

Blind Acquisition Performance for Faded Digital Signals

I. Vaughan L. Clarkson

School of Information Technology & Electrical Engineering
The University of Queensland, Qld., 4072, AUSTRALIA
v.clarkson@itee.uq.edu.au

Iain B. Collings

School of Electrical and Information Engineering
The University of Sydney, NSW 2006, AUSTRALIA
i.collings@ee.usyd.edu.au

Abstract—This paper presents an analytic expression for the probability of correct acquisition for blind reception of PAM, ASK and QAM digital modulation signals. The expressions are a function of the number of measured symbols. Applications include modulation acquisition for eavesdropping, as well as pilot-less digital broadcasting over rapidly fading channels.

I. INTRODUCTION

Blind signal reception has a wide range of applications, from modulation acquisition for eavesdropping, to pilot-less digital broadcasting over rapidly fading channels. Blind reception relies solely on the received channel output and some *a priori* (often statistical) knowledge of the input signal.

Traditionally, blind algorithms are based on exploiting higher order statistics of baud-rate sampled received signals, and most recent algorithms are based on subspace decompositions. See [1] for a summary of the area. Examples include methods exploiting only second-order statistics, sub-channel matching algorithms, and MUSIC algorithms. Other techniques include whitening the covariance matrix for the channel outputs which alleviates the sensitivity to unknown channel order, and other schemes which rely on the signal having a constant modulus constellation. These techniques all rely on the channel remaining constant for the duration of transmission, and require a large number of measurements.

In this paper we target relatively fast fading channels, and where adequate training is either not possible (eg. as in packet data transmission) or is not known (eg. as in eavesdropping applications, or due to timing issues). The problem is particularly exacerbated when the fading is too fast to track, even with existing adaptive algorithms such as Kalman filters (eg. as in [2]). The aim here is to estimate the channel using the least possible number of received symbols. This paper considers flat fading, however the techniques can be extended to frequency selective channels.

The main issue for blind detection is that without channel knowledge there are a number of potential detection ambiguities. Regardless of the accuracy of any particular estimation algorithm, in the absence of training data there is always a rotation ambiguity resulting from the symmetry of the modulation format. For example, for QAM it is impossible to distinguish any multiple of a 90 degree rotation, even if one is able to measure all symbols in the received constellation. We call these rotationally-equivalent constellations the *fundamental constellations*. Of course if only limited measurements are made, then the ambiguities are even greater.

In this paper we provide analytical expressions for the probability of acquiring one of the fundamental constellations

for PAM, ASK, and QAM, in the absence of measurement noise, as a function of the number of received symbols. This quantity is then used as the basis for an approximation to the blind acquisition high SNR BER floor in fast fading channels. A new acquisition algorithm is discussed, and results are presented which show good alignment with the analytical expression.

II. MATHEMATICAL BACKGROUND

We first present some elementary results in number theory. Most of the material in this section is distilled from [3].

A. Gaussian Integers

As usual, $\mathbb{Z}$ is the set of integers, sometimes called *rational integers*. The *Gaussian integers* are the set $\mathbb{Z}[j]$ of all complex numbers $a+bj$ where both a and b are integers, and $j = \sqrt{-1}$.

Like the rational integers, the Gaussian integers can be uniquely factorized into prime factors. Any $z \in \mathbb{Z}[j]$ can be expressed as

$$z = p_1 p_2 \dots p_N$$

where the p_j are *Gaussian primes*. If a Gaussian integer is prime then so is its product with a unit ± 1 or $\pm j$. Primes related in such a way are called *associates*. Prime factorization is unique up to rearrangement of terms and their substitution by associates.

B. Ideals

Here we define ideals only in rational and Gaussian integers. An *ideal* $\mathcal{I}$ is a subset of the (Gaussian or rational) integers $\mathcal{R}$ with the properties that, when $a, b \in \mathcal{I}$ and $r \in \mathcal{R}$, we have $a + b \in \mathcal{I}$ and $ra \in \mathcal{I}$.

For rational and Gaussian integers, an ideal can be represented by a single element, its *generator* (i.e., all ideals are so-called *principal ideals*). Given a generator g , the ideal is the set $\{kg \mid k \in \mathcal{R}\}$. We use the notation $\langle g \rangle$ to represent the ideal generated by g . Of course for rational integers, $\langle g \rangle = \langle -g \rangle$, and for Gaussian integers, $\langle g \rangle = \langle jg \rangle = \langle -jg \rangle$.

We define the *norm* of an ideal as the absolute value of its generators, i.e., $|\langle g \rangle| = |g|$.

Ideals can be multiplied by multiplying the generators, and therefore they can also be factorized. In fact, ideals have a unique prime factorization into *prime ideals*. The prime ideals are generated by prime elements.

Notice that $\langle 0 \rangle$ is a 'special case' of the ideals, in that it is the only ideal that contains a finite number of elements. We usually take care to exclude this zero ideal from consideration.

C. The Möbius Function & Inversion Formula

The (classical) Möbius function is defined on the rational integers such that

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has one or more repeated factors,} \\ 1 & \text{if } n = 1, \\ (-1)^k & \text{if otherwise } n \text{ has } k \text{ prime factors.} \end{cases} \quad (1)$$

A well known identity is that

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \mu(n) n^{-s}.$$

where $\zeta(s)$ is the Riemann zeta function.

There are a (great) number of inversion formulae associated with the Möbius function. One particularly useful here is if

$$A(n) = \sum_{m=1}^{\infty} B(mn) \quad (2)$$

for some functions A and B defined on the naturals, then

$$B(n) = \sum_{m=1}^{\infty} \mu(m) A(mn). \quad (3)$$

Following [4], we can generalise the Möbius function in the obvious way to ideals: simply replace the integer argument n in (1) with the argument $\mathfrak{I}$ (the context will make clear the sense in which μ is used). In particular, following all the same arguments that lead to Theorem 270 in [3], we may restate (2) and (3) in terms of ideals (see also [5]).

Theorem 1: When $\mathcal{R}$ is the set of rational or Gaussian integers,

$$A(\mathfrak{n}) = \sum'_{\mathfrak{m} \subseteq \mathcal{R}} B(\mathfrak{m}\mathfrak{n}) \quad \text{iff} \quad B(\mathfrak{n}) = \sum'_{\mathfrak{m} \subseteq \mathcal{R}} \mu(\mathfrak{m}) A(\mathfrak{m}\mathfrak{n}),$$

where A and B are functions defined on the ideals of $\mathcal{R}$, and where we use $\sum'$ to indicate that the sum excludes $\langle 0 \rangle$.

We define a function f to be *multiplicative* (when defined on ideals) if $f(\mathfrak{m}\mathfrak{n}) = f(\mathfrak{m})f(\mathfrak{n})$ whenever the greatest common divisor is $\langle 1 \rangle$. Following [4], we can state the following theorem.

Theorem 2: If f is defined on ideals in $\mathcal{R}$, the rational or Gaussian integers, and f is multiplicative then

$$\sum'_{\mathfrak{n} \subseteq \mathcal{R}} f(\mathfrak{n}) = \prod_{\mathfrak{p} \text{ prime}} \sum_{k=0}^{\infty} f(\mathfrak{p}^k)$$

whenever either side is absolutely convergent.

III. SIGNAL MODELS

First let us examine the M -ary PAM/ASK signal model with Gray mapping and with M even. The i^{th} symbol (in time) is a 2's-complement signed integer, x_i . Thus,

$$-M/2 \leq x_i < M/2. \quad (4)$$

For PAM, the amplitude $2x_i + 1$ is transmitted (into the discrete-time channel), and for ASK it is mixed with a carrier before transmission.

We consider flat fading channels with white Gaussian noise (variance σ^2) in the receiver. The received symbols, y_i , are therefore given by

$$y_i = A(2x_i + 1) + \xi_i \quad (5)$$

where $A > 0$ (A and ξ_i are complex in the case of ASK).

The blind acquisition problem is to estimate x_i based on measurements y_i without knowledge of A and in the absence of training data.

In the case of M -ary QAM the modulation process can be viewed as mapping the data to a Gaussian integer, x_i . The transmitted symbol is then given by the constellation point $2x_i + 1 + j$, representing the amplitude and phase of the carrier. The transmitted value is assumed to lie inside a set $2\lambda\mathcal{S}$, which we call the *constellation shape*, for an appropriate real scaling factor $\lambda > 0$, and $\mathcal{S}$ a set satisfying the conditions that

- 1) $|x|^2 \leq \frac{1}{2} \Rightarrow x \in \mathcal{S}$,¹
- 2) $|x|^2 > 1 \Rightarrow x \notin \mathcal{S}$ and
- 3) the area of $\mathcal{S}$ exists, i.e., its indicator function is Riemann integrable. Recall that, given a set $\mathcal{U} \subseteq \mathbb{C}$ and $x \in \mathbb{C}$, the *indicator function* $\Phi(\mathcal{U}, x)$ of $\mathcal{U}$ is defined so that

$$\Phi(\mathcal{U}, x) = \begin{cases} 1 & \text{if } x \in \mathcal{U}, \\ 0 & \text{otherwise.} \end{cases}$$

The unit circle and the unit rotated-square are therefore acceptable choices for $\mathcal{S}$, and correspond to constellation shapes which are used in practice. Note that, implicitly, M is a function of λ .

The received symbols are

$$y_i = A(2x_i + 1 + j) + \xi_i \quad (6)$$

where A is complex.

As mentioned previously, the fact that A is complex leads to multiple fundamental constellations which are indistinguishable regardless of the number of symbols measured. To overcome this problem it is typical either to transmit a pilot symbol at the start of a block, or to employ differential encoding.

IV. MAXIMUM-LIKELIHOOD ESTIMATION

The log-likelihood function for PAM is

$$L_{\text{PAM}}(\hat{\mathbf{x}}, \hat{A} \mid \mathbf{y}) = -\|\mathbf{y} - \hat{A}(2\hat{\mathbf{x}} + \mathbf{1})\|^2 \quad (7)$$

for admissible $\mathbf{x}$, where constant factors have been discarded, $\|\cdot\|$ represents the Euclidean norm of its argument, $\mathbf{x} = (x_1, \dots, x_n)$, and $\mathbf{y} = (y_1, \dots, y_n)$. By *admissible* $\mathbf{x}$, we mean that (4) is satisfied. For inadmissible $\mathbf{x}$, the likelihood is zero. The vector $\mathbf{1}$ has 1 in every element.

From (7), it follows that the maximum-likelihood (ML) estimate of A , given $\hat{\mathbf{x}}$, is the solution to a least-squares problem and therefore

$$\hat{A}_{\text{ML}} = \frac{(2\hat{\mathbf{x}} + \mathbf{1})^T \mathbf{y}}{\|2\hat{\mathbf{x}} + \mathbf{1}\|^2}. \quad (8)$$

¹In fact, it is possible to improve $\frac{1}{2}$ to $\frac{1}{5}$ here, with only minor alterations to subsequent arguments.

Where two or more estimates have equal likelihood, we will choose the estimate for which $\hat{A}_{\text{ML}}$ is largest.

The corresponding expressions can be derived for QAM.

V. ERROR ANALYSIS IN THE ZERO-NOISE CASE

As noted previously, even in the absence of noise, it is possible that the ML estimate is not unique.

A. M -ary PAM

First consider that when there is no noise, $L_{\text{PAM}}(\hat{\mathbf{x}}, \hat{A} \mid \mathbf{y})$ equals zero for any admissible $\hat{\mathbf{x}}$ and odd integer k where

$$\hat{A} = \frac{A}{k}, \quad \hat{\mathbf{x}} = k\mathbf{x} + \frac{k-1}{2}\mathbf{1}$$

Fortunately, these solutions do not present a problem to the ML estimation algorithm we have proposed, since we choose the largest value of $\hat{A}$ when there is a tie.

Clearly, $\hat{A}$ will not yield a ML estimate unless $\mathbf{y}/\hat{A} \in \mathbb{Z}^n$. We already know that $\mathbf{y}/A = \mathbf{z} = 2\mathbf{x} + \mathbf{1}$ is an integer vector. Therefore, a necessary condition for an incorrect acquisition is that there exists some $\hat{A} = \gamma A$ with $\gamma > 1$ such that

$$\mathbf{y}/\hat{A} = \mathbf{z}/\gamma \in \mathbb{Z}^n$$

We see that γ cannot be irrational for then $\mathbf{z}/\gamma$ could not be integral. Since γ must be rational, write $\gamma = p/q$ where p/q is in lowest terms and $p > 1$. In order for $\mathbf{z}/\gamma$ to be integral, p must therefore divide every element of $\mathbf{z}$. Hence, a necessary condition for a decoding error in the zero-noise case is that

$$\gcd\{z_1, \dots, z_n\} > 1$$

where $\gcd\{\cdot\}$ is the *greatest common divisor (g.c.d.)* of its arguments. Notice that the g.c.d. cannot be even, since each of the z_i are odd. If there is a g.c.d. greater than one, then it must be odd, and therefore each quotient with the g.c.d. is odd too. Therefore, with $\gamma = p$, the resulting $\hat{\mathbf{x}}$ is also admissible, and we see that our necessary condition for making a decoding error is also a sufficient condition.

This leads us to the following theorem, which is very similar in style to Theorem 3.1 of [6].

Theorem 3: Let E represent the event that a ML decoding error is made on a series of noiseless observations y_i , $i = 1, \dots, n$, $n > 1$, of M -ary PAM symbols as defined by (5). If each source symbol is independent and uniformly distributed then

$$\lim_{M \rightarrow \infty} \Pr\{E\} = 1 - \frac{1}{(1 - 2^{-n})\zeta(n)}.$$

Proof: Let D_k be the event that k divides each z_i . By a simple counting argument, and under the assumption of independent and uniformly distributed source symbols,

$$\Pr\{D_k\} = \begin{cases} \left(\frac{2}{M} \left\lfloor \frac{M-1+k}{2k} \right\rfloor\right)^n & \text{if } k \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Let G be the g.c.d. of the z_i . Then we also have that

$$\Pr\{D_k\} = \sum_{m=1}^{\infty} \Pr\{G = mk\}.$$

From the foregoing discussion, we know that a decoding error can only occur when this g.c.d. is greater than 1. Hence,

$$\Pr\{E\} = \Pr\{G > 1\} = 1 - \Pr\{G = 1\}.$$

Using the Möbius inversion formula (2), (3), we have that

$$\Pr\{G = k\} = \sum_{m=1}^{\infty} \mu(m) \Pr\{D_{km}\}.$$

Now, we would like to evaluate

$$\lim_{M \rightarrow \infty} \Pr\{G = 1\} = \lim_{M \rightarrow \infty} \sum_{k=1}^{\infty} \mu(k) \Pr\{D_k\}.$$

In order to exchange limits and summation, we apply the Weierstrass M -test to the summands. Observe that

$$|\mu(k) \Pr\{D_k\}| \leq \left(\frac{2}{M} \left\lfloor \frac{M-1+k}{2k} \right\rfloor\right)^n \leq \left(\frac{2}{k}\right)^n.$$

Now, when $n > 1$,

$$\sum_{k=1}^{\infty} \left(\frac{2}{k}\right)^n = 2^n \sum_{k=1}^{\infty} k^{-n} = 2^n \zeta(n) < \infty.$$

Hence, limits and summation can be swapped and we have

$$\begin{aligned} \lim_{M \rightarrow \infty} \Pr\{G = 1\} &= \sum_{k=1}^{\infty} \lim_{M \rightarrow \infty} \mu(k) \Pr\{D_k\} \\ &= \sum_{k=1}^{\infty} \mu(k) d(k) k^{-n} \end{aligned} \quad (9)$$

where $d(k)$ is equal to 1 if m is odd or 0 otherwise.

Notice that $f(k) = \mu(k) d(k) k^{-n}$ is multiplicative. Therefore, by Theorem 2,

$$\begin{aligned} \lim_{M \rightarrow \infty} \Pr\{G = 1\} &= \prod_{p \text{ prime}} \sum_{k=0}^{\infty} \mu(p^k) d(p^k) p^{-kn} \\ &= \prod_{p > 2 \text{ prime}} (1 - p^{-n}) \\ &= \left[\prod_{p > 2 \text{ prime}} \frac{1}{1 - p^{-n}} \right]^{-1} \\ &= \left[\prod_{p > 2 \text{ prime}} \sum_{k=1}^{\infty} p^{-nk} \right]^{-1} \\ &= \left[\sum_{k > 0 \text{ odd}} k^{-n} \right]^{-1} \\ &= \left[\sum_{k=1}^{\infty} k^{-n} - \sum_{k > 0 \text{ even}} k^{-n} \right]^{-1} \\ &= \left[(1 - 2^{-n}) \sum_{k=1}^{\infty} k^{-n} \right]^{-1} \\ &= \frac{1}{(1 - 2^{-n})\zeta(n)}. \end{aligned}$$

The result follows. ■

Now (9) yields a very good approximation to the probability of a decoding error in the zero-noise case. We see that

$$\lim_{M \rightarrow \infty} \Pr\{G = 1\} = 1 - 3^{-n} - 5^{-n} + \dots$$

Hence, we can approximate the decoding error for large n as

$$\lim_{M \rightarrow \infty} \Pr\{E\} \approx 3^{-n}.$$

That is, the probability of a decoding error is dominated for large n by the probability that all the z_i are multiples of 3.

B. M -ary QAM

Let us now turn to the M -ary QAM case, for which we follow a broadly similar approach. However, for QAM, we will find it convenient to use the Gaussian integers and ideals.

As with PAM, it is possible to make $L_{\text{QAM}}(\hat{\mathbf{x}}, \hat{A} \mid \mathbf{y})$ equal to zero. One solution is $\hat{A} = A$, but so also is $\hat{A} = A/k$ where k is any Gaussian integer not belonging to the ideal $\langle 1+j \rangle = \langle 1-j \rangle$ (cf. the PAM case, where k could be any rational integer which did not belong to the ideal $\langle 2 \rangle$, the even numbers). Here,

$$\hat{\mathbf{x}} = k\mathbf{x} + \frac{k-1}{1-j}\mathbf{1}.$$

In particular, k can be any unit. Therefore (and as we would intuitively expect), we can never determine A unambiguously: rotations of any multiple of $\pi/4$ are equally likely. Hence, it is necessary to use coding at the transmitter that is invariant under such rotations. One option is differentially encoded (DE) QAM. However, all other values of k need not trouble us, since in that case $|k| > 1$, and we have designed our ML procedure to choose that value of $\hat{A}$ with largest absolute value from amongst all equally likely values.

Let us now examine if there is any other $\hat{A}$ that could maximise the likelihood. First observe that, in the noiseless case, the y_i can be written as

$$y_i = A(1+j)[(1-j)x_i + 1] = Bz_i$$

where $B = (1+j)A$ and $z_i = (1-j)x_i + 1$. That is, the z_i are Gaussian integers which do not belong to the ideal $\langle 1+j \rangle$. The z_i also belong to the set $(1-j)\lambda\mathcal{S}$. Writing $\hat{B} = (1+j)\hat{A}$, we see that it is a necessary condition for a decoding error in the zero-noise case that there be values of $\hat{B} \neq B$ such that

$$\mathbf{y}/\hat{B} = \mathbf{z}/\gamma \in \mathbb{Z}[i]^n$$

where $\hat{B} = \gamma B$. Clearly, γ cannot be irrational, so we must be able to write $\gamma = p/q$ in lowest terms, where $p, q \in \mathbb{Z}[i]$ and $|p| > 1$. We see that p must divide every z_i and so

$$|\gcd\{z_1, \dots, z_n\}| > 1.$$

Note that p is not a multiple of $1+j$ because none of the z_i are. Therefore, with $\gamma = p$, each of the quotients z_i/p is also not divisible by $1+j$. Furthermore, we also see that, because of the properties of $\mathcal{S}$, the fact that the z_i are in $(1-j)\lambda\mathcal{S}$ implies that the quotients are also in this set, since $|p|^2 \geq 2$. Hence, the quotients are also admissible and so the necessary

condition for an acquisition error in the noiseless case is also a sufficient condition.

The procedure we used for obtaining an analytic expression for the blind acquisition performance of PAM, can be extended to this QAM case. Unfortunately we are limited in space, so we state the following theorem without proof. Numerical results are presented in Section VII.

Theorem 4: Let E represent the event that a ML decoding error is made on a series of noiseless observations y_i , $i = 1, \dots, n$, $n > 2$, of M -ary QAM symbols as defined by (6). If each source symbol is independent and uniformly distributed then

$$\lim_{\lambda \rightarrow \infty} \Pr\{E\} = 1 - \frac{1}{(1-2^{-n})\beta(n)\zeta(n)}.$$

where $\beta(s)$ is the *Dirichlet beta function*.

VI. A DECODING ALGORITHM

In this section, we discuss an algorithm for blind decoding of the received data. Our approach is inspired by the maximum-likelihood procedure, but is not necessarily ML.

Let us first revisit the ML procedure for PAM. We define the vector

$$\mathbf{z} = 2\mathbf{x} + \mathbf{1}.$$

From (8), we find that

$$\hat{A}_{\text{ML}} = \frac{\mathbf{y} \cdot \hat{\mathbf{z}}}{\hat{\mathbf{z}} \cdot \hat{\mathbf{z}}} = \frac{\|\mathbf{y}\| \cos \theta}{\|\hat{\mathbf{z}}\|}$$

where $\cdot$ here represents the dot (inner) product and θ is the angle between $\mathbf{y}$ and $\hat{\mathbf{z}}$. Substituting into (7), we find that

$$L_{\text{PAM}}(\hat{\mathbf{x}}, \hat{A} \mid \mathbf{y}) = -\mathbf{y} \cdot \mathbf{y} + \frac{(\mathbf{y} \cdot \hat{\mathbf{z}})^2}{\hat{\mathbf{z}} \cdot \hat{\mathbf{z}}} = -\|\mathbf{y}\|^2 \sin^2 \theta.$$

Hence, the maximum-likelihood procedure is to find the vector $\hat{\mathbf{z}}$ consisting only of odd-integer elements which lies closest to $\mathbf{y}$ in angle, under the additional constraint that each element of $\hat{\mathbf{z}}$ is less than M in absolute value.

Immediately, we can see that the ML procedure can be implemented, since the number of candidate $\hat{\mathbf{z}}$ vectors to test is finite. This is because of the constraint on the absolute values of the elements of $\hat{\mathbf{z}}$. The number of candidate vectors is M^n . Since this implies a running time for the algorithm which is exponential in the number of symbols, we seek some way of eliminating candidates from consideration *a priori*.

One way of achieving this is to notice that given any candidate, the volume in $\mathbb{R}^n$ that might contain superior candidates (candidates with higher likelihood) is a cone whose apex lies at the origin, whose principal axis is in the direction of $\mathbf{y}$, whose base is one of the walls of the cube $[-M+1, M-1]^n$ and on the surface of which lies the candidate $\hat{\mathbf{z}}$. Therefore, given any candidate, the search for a superior candidate can be expedited by restricting the search to the interior of the cone so defined. If a superior candidate is found, the cone is narrowed and the search repeated. When no superior candidate can be found, the candidate must be ML. This is a similar approach to that used for *sphere decoding* [7], and this might instead be called *cone decoding*. It is also an example of *simultaneous Diophantine*

approximation (with respect to the Euclidean norm; in the relative sense) [8]–[10].

Insofar as the similarity with sphere decoding extends, we note that the best known algorithms for sphere decoding which guarantee that the most likely candidate is found have a running time that is exponential in the dimension. Instead, we seek an algorithm with a running time that is polynomial in the dimension (number of symbols). For this reason, we propose a slightly different approach.

Unfortunately there is not enough space here to provide full details of the algorithm, however it is essentially a ‘nearest integer point’ problem which can be tackled using Babai’s algorithm [11]. While Babai’s algorithm does not guarantee that the nearest point will be found, it instead guarantees that a point will be found whose distance is within a known factor of the shortest distance. Importantly, it finds such a point in polynomial time.

VII. SIMULATION RESULTS

Simulations are now used to compare the theoretical results for decoding errors in the high SNR case against a practical implementation of our blind decoder. The performance of the Babai decoder was tested for 64-DEQAM, and a value $\epsilon = 1/99$ was used. Blind acquisition was performed based on a finite number of received symbols. Figure 1 presents results for the cases $n = 3$ to $n = 7$, and the SNR over a range from 28 dB to 66 dB. The acquisition algorithm simulation results are plotted with discrete symbols (and of course longer running-times would smooth out the points). The analytic limiting BERs derived using Theorem 4 are plotted as dotted horizontal lines. The BER is derived from the expression for $\Pr\{E\}$ by assuming that, when a decoding error is made on a block of symbols, we expect half the bits will be wrong, otherwise there will be, of course, no bit errors. Hence, the limiting BER is taken to be $\Pr\{E\}/2$.

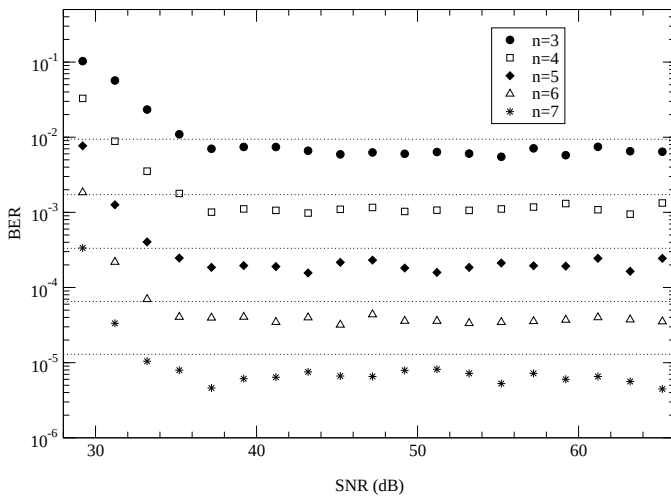


Fig. 1. Blind decoding performance for 64-DEQAM.

First, we observe that for each value of n , the simulations show the BER reaches its asymptotic (‘high SNR’) value for

SNRs less than 40 dB. Second, we observe that high SNR values for the simulated data are lower than those predicted. While this requires more investigation, the authors hypothesise that it is due to the finite constellation $M = 64$, where as the limiting BER was derived assuming an infinite size lattice.

VIII. CONCLUSIONS

This paper presented an analytic lower bound on the probability of correct acquisition for blind reception of PAM and ASK digital modulation signals, as a function of the number of measured symbols. QAM signals were also discussed, as was a new acquisition algorithm. The analytic expressions were shown to match simulated results. Extensions are possible to frequency selective channels and other modulation formats.

IX. ACKNOWLEDGEMENT

The authors would like to thank DANIEL RYAN for several useful suggestions which have improved this paper.

REFERENCES

- [1] Z. Ding and Y. G. Li, *Blind equalization and identification*. Marcel Dekker, Inc., 2001.
- [2] I. B. Collings, A. Logothetis, and V. Krishnamurthy, “Estimation of Markov modulated channels using the EM algorithm,” in *Proc. of the IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Paris, France, April 1997, pp. 405–408.
- [3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. Oxford University Press, 1979.
- [4] G. E. Collins and J. R. Johnson, “The probability of relative primality of Gaussian integers,” in *Symbolic and Algebraic Computation*, ser. Lecture Notes in Computer Science, vol. 358. Springer-Verlag, 1988, pp. 252–258.
- [5] N. Chen, Z. Chen, S. Liu, Y. Shen, and X. Ge, “Algebraic rings of integers and some 2D lattice problems in physics,” *J. Phys. A*, vol. 29, pp. 5591–5603, 1996.
- [6] S. D. Casey and B. M. Sadler, “Modifications of the Euclidean algorithm for isolating periodicities from a sparse set of noisy measurements,” *IEEE Trans. Signal Process.*, vol. 44, no. 9, pp. 2260–2272, Sept. 1996.
- [7] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,” *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.
- [8] J. W. S. Cassels, *An Introduction to Diophantine Approximation*. Cambridge University Press, 1957.
- [9] A. J. Brentjes, *Multi-Dimensional Continued Fraction Algorithms*, ser. Mathematical Centre Tracts. Amsterdam: Mathematisch Centrum, 1981, vol. 145.
- [10] I. V. L. Clarkson, “Approximation of linear forms by lattice points with applications to signal processing,” Ph.D. dissertation, The Australian National University, 1997.
- [11] L. Babai, “On Lovász’ lattice reduction and the nearest lattice point problem,” *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.