( A \) (or a translate of \( A \)) inside, any bounded region \( R \) of volume \( V(R) \) is approximately

\[
|Q| = \left( 1 + \left( \frac{V(R)}{V(\Lambda)} \right) \right)^{n}.
\]

(9)

This result is obtained by considering an augmented region \( R^{*} \) which is the union of the fundamental regions associated with all the lattice points inside \( R \) and on its border, which needs an additional volume such that \( V(R^{*}) = V(R) + V(\Lambda)\). Since the normalized power, proportional to the volume raised to the power \( 2/n \), is additive.

Let us denote by \( S \) (resp. \( N \)) the average signal (resp. noise) power (both considered as \( n \)-dimensional signals). If we denote by \( \bar{r} = \sqrt{S/N} \) the radius of a sphere of volume equal...
to $V(A)$, then the radius $r^*$ of a sphere of the same volume as that of the segmented region $B_1$ is such that $V(r^*) = \frac{1}{2} \frac{2^n}{2^{n-1}} r^*$ and $V = \frac{V^n}{2^n}$. Therefore, Proposition 1 results in $\mathbb{E}[C^2] = \mathbb{E}[U^2]$, which corresponds to a rate per dimension of

$$R = \frac{1}{2} \log(1 + S^2).$$

(10)

This estimate of the rate has been used in conjunction with the sphere hardening argument (one must have $S > N$ in order to ensure that the error probability goes to zero as $n \to \infty$) in the original proof of the capacity theorem [13], and recently in the proof that lattices exist which achieve the channel capacity [9].

Combining (7), (9) and (10) results in:

**PROPOSITION 2.** The average signal power normalized to 2 dimensions of any constellation $\Omega$ consisting of the points of a lattice $\Lambda$ (or a translate of $\Lambda$) that lie within a region $R$ is approximately equal to $P(C) = 2E[\mathbb{E}[X^2]] V^2(n) = 2E[\mathbb{E}[X^2]] V^2(n) - 1 V^2(A)$.

### V. GAINS OF LATTICE CODES

The gain $\gamma(a; \Omega)$ of an $n$-dimensional constellation $\Omega = C(\Lambda, R)$ with respect to another one $\Omega_2 = C(\Lambda_2, R_2)$ at the same rate $R$ can be defined as the ratio of their figures of merit, the exponent minus plus standing for values based on (6) in terms of the packing radius $R$ or in terms of the covering radius $r$, respectively:

$$\gamma(a; \Omega) = \frac{P(C(a))}{P(C)}.$$

Now, under the continuous approximation (7), it follows that $\gamma(a; \Omega) = \frac{P(C(a))}{P(C)}$. We can therefore split the above gains in two factors:

$$\gamma(a; \Omega) = \frac{P(C(a))}{P(C)} \frac{V^2(n)}{V^2(n)}.$$

(11)

and $\gamma(R; n)$, which is identical to the fundamental gain as defined in [7].

Applying the above approximations to Theorem 1 gives the following lower and upper bounds:

$$Q\left(\frac{V^2(n)}{2^{n-1}}\right) - \frac{2n}{2^{n-1}} n \leq \gamma(a; \Omega) \leq \frac{V^2(n)}{2^{n-1}} \frac{3n}{2^{n-1}} n.$$  

(12)

These bounds are applied to a few lattices at different transmission rates. We also compare the results on the error rate for the mother lattice with experimental results obtained from a commercial modem in $P = 3.5$ bit per dimension [10].

### VI. ASYMPTOTIC BEHAVIOUR OF LATTICE CODES

**PROPOSITION 3.** The gains of the best lattice $\Lambda$ for an arbitrarily large number of dimensions are bounded as:

$$\lim_{n \to \infty} \gamma(a; \Lambda(n)) = 1/2n \leq \gamma(a; \Lambda(n)) \leq \gamma(a; \Lambda(n)) = 1/2n.$$

(13)

Moreover, the shape gain is bounded as:

$$\lim_{n \to \infty} \gamma(a; \Lambda(n)) \leq 6.$$

(14)

for any dimensionality, the equality to the upper bound being obtained for a spherical region.

**B.bounds (13) mainly result from (11) and the inequalities (3) and (4). Bounds (14) are found in [11].

We know that lattice codes exist which asymptotically reach the channel capacity [8,9] and we now look at the conditions a lattice code should fulfill for having this asymptotic behaviour, in terms of its coding gain. Both the lower and upper bounds in (12) are minimized by taking the maximum of $\gamma(a; \Omega)$ i.e. $1/2n$ according to (14), which implies that the region $R$ is asymptotically spherical.

The capacity per dimension is $C = (1/2) \log(1 + S^2)$, so we may replace $S^2$ by $2^{n-1} - 1$ in the lower bound of (12).

According to (13b), the factor of $2^{n-1} - 1$ in the argument of $Q(n)$ in this bound approaches 1 as $n$ goes to infinity.

On the other hand, the weak law of large numbers implies the sphere hardening phenomenon: $\lim Q(2^n h(n)) = 1$ if $h(n) \approx 1$, so the lower bound in (12) can be met for rates $R$ up to the channel capacity $C$. On the
boundary, (13a) shows that the upper bound cannot be met for $R$ close to the channel capacity $C$; even the channel limit rate $R_p = (1/2)\log_2(1 + \gamma_p/\gamma)$ cannot be achieved. Since the capacity can asymptotically be achieved, we must conclude that lattice codes exist such that $P_e(n)$ actually approaches its lower bound in (12) as $n$ goes to infinity.

These results have an interesting geometric interpretation: the lower bound in (12) depends on the lattice covering radius $\gamma$ via $\gamma(a)$ and $\delta$, whereas the upper bound in (12) depends on its packing radius $\rho$ via $\gamma(\Lambda)$ and $\delta$. Since the error probability of the best code approaches the lower bound, the radius $\rho$ of its decision region, assumed to be spherical, should approach the covering radius. The radius $\rho$ of a sphere of same volume as the Voronoi region also approaches the same limit as $n$ goes to infinity. According to [9], we have $p < s < r$, but as $n$ approaches infinity the last three radii converge to the same limit for the best lattice code, and this limit is strictly larger than that of the first one. The Voronoi region of this code behaves essentially as a sphere of radius $r$, although its packing radius is distinctly smaller.

Even the best packing of spheres does not achieve capacity (see (3)). By allowing partial overlap when packing $n$-spheres we gain more degrees of freedom to construct signal sets and thus more centers per volume unit, hence higher rates, can be achieved. For instance, the decoding rule used in [9] to prove the existence of good lattices used $n$-spheres of radius $\rho > r$, hence with partial overlap, as decision regions. We think that the problem of achieving capacity is linked to the asymptotic thickness of arbitrarily large dimensionalities rather than to the asymptotic density as believed by many researchers. We thus propose to interpret a family of good codes (i.e., which asymptotically achieve capacity) as a family of coverings for which $\Theta^{n^2} \rightarrow 1$ (or $\Theta^{n^2/n} \rightarrow 1/2e$), although $\Theta \rightarrow \infty$.

VII. CONCLUSION

We presented upper and lower bounds on the performance of communication systems based on lattice codes combined with QAM in terms of figures of merit. Our aim was to gain insight in the tradeoff between rate and signal-to-noise ratio. Further, an improvement has been proposed on the continuous approximation for estimating the rate. Bounds on the best gains per dimension (related to packing and covering) were presented for arbitrarily large dimensionalities. We conjecture that the problem of achieving capacity is connected to the asymptotic behaviour of the thickness of lattices.

REFERENCES