

Blind Detection of PAM and QAM in Fading Channels

Daniel J. Ryan, *Student Member, IEEE*,
 I. Vaughan L. Clarkson, *Senior Member, IEEE*, and
 Iain B. Collings, *Senior Member, IEEE*

Abstract—This correspondence considers block detection for blind wireless digital transmission. At high signal-to-noise ratio (SNR), block detection errors are primarily due to the received sequence having multiple possible decoded sequences with the same likelihood. We derive analytic expressions for the probability of detection ambiguity written in terms of a Dedekind zeta function, in the zero noise case with large constellations. Expressions are also provided for finite constellations, which can be evaluated efficiently, independent of the block length. Simulations demonstrate that the analytically derived error floors exist at high SNR.

Index Terms—Blind detection, block detection, error floor, fading, noncoherent communication, number theory, sequence detection, wireless communications.

I. INTRODUCTION

Reliable reception of digital signals over unknown fading channels has recently received significant attention especially for the case of the block-fading channel model. For example, under the assumption of transmitter co-operation, some elegant information-theoretic capacity results have been derived for noncoherent single or multiple-antenna systems at high SNR [1]–[3]. At low signal-to-noise ratio (SNR) it has been shown by numerical simulation that quadrature amplitude modulation (QAM) signaling can achieve near-capacity in the single-antenna noncoherent block Rayleigh-fading channel [4]. The challenge is to investigate the practical block error rates (BLER) which can be achieved.

The main problem with noncoherent reception is the inherent ambiguity associated with the joint estimation of channel and data. For example, in a block-flat-fading single-antenna noncoherent model, a detection ambiguity exists if one possible transmit-symbol sequence is a complex scalar multiple of another. Even in the absence of noise, two problems arise. First, there is the well known problem of *phase ambiguity* [5]. For example for rectangular QAM, because of the $\pi/2$ rotational symmetry there is no way to tell at the receiver which of four possible phases has been imposed by the channel.

The second problem is what we call *divisor ambiguity*. The simplest example is to be found in pulse-amplitude modulation (PAM). Consider Fig. 1(a), in which a simple 4-ary PAM constellation is depicted. If only the highlighted points of the constellation were selected for transmission in a particular block of data, it would be impossible at the receiver to decide between the correct channel amplitude and a value three times

smaller—even in the absence of noise. Confusion at the receiver about the correct divisor will lead to decoding error. In Fig. 1(b) and (c), we show how similar ambiguities can arise in both rectangular and hexagonal QAM; where now the ambiguous divisor is a complex number, meaning that the ambiguity can be of both amplitude and phase. The performance degradation due to sequence ambiguities was examined through simulation in [6] for BPSK in ISI channels. More recent work has included a technique proposed in [7] for QAM constellations.

In this correspondence we consider the probability of block detection error due to divisor ambiguities when transmitting over block-fading narrow-band channels. We derive analytical expressions for the BLER at high SNR of PAM, rectangular QAM, and a hexagonal QAM constellation representing the optimum sphere packing in two dimensions. These expressions have practical relevance for fast fading channels where the use of pilot symbols would severely limit the throughput and outweigh their usefulness for channel estimation, even at high SNR. Our analysis exploits the fact that these constellations can be represented as subsets of the rational, Gaussian or Eisenstein integers respectively. We first show that, in the absence of noise, a divisor ambiguity occurs only when the greatest common divisor of the (integer) transmit vector has a magnitude not equal to 1. By taking the limit as the constellation size goes to infinity, we derive BLER expressions in terms of a Dedekind zeta function of the sequence length. The probability of detection error thus decreases roughly exponentially with sequence length. We also derive exact expressions for finite sized constellations in terms of finite sums over the constellation points. Numerical evaluation indicates that these expressions converge to the infinite constellation size BLER as the block length increases. Interestingly, the convergence is not monotonic with increasing constellation size.

Finally, Monte Carlo simulation results are presented for the maximum likelihood (ML) noncoherent detector. The results show very good alignment with the theoretical expressions.

II. MATHEMATICAL BACKGROUND

First we present some elementary results in number theory. For more details see [8].

A. Gaussian and Eisenstein Integers

The Gaussian integers $\mathbb{Z}[i]$ are the set of all complex numbers $a + bi$ where both a and b are rational integers, and $i = \sqrt{-1}$. Like rational integers, they form a *unique factorization domain*, i.e., they can be uniquely factorized into prime factors. Any $z \in \mathbb{Z}[i]$ 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 $\pm i$. Primes related in such a way are called *associates*. Prime factorization is unique up to rearrangement of terms and substitution by associates.

The *Eisenstein integers* $\mathbb{Z}[\omega]$, are the set of all complex numbers $a + b\omega$ where a and b are rational integers and $\omega = \frac{1}{2}(-1 + i\sqrt{3})$. The units of the Eisenstein integers are $\pm 1, \pm\omega$ and $\pm(1 + \omega)$. The Eisenstein integers also form a unique factorization domain.

We use R to denote a ring of integers, and \mathbb{F}_R to denote an appropriate extension field of R , i.e., $\mathbb{F}_{\mathbb{Z}} = \mathbb{R}$, and $\mathbb{F}_{\mathbb{Z}[i]} = \mathbb{F}_{\mathbb{Z}[\omega]} = \mathbb{C}$.

B. Ideals

An *ideal* \mathfrak{I} is a subset of the ring of integers R with the properties that, when $a, b \in \mathfrak{I}$ and $r \in R$, then $a + b \in \mathfrak{I}$ and $ra \in \mathfrak{I}$. For the rational, Gaussian and Eisenstein integers, an ideal \mathfrak{I} can be represented by just one element, its *generator*. Given a generator g , the ideal is the set $\{kg \mid k \in R\}$. We use the notation $\langle g \rangle$ to represent the ideal generated by g . The generator is not unique if R has more than

Manuscript received March 4, 2005; revised August 3, 2005. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Adelaide, SA, Australia, September 2005, and as an Invited Paper at the Defense Applications of Signal Processing Workshop, Midway, UT, Mar. 2005. Part of this work was carried out while I. V. L. Clarkson was on study leave with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada.

D. J. Ryan is with the Telecommunications Laboratory, School of Electrical and Information Engineering, The University of Sydney, NSW 2006, Australia. He is also with Wireless Technologies Laboratory, CSIRO ICT Centre, Sydney, NSW 1710, Australia (e-mail: dan@ee.usyd.edu.au; daniel.ryan@csiro.au).

I. V. L. Clarkson is with the School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, Qld. 4072, Australia (e-mail: v.clarkson@itee.uq.edu.au).

I. B. Collings is with Wireless Technologies Laboratory, CSIRO ICT Centre, Sydney, NSW 1710, Australia (e-mail: iain.collings@csiro.au).

Communicated by X. Wang, Associate Editor for Detection and Estimation. Digital Object Identifier 10.1109/TIT.2005.864482

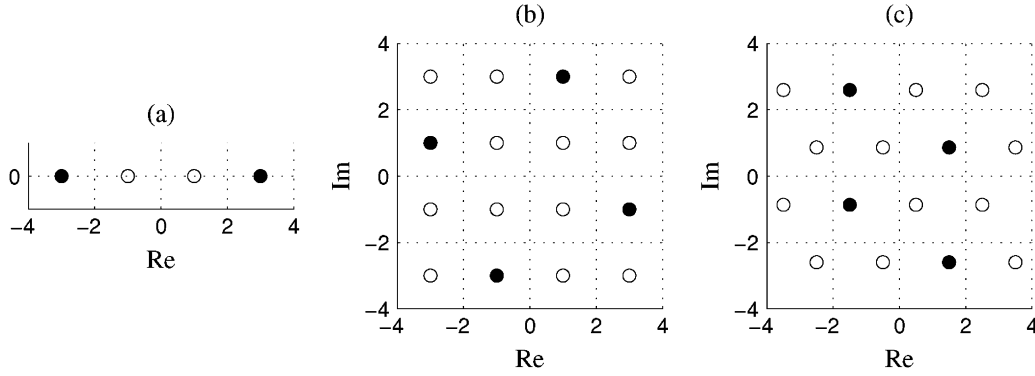


Fig. 1. Basic constellations and pathological sub-constellations (highlighted) that result in a divisor ambiguity, (a) quarterternary PAM, (b) 16-ary square QAM, and (c) 16-ary hexagonal QAM.

one unit, since multiplication by a unit yields another generator of the same ideal. Therefore in the rational integers, $\langle g \rangle = \langle -g \rangle$, and for the Gaussian integers, $\langle g \rangle = \langle -g \rangle = \langle ig \rangle = \langle -ig \rangle$.

We define the *norm* $N(\mathfrak{g})$ of an ideal $\mathfrak{g} = \langle g \rangle$ in the number-theoretic sense, for example, for the rational integers $N(\mathfrak{g}) = |g|$; for the Gaussian integers, $N(\mathfrak{g}) = |g|^2 = |a + bi|^2 = a^2 + b^2$, where $|\cdot|$ denotes absolute value¹ and here $g = a + bi$; and for the Eisenstein integers, $N(\mathfrak{g}) = |g|^2 = |a + b\omega|^2 = a^2 - ab + b^2$, where here $g = a + b\omega$.

Ideals can be multiplied by multiplying the generators, and therefore they can also be factorized. In fact, if R is a unique factorization domain, each ideal in R has a unique prime factorization into *prime ideals*. The prime ideals have prime generators.

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 will take care to exclude this zero ideal from consideration.

C. Zeta Functions

For the natural numbers the *Riemann zeta function* is defined for $s > 1$ as

$$\zeta(s) \triangleq \sum_{m=1}^{\infty} m^{-s}.$$

The *Dedekind zeta function* is a generalization of the Riemann zeta function defined over ideals of an arbitrary ring of integers R . It is defined as the infinite sum of ideals

$$\zeta_R(s) \triangleq \sum_{\mathfrak{m} \subseteq R} N(\mathfrak{m})^{-s} \quad (1)$$

for $s > 1$, where we use \sum^{\dagger} to indicate that the sum excludes $\langle 0 \rangle$.

From (1) the Dedekind zeta function defined over $R = \mathbb{Z}$ is

$$\zeta_{\mathbb{Z}}(s) = \sum_{\mathfrak{m} \subseteq \mathbb{Z}} N(\mathfrak{m})^{-s} = \zeta(s).$$

¹The notation $|\cdot|$ will also be used for sets, to indicate cardinality.

Similarly, the Dedekind zeta function defined over $R = \mathbb{Z}[i]$ is

$$\begin{aligned} \zeta_{\mathbb{Z}[i]}(s) &= \sum_{\mathfrak{m} \subseteq \mathbb{Z}[i]} N(\mathfrak{m})^{-s} \\ &= \sum_{a=1}^{\infty} \sum_{b=0}^{\infty} |a + bi|^{-2s} \\ &= \beta(s)\zeta(s) \end{aligned}$$

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

$$\beta(s) \triangleq \sum_{m=0}^{\infty} (-1)^m (2m+1)^{-s}.$$

Finally, the Dedekind zeta function defined over $R = \mathbb{Z}[\omega]$ is

$$\begin{aligned} \zeta_{\mathbb{Z}[\omega]}(s) &= \sum_{\mathfrak{m} \subseteq \mathbb{Z}[\omega]} N(\mathfrak{m})^{-s} \\ &= \sum_{a=1}^{\infty} \sum_{b=0}^{a-1} (a^2 - ab + b^2)^{-s} \\ &= L_{-3}(s)\zeta(s) \end{aligned}$$

where $L_{-3}(s)$ is a *Dirichlet L function* defined as

$$\begin{aligned} L_{-3}(s) &= \sum_{m=0}^{\infty} \frac{1}{(3m+1)^s} - \frac{1}{(3m+2)^s} \\ &= \sum_{m=1}^{\infty} \frac{2 \sin(\frac{2\pi m}{3})}{m^s}. \end{aligned}$$

D. The Möbius Function and Inversion Formula

When the ring of integers R is also a unique factorization domain such as \mathbb{Z} , $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$ by following [8] we can generalize the (*classical*) *Möbius function* and related theorems and identities, to be defined in terms of the ideals of R . We define the Möbius function as shown in the equation at the bottom of the page. A well-known identity that we now define in terms of ideals is that for $s > 1$,

$$\frac{1}{\zeta_R(s)} = \sum_{\mathfrak{m} \subseteq R} \mu(\mathfrak{m}) N(\mathfrak{m})^{-s}.$$

$$\mu(\mathfrak{m}) = \begin{cases} 0, & \text{if } \mathfrak{m} \text{ has one or more repeated prime ideal factors} \\ 1, & \text{if } \mathfrak{m} = \langle 1 \rangle \\ (-1)^k, & \text{if } \mathfrak{m} \text{ has } k \text{ unique prime ideal factors.} \end{cases}$$

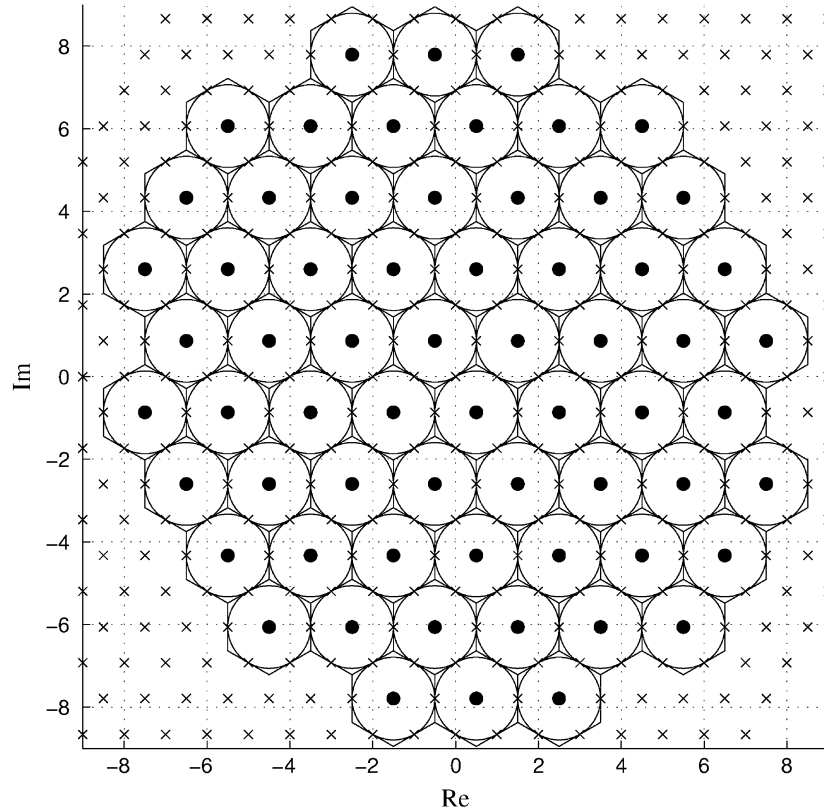


Fig. 2. Hexagonal 64-QAM constellation. Dots indicate constellation points. Crosses indicate other points in the hexagonal lattice. The hexagons are the Voronoi cells of the constellation and the circles are the corresponding sphere-packing.

There are a great number of inversion formulae associated with the Möbius function. We can obtain the following theorem for ideals, by following the same arguments in deriving Theorem 270 from [8] (see also [9]).

Theorem 1: Given functions A and B defined on the ideals of R

$$A(\mathbf{n}) = \sum_{\mathbf{m} \subseteq R} B(\mathbf{m}\mathbf{n})$$

if and only if

$$B(\mathbf{n}) = \sum_{\mathbf{m} \subseteq R} \mu(\mathbf{m})A(\mathbf{m}\mathbf{n}).$$

Also note that a function f is *multiplicative* if $f(\mathbf{m}\mathbf{n}) = f(\mathbf{m})f(\mathbf{n})$ whenever the greatest common divisor of \mathbf{m} and \mathbf{n} is $\langle 1 \rangle$. Consequently, we can also restate Theorem 3.1 of [10] in terms of ideals.

Theorem 2: If f is defined on ideals in R and f is multiplicative, then

$$\sum_{\mathbf{m} \subseteq R} f(\mathbf{m}) = \prod_{\mathbf{p} \text{ prime}} \sum_{k=0}^{\infty} f(\mathbf{p}^k)$$

whenever either side is absolutely convergent.

III. SYSTEM MODEL

A. Signal Model

We assume that at time t the transmitted symbol x_t is independently and uniformly chosen from a constellation $\mathcal{C} \subset R$, where for PAM

$R = \mathbb{Z}$, for rectangular QAM $R = \mathbb{Z}[i]$, and for hexagonal QAM $R = \mathbb{Z}[\omega]$.

For M -ary PAM, M is even and \mathcal{C} is the set of odd integers in the range $[-M+1, M-1]$. For rectangular QAM the points are taken from the complement of the ideal $\langle 1+i \rangle$. This is to aid our analysis, and is in contrast to the standard parametrization (i.e., as a subset of the Gaussian integers with odd real and imaginary components). Note that in our parametrization the rectangular constellation is rotated by 45° and the amplitude is scaled by a factor of $1/\sqrt{2}$. More specifically, $\mathcal{C} \subset \mathbb{Z}[i] \setminus \langle 1+i \rangle$, where $\mathfrak{c} \setminus \mathfrak{b}$ indicates the set of integers formed by taking the ideal \mathfrak{c} and excluding the ideal \mathfrak{b} . Note that the particular subset defines the constellation shape. For example, for square M -ary QAM, $x_t \in \mathbb{Z}[i] \setminus \langle 1+i \rangle$ with $|\operatorname{Re}\{x_t\}| + |\operatorname{Im}\{x_t\}| \leq \sqrt{M}-1$.

We also analyze a useful class of hexagonal QAM constellations. The hexagonal lattice provides the densest sphere packing in \mathbb{R}^2 or equivalently \mathbb{C} [11, p. 12], and thus is more power efficient than rectangular QAM [12]. The set of points of the hexagonal lattice on the complex plane is given by the set of Eisenstein integers $\mathbb{Z}[\omega]$. All points can be written in the form $x_t = a + b\omega$, where $a, b \in \mathbb{Z}$ and $\omega = \frac{1}{2}(-1 + \sqrt{3}i)$. In this correspondence, we examine the constellation formed from the subset $\mathbb{Z}[\omega] \setminus \langle 2 \rangle$ with the added restriction that if $x_t = a + b\omega \in \mathcal{C}$, then a is even and b is odd.² Fig. 2 shows an example 64-ary hexagonal QAM constellation satisfying these conditions.

For the purpose of analysis in the rectangular and hexagonal QAM cases we will also make the following technical assumption. Namely, that each x_t lies inside a region $\lambda\mathcal{S}$, where $\lambda > 0$ is an appropriate

²Note that there are at least two other natural ways to align hexagonal constellations in a coordinate system. The results we derive in this correspondence only apply to the alignment we are considering. However, corresponding results can be derived for other alignments by directly applying the same techniques.

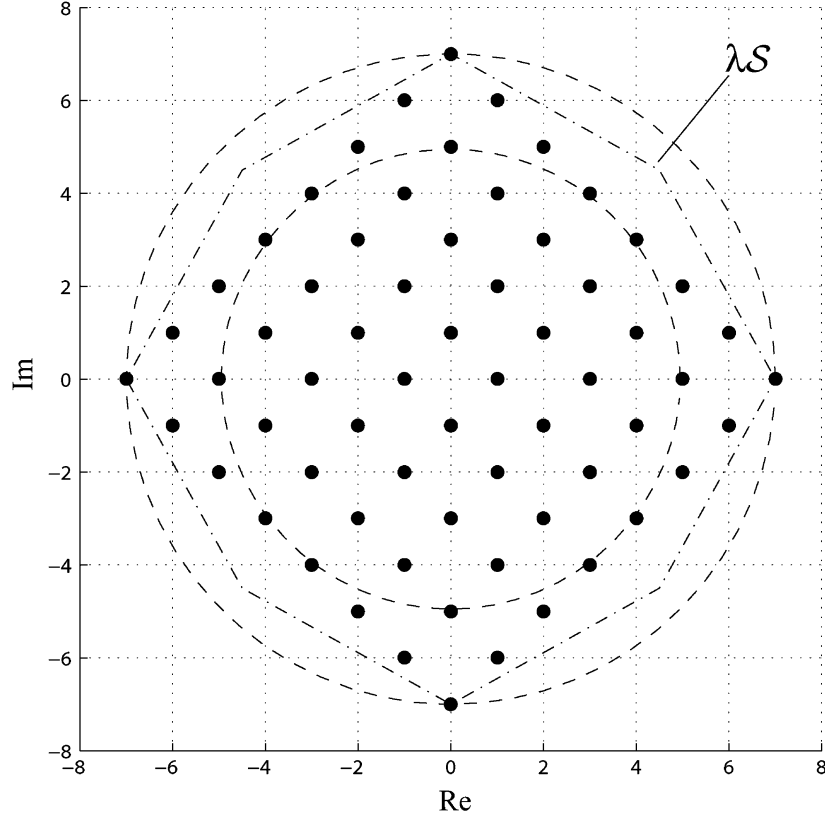


Fig. 3. 64-QAM constellation, with an appropriate choice of λS . The inner circle shows the region given by λ times the first condition on S , and the outer circle shows the region given by λ times the second condition on S . These regions correspond to $\lambda = 7$.

real scaling factor, and S is a region of the complex plane satisfying the following conditions:

- 1) $\alpha \in S$ for all $\alpha \in \mathbb{C}$ such that $|\alpha|^2 \leq \frac{1}{2}$ (inner circle condition);
- 2) $\alpha \notin S$ for all $\alpha \in \mathbb{C}$ such that $|\alpha|^2 > 1$ (outer circle condition);
- 3) the area of S exists, i.e., its indicator function is Riemann integrable.

Defining the boundaries of the constellation in this fashion allows us to incorporate all power-efficient rectangular QAM constellation shapes into our analysis, such as square, cross and circular constellations. Similarly, various hexagonal QAM constellation shapes can also be incorporated.

In Fig. 3, we plot \mathcal{C} for a square 64-QAM constellation (rotated and scaled, so as to be a subset of $\mathbb{Z}[i] \setminus \langle 1+i \rangle$), along with a possible choice of λS . The inner dashed circle corresponds to condition 1 scaled by λ . The outer dashed circle corresponds to the inner dashed circle scaled by λ . Clearly, S satisfies the three conditions. Moreover, note that all the points in \mathcal{C} lie in λS .

We consider flat fading channels with additive white Gaussian noise η_t , with variance σ^2 per real dimension in the PAM case, or per complex dimension otherwise. We assume that the channel h is constant for n symbols and thus we can write the channel output $\mathbf{y} = (y_1, \dots, y_n)^T$ in terms of the input sequence $\mathbf{x} = (x_1, \dots, x_n)^T$ as follows:

$$\mathbf{y} = h\mathbf{x} + \boldsymbol{\eta} \quad (2)$$

where $\boldsymbol{\eta} = (\eta_1, \dots, \eta_n)^T$, and for PAM h and η_t are real with $h > 0$, and for QAM h and η_t are complex. As mentioned previously, when h is complex there exists a phase ambiguity regardless of the number of symbols measured.

B. Detection

The log-likelihood function for PAM, rectangular QAM and hexagonal QAM is

$$L(\mathbf{y}; \mathbf{x}, h) = -\|\mathbf{y} - h\mathbf{x}\|^2 \quad (3)$$

where constant factors have been discarded and $\|\cdot\|$ represents the Euclidean norm of its argument. It follows that the ML estimate of h , given \mathbf{x} , is

$$\hat{h}_{\text{ML}} = \frac{\mathbf{x}^H \mathbf{y}}{\|\mathbf{x}\|^2} \quad (4)$$

where $(\cdot)^H$ denotes Hermitian transpose.

Therefore, the conditional ML estimate of \mathbf{x} (in the absence of training data) is given by

$$\begin{aligned} \hat{\mathbf{x}}_{\text{ML}} &= \arg \max_{\hat{\mathbf{x}} \in \mathcal{C}^n} L\left(\mathbf{y}; \hat{\mathbf{x}}, \frac{\hat{\mathbf{x}}^H \mathbf{y}}{\|\hat{\mathbf{x}}\|^2}\right) \\ &= \arg \max_{\hat{\mathbf{x}} \in \mathcal{C}^n} \frac{|\hat{\mathbf{x}}^H \mathbf{y}|}{\|\hat{\mathbf{x}}\|}. \end{aligned} \quad (5)$$

This data estimate is equivalent to that produced by the Generalized Likelihood Ratio Test [13].

We will assume that detection up to a phase ambiguity is a correct detection, and the phase ambiguity is resolved otherwise. Finally, for cases where there is more than one value of $\hat{\mathbf{x}}$ which maximizes (5), we will choose the estimate for which the corresponding \hat{h}_{ML} is largest.

IV. ASYMPTOTIC BLOCK ERROR RATE

Note that for any nonzero scalar $\beta \in \mathbb{F}_R$

$$\frac{|\mathbf{x}^H \mathbf{y}|}{\|\mathbf{x}\|} = \frac{|(\beta \mathbf{x})^H \mathbf{y}|}{\|\beta \mathbf{x}\|}.$$

Therefore, even in the absence of noise, the conditional-ML estimate is not unique if there exists an $\mathbf{x}' \in \mathcal{C}^n$ and $\gamma \in \mathbb{F}_R$ such that $\mathbf{x}' = \gamma \mathbf{x}$. It can easily be shown that this is the only condition for a nonunique estimate.

Recall that in the detection algorithm we have proposed, we choose the largest value of \hat{h} (or equivalently the smallest $\hat{\mathbf{x}}$), whenever there is a tie in the likelihood. Clearly, if $|\gamma| < 1$ the conditional-ML estimate would be chosen to be \mathbf{x}' , corresponding to a detection error.

To evaluate the probability of such errors occurring, we consider all (\mathbf{x}', γ) pairs which correspond to \mathbf{x} . Note that the elements of \mathbf{x}' and \mathbf{x} are in R , and as such γ must be rational and can be written in lowest terms $\gamma = p/q$. It follows that $\langle q \rangle | \langle x_t \rangle$ for all t . As discussed above detection errors occur when $\langle \gamma \rangle < 1$, and since p/q is in lowest terms, it corresponds to $|q| > |p| \geq 1$. Therefore, if a detection error occurs in the absence of noise then

$$\text{gci}\{\langle x_1 \rangle, \dots, \langle x_n \rangle\} \neq \langle 1 \rangle \quad (6)$$

where $\text{gci}\{\cdot\}$ is the greatest common ideal divisor or equivalently the *greatest common ideal (g.c.i.)* of its arguments. We now show that the reverse also holds; i.e., that (6) implies an error.

For PAM, notice that the g.c.i. of \mathbf{x} cannot have an even generator, since each of the x_t are odd. It follows that if $\langle g \rangle$ is the g.c.i. of \mathbf{x} then $g^{-1}\mathbf{x}$ has odd elements, and therefore $g^{-1}\mathbf{x} \in \mathcal{C}^n$. In other words, when $\langle g \rangle \neq \langle 1 \rangle$ there is another sequence $\mathbf{x}' = g^{-1}\mathbf{x}$ which also maximizes the likelihood function, and which has a larger corresponding channel estimate $\hat{h}'_{\text{ML}} = |g| \hat{h}_{\text{ML}}$. Since our detection algorithm chooses the sequence with the largest corresponding channel estimate, a detection error will occur. Thus (6) is also a sufficient condition for an error in the PAM case.

Similarly, for rectangular QAM, the g.c.i. of \mathbf{x} cannot be in $\langle 1+i \rangle$ since $x_t \in \mathbb{Z}[i] \setminus \langle 1+i \rangle$. Therefore, if $\langle g \rangle$ is the g.c.i. of \mathbf{x} , then $g^{-1}\mathbf{x}$ has elements in $\mathbb{Z}[i] \setminus \langle 1+i \rangle$. Note also that the smallest possible common ideal other than $\langle 1 \rangle$ has a generator with magnitude greater than or equal to $\sqrt{5}$. Therefore for $\langle g \rangle \neq \langle 1 \rangle$, we know that each element of $g^{-1}\mathbf{x}$ is inside the inner circle condition of the region $\lambda \mathcal{S}$ described in the previous section. Hence, $g^{-1}\mathbf{x} \in \mathcal{C}^n$, which will lead to a detection error. Therefore (6) is also a sufficient condition for an error to have occurred in the rectangular QAM case.

For hexagonal QAM, the g.c.i. of \mathbf{x} cannot be in $\langle 2 \rangle$ since $x_t \in \mathbb{Z}[\omega] \setminus \langle 2 \rangle$. As in the rectangular QAM case, if $\langle g \rangle$ is the g.c.i. of \mathbf{x} then $\mathbf{x}'' \triangleq g^{-1}\mathbf{x}$ has elements in $\mathbb{Z}[\omega] \setminus \langle 2 \rangle$, however it is not necessarily the case that \mathbf{x}'' has elements $x''_i = a''_i + b''_i \omega$ such that a''_i is even and b''_i is odd (as required for hexagonal QAM). However, there does exist a *unit* of the Eisenstein integers, u , such that $\mathbf{x}' = g^{-1}u\mathbf{x}$ has elements $x'_i = a'_i + b'_i \omega$ such that a'_i is even and b'_i is odd for all t . As before, note that the smallest possible common ideal other than $\langle 1 \rangle$ has a generator with magnitude greater than or equal to $\sqrt{3}$ in this hexagonal QAM case. Therefore for $\langle g \rangle \neq \langle 1 \rangle$, we know that each element of \mathbf{x}' is inside the inner circle condition of the region $\lambda \mathcal{S}$ described in the previous section. Hence, $\mathbf{x}' \in \mathcal{C}^n$ and a detection error occurs. Therefore (6) is also a sufficient condition for a detection error to have occurred in the hexagonal QAM case.

This leads us to the following theorem giving the probability of detection error in the absence of noise as a function of the sequence length. The following theorem applies to PAM, rectangular QAM and

hexagonal QAM and is a generalization of a result for rational integers [14, p. 523] and [15, Th. 3.1].

Theorem 3: Let E represent the event that a conditional-ML detection error is made on a series of n noiseless observations of M -ary PAM, rectangular QAM or hexagonal QAM symbols \mathbf{y} , as defined by (2). If each source symbol $x_t \in \mathcal{C} \subset R$ (where for PAM $R = \mathbb{Z}$, for rectangular QAM $R = \mathbb{Z}[i]$; and for hexagonal QAM $R = \mathbb{Z}[\omega]$) is independent and uniformly distributed, then

$$\lim_{\lambda \rightarrow \infty} \Pr\{E\} = 1 - \frac{1}{(1 - N(\mathfrak{o})^{-n} \zeta_R(n))}. \quad (7)$$

where for PAM and hexagonal QAM $\mathfrak{o} = \langle 2 \rangle$, and for QAM $\mathfrak{o} = \langle 1+i \rangle$. The scaling factor λ is defined for rectangular QAM and hexagonal QAM as in Section III, and for PAM $\lambda = M$.

Proof: Consider a random independently chosen sequence $x_t \in \mathcal{C} \subset R, t = 1, \dots, n$. Define $G = \text{gci}\{\langle x_1 \rangle, \dots, \langle x_n \rangle\}$. From the foregoing discussion, we know that a detection error can only occur when $G \neq \langle 1 \rangle$. Hence,

$$\Pr\{E\} = \Pr\{G \neq \langle 1 \rangle\} = 1 - \Pr\{G = \langle 1 \rangle\}. \quad (8)$$

Let $D_{\mathfrak{c}}$ be the event that the ideal \mathfrak{c} , divides each $\langle x_t \rangle$. We can relate $\Pr\{D_{\mathfrak{c}}\}$ to G as follows:

$$\Pr\{D_{\mathfrak{c}}\} = \sum_{\mathfrak{m} \subseteq R} \Pr\{G = \mathfrak{m}\mathfrak{c}\}.$$

Applying Theorem 1 gives

$$\Pr\{G = \mathfrak{c}\} = \sum_{\mathfrak{m} \subseteq R} \mu(\mathfrak{m}) \Pr\{D_{\mathfrak{m}\mathfrak{c}}\}. \quad (9)$$

Now, we are interested in the case $\mathfrak{c} = \langle 1 \rangle$ in the limit $\lambda \rightarrow \infty$, i.e.,

$$\lim_{\lambda \rightarrow \infty} \Pr\{G = \langle 1 \rangle\} = \lim_{\lambda \rightarrow \infty} \sum_{\mathfrak{m} \subseteq R} \mu(\mathfrak{m}) \Pr\{D_{\mathfrak{m}}\}.$$

In order to exchange limits and summation (on the right hand side of (9)), we apply the Weierstrass M -test to the summands. We show separately that the Weierstrass M -test is satisfied for PAM, rectangular QAM and hexagonal QAM in Appendices A, B and C respectively. Hence, limits and summation can be swapped and we have

$$\lim_{\lambda \rightarrow \infty} \Pr\{G = \langle 1 \rangle\} = \sum_{\mathfrak{c} \subseteq R} \lim_{\lambda \rightarrow \infty} \mu(\mathfrak{c}) \Pr\{D_{\mathfrak{c}}\}. \quad (10)$$

For PAM, rectangular QAM and hexagonal QAM

$$\lim_{\lambda \rightarrow \infty} \Pr\{D_{\mathfrak{c}}\} = \prod_{t=1}^n \lim_{\lambda \rightarrow \infty} \Pr\{\mathfrak{c} | \langle x_t \rangle\} \quad (11)$$

where the notation $\mathfrak{c} | \mathfrak{b}$ indicates that the ideal \mathfrak{c} divides the ideal \mathfrak{b} , i.e., that the points in \mathfrak{b} are contained in \mathfrak{c} .

As $\lambda \rightarrow \infty$, we have for PAM and rectangular QAM: $\mathcal{C} \rightarrow \langle 1 \rangle \setminus \mathfrak{o}$, where $\mathfrak{o} = \langle 2 \rangle$ for PAM, and $\mathfrak{o} = \langle 1+i \rangle$ for rectangular QAM. Therefore, as $\lambda \rightarrow \infty$, the probability that $\mathfrak{c} | \langle x_t \rangle$, is the ratio of density of points (which we define as the number of integers per unit volume) in $\mathfrak{c} \setminus \mathfrak{o}$ to the density of points in $\langle 1 \rangle \setminus \mathfrak{o}$.

For PAM and rectangular QAM, note that since an ideal \mathfrak{l} is a lattice with determinant $N(\mathfrak{l})$, the density of points of an ideal \mathfrak{l} on the plane

is $1/N(\mathfrak{I})$ [11]. Correspondingly, for \mathfrak{I} such that $\mathfrak{o} \nmid \mathfrak{I}$, the density of points of $\mathfrak{I} \setminus \mathfrak{o}$ is $1/(2N(\mathfrak{I}))$, and for \mathfrak{I} such that $\mathfrak{o} \mid \mathfrak{I}$ the density of points is zero. Therefore, for $\mathfrak{o} \nmid \mathfrak{c}$

$$\lim_{\lambda \rightarrow \infty} \Pr\{\mathfrak{c} \mid \langle x_t \rangle\} = \frac{2N(\langle 1 \rangle)}{2N(\mathfrak{c})} = \frac{1}{N(\mathfrak{c})}.$$

In the hexagonal QAM case, as $\lambda \rightarrow \infty$ the constellation \mathcal{C} approaches the set $\{x = a + b\omega \mid x \in \langle 1 \rangle \setminus \mathfrak{o}, a \text{ even}, b \text{ odd}\}$ where $\mathfrak{o} = \langle 2 \rangle$. The density of points of an ideal \mathfrak{I} on the complex plane in the above set is $4/(3\sqrt{3}N(\mathfrak{I}))$. Correspondingly, for \mathfrak{I} such that $\mathfrak{o} \nmid \mathfrak{I}$, the density of points of $\mathfrak{I} \setminus \mathfrak{o}$ in the above set is $4/(3\sqrt{3}N(\mathfrak{I}))$, and for \mathfrak{I} such that $\mathfrak{o} \mid \mathfrak{I}$ the density of points is zero. Therefore, for $\mathfrak{o} \nmid \mathfrak{c}$

$$\lim_{\lambda \rightarrow \infty} \Pr\{\mathfrak{c} \mid \langle x_t \rangle\} = \frac{3\sqrt{3}N(\langle 1 \rangle)}{4} \frac{4}{3\sqrt{3}N(\mathfrak{c})} = \frac{1}{N(\mathfrak{c})}.$$

which is the same expression derived for PAM and rectangular QAM. Therefore for PAM, rectangular QAM, and hexagonal QAM, we obtain from (11)

$$\lim_{\lambda \rightarrow \infty} \Pr\{D_{\mathfrak{c}}\} = \begin{cases} \left(\frac{1}{N(\mathfrak{c})}\right)^n, & \text{if } \mathfrak{o} \nmid \mathfrak{c} \\ 0, & \text{otherwise.} \end{cases} \quad (12)$$

Substituting (12) into (10) gives

$$\lim_{\lambda \rightarrow \infty} \Pr\{G = \langle 1 \rangle\} = \sum_{\mathfrak{c} \subseteq R} \mu(\mathfrak{c})d(\mathfrak{c})N(\mathfrak{c})^{-n} \quad (13)$$

where $d(\mathfrak{c}) = 0$ if $\mathfrak{o} \mid \mathfrak{c}$ and 1 otherwise.

Applying Theorem 2 gives

$$\lim_{\lambda \rightarrow \infty} \Pr\{G = \langle 1 \rangle\} = \prod_{\mathfrak{p} \text{ prime}} \sum_{m=0}^{\infty} \mu(\mathfrak{p}^m)d(\mathfrak{p}^m)N(\mathfrak{p})^{-nm} \quad (14)$$

$$= \prod_{\substack{\mathfrak{p} \text{ prime} \\ \mathfrak{p} \neq \mathfrak{o}}} (1 - N(\mathfrak{p})^{-n}) \quad (15)$$

$$= \left[\prod_{\substack{\mathfrak{p} \text{ prime} \\ \mathfrak{p} \neq \mathfrak{o}}} \frac{1}{1 - N(\mathfrak{p})^{-n}} \right]^{-1} \quad (16)$$

$$= \left[\prod_{\substack{\mathfrak{p} \text{ prime} \\ \mathfrak{p} \neq \mathfrak{o}}} \sum_{m=0}^{\infty} N(\mathfrak{p})^{-nm} \right]^{-1} \quad (17)$$

$$= \left[\sum_{\substack{\mathfrak{c} \subseteq R \\ \mathfrak{o} \nmid \mathfrak{c}}} N(\mathfrak{c})^{-n} \right]^{-1} \quad (18)$$

$$= \left[\sum_{\mathfrak{c} \subseteq R} N(\mathfrak{c})^{-n} - \sum_{\substack{\mathfrak{c} \subseteq R \\ \mathfrak{o} \mid \mathfrak{c}}} N(\mathfrak{c})^{-n} \right]^{-1} \quad (19)$$

$$= \left[(1 - N(\mathfrak{o})^{-n}) \sum_{\mathfrak{c} \subseteq R} N(\mathfrak{c})^{-n} \right]^{-1} \quad (20)$$

where (15) follows from (14) since it can be easily verified that the component functions $\mu(\cdot)$, $d(\cdot)$, and $N(\cdot)$ are multiplicative; (17) follows from (16) since $N(\mathfrak{p}) > 1$ for all \mathfrak{p} ; cross-multiplying the terms of (17) produces a summation over all elements in R such that $\mathfrak{o} \nmid \mathfrak{c}$ resulting in (18).

Substituting (20) into (8), and substituting the appropriate value of $N(\mathfrak{o})$ gives the result. \square

Note that (7) yields a very good approximation to the probability of a detection error for finite sized constellations, as will be demonstrated via numerical studies in Section VI.

Note that it is possible to make simple approximations to (7). Using (13) we see that for PAM

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

and hence, $\lim_{M \rightarrow \infty} \Pr\{E\} \approx 3^{-n}$. This indicates that the BLER is dominated by the probability that all the x_t are multiples of 3.

For rectangular QAM, we get $\lim_{\lambda \rightarrow \infty} \Pr\{E\} \approx 2 \cdot 5^{-n}$, hence the BLER is dominated by the probability that the x_t are all elements of either $\langle 2 + i \rangle$ or $\langle 1 + 2i \rangle$. For hexagonal QAM, we get $\lim_{\lambda \rightarrow \infty} \Pr\{E\} \approx 3^{-n}$, hence the BLER is dominated by the probability that the x_t are all elements of $\langle 2 + \omega \rangle$.

V. ANALYSIS FOR FINITE CONSTELLATIONS

We now present closed-form expressions of the probability of detection error in the zero noise case, for finite M . Naively, we could check all M^n possible transmitted sequences. However, this is infeasible for large n . We perform a counting argument, which is applicable to PAM and both QAM schemes and could easily incorporate a variety of lattice based codes.

We define $\mathcal{D}_{\mathfrak{c}}(\mathfrak{d})$ as the set

$$\mathcal{D}_{\mathfrak{c}}(\mathfrak{d}) \triangleq \{\mathfrak{q}; \mathfrak{q} \cap \mathcal{C} \neq \emptyset, \mathfrak{d} \mid \mathfrak{q}\} \quad (21)$$

for all \mathfrak{d} such that $\mathfrak{q} \cap \mathcal{C} \neq \emptyset$.

As discussed in Section IV, any transmitted sequence which has a g.c.i. not equal to $\langle 1 \rangle$ will result in a detection error. Equivalently, any transmitted sequence made up of the integers which are elements of $\mathcal{D}_{\mathfrak{c}}(\mathfrak{d})$ where $\mathfrak{d} \neq \langle 1 \rangle$ will result in a detection error, since the g.c.i. must then be divisible by \mathfrak{d} . The number of sequences of ideals of length n formed from $\mathcal{D}_{\mathfrak{c}}(\mathfrak{d})$ is $|\mathcal{D}_{\mathfrak{c}}(\mathfrak{d})|^n$ where here $|\cdot|$ denotes set cardinality.

We now proceed to count the total number of sequences resulting in a detection error. This is found by summing $|\mathcal{D}_{\mathfrak{c}}(\mathfrak{d})|^n$ over all possible divisors $\mathfrak{d} \neq \langle 1 \rangle$ and taking care to avoid counting a sequence multiple times, i.e.,

$$- \sum_{\substack{\mathfrak{d} \in \mathcal{C} \\ \mathfrak{d} \neq \langle 1 \rangle}} \mu(\mathfrak{d})|\mathcal{D}_{\mathfrak{c}}(\mathfrak{d})|^n \quad (22)$$

where the Möbius function is used to ensure each sequence is counted only once. The probability of detection error can be calculated by dividing (22) by the total number of sequences.

We are now able to state main results for PAM, rectangular QAM, and hexagonal QAM.

Lemma 1: Let E represent the event that a conditional-ML detection error is made on a series of n noiseless observations of M -ary PAM symbols \mathbf{y} , as defined by (2). If each source symbol $x_t \in \mathcal{C} \subset \mathbb{Z} \setminus \langle 2 \rangle$ is independent and uniformly distributed then

$$\Pr\{E\} = - \left(\frac{2}{M}\right)^n \sum_{\substack{d=3 \\ d \text{ odd}}}^{M-1} \mu(d) \left[\frac{M-1+d}{2d} \right]^n. \quad (23)$$

Proof: We first substitute the natural number d for \mathfrak{d} in (22) which is permissible since it is the generator for the ideal. For PAM, it can easily be shown that $|\mathcal{D}_{\mathfrak{c}}(d)| = \lfloor (M-1+d)/(2d) \rfloor$. To obtain $\Pr\{E\}$, we divide (22) by the total number of ideal sequences of length n which can be made from \mathcal{C} , which is $(M/2)^n$. \square

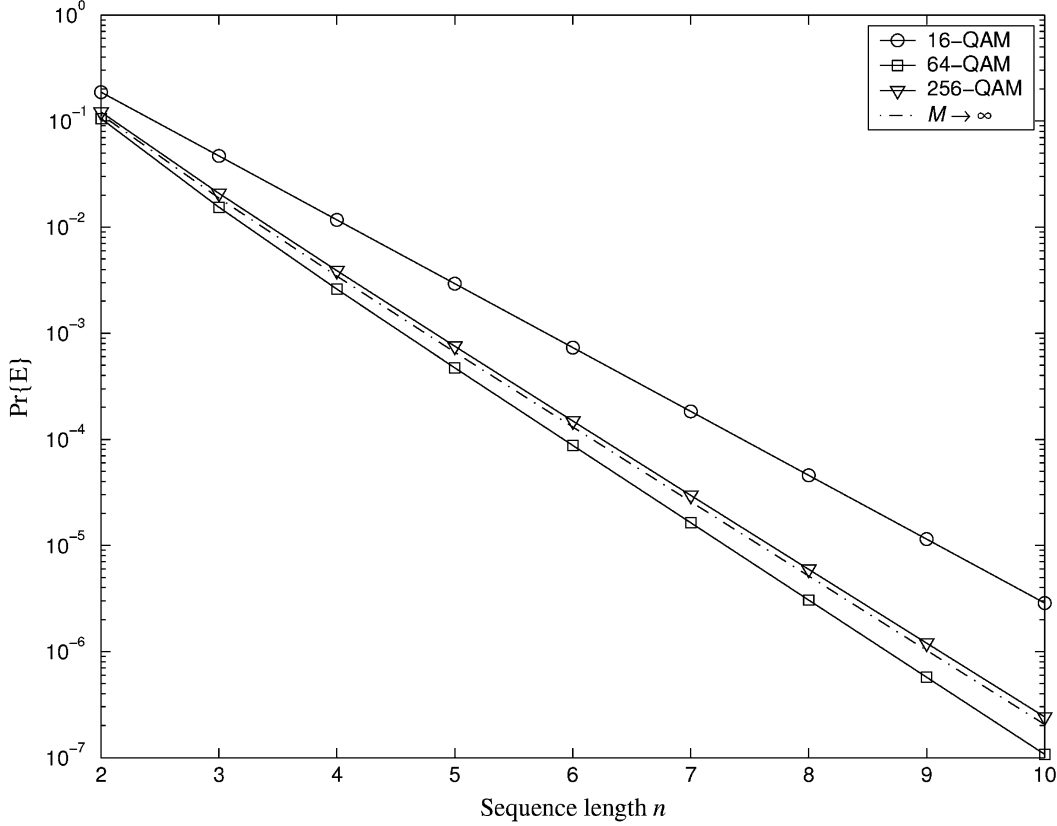


Fig. 4. $\Pr\{E\}$ for various M -ary square QAM modulation schemes.

Note that if we take the limit of (23) as $M \rightarrow \infty$ and assume that the limit and summation can be swapped, we obtain (the PAM case of) the asymptotic expression (13).

Lemma 2: Let E represent the event that a conditional-ML detection error is made on a series of n noiseless observations of M -ary rectangular QAM symbols \mathbf{y} as defined by (2) with the added condition that the rectangular QAM constellations are invariant to rotations of multiples of 90 degrees (i.e., if $x_t \in \mathcal{C}$ then $\alpha x_t \in \mathcal{C}$, where α is a unit of the Gaussian integers). If each source symbol $x_t \in \mathcal{C} \subset \mathbb{Z}[i] \setminus \{1 + i\}$ is independent and uniformly distributed then

$$\Pr\{E\} = - \left(\frac{4}{M} \right)^n \sum_{\substack{\mathfrak{d} \in \mathcal{C} \\ \mathfrak{d} \neq (1)}} \mu(\mathfrak{d}) |\mathcal{D}_{\mathcal{C}}(\mathfrak{d})|^n$$

where $\mathcal{D}_{\mathcal{C}}(\mathfrak{d})$ is given in (21).

Proof: For rectangular QAM, the cardinality of the set $\mathcal{D}_{\mathcal{C}}(\mathfrak{d})$ is calculated by brute force enumeration. To obtain $\Pr\{E\}$, we divide the number of error (ideal) sequences given in (22) by the total number of sequences of ideals of length n that can be made from \mathcal{C} , which is $(M/4)^n$. \square

Lemma 3: Let E represent the event that a conditional-ML detection error is made on a series of n noiseless observations of M -ary hexagonal QAM symbols \mathbf{y} as defined by (2) with the added condition that the hexagonal QAM constellations are invariant to rotations of 180° (i.e., if $x_t \in \mathcal{C}$ then $-x_t \in \mathcal{C}$). If each source symbol $x_t \in \mathcal{C}$ is independent and uniformly distributed then

$$\Pr\{E\} = - \left(\frac{2}{M} \right)^n \sum_{\substack{\mathfrak{d} \in \mathcal{C} \\ \mathfrak{d} \neq (1)}} \mu(\mathfrak{d}) |\mathcal{D}_{\mathcal{C}}(\mathfrak{d})|^n$$

where $\mathcal{D}_{\mathcal{C}}(\mathfrak{d})$ is given in (21).

Proof: The proof is identical to the previous lemma, with the exception that the total number of sequences of ideals of length n that can be made from \mathcal{C} is $(M/2)^n$. \square

By way of example, Fig. 4 shows $\Pr\{E\}$ versus sequence length n for various M -ary square QAM constellations. The limiting case $M \rightarrow \infty$ given by Theorem 3 is also plotted. Similar graphs can be obtained for PAM and hexagonal QAM. Clearly, as M increases, $\Pr\{E\}$ approaches the limiting case. Note that for a given sequence length n , $\Pr\{E\}$ is not a monotonic function of M , which ultimately relates to the distribution of primes. Recall at high SNR $\Pr\{E\}$ is intimately related to the ratio of the total number of ambiguous sequences to the total number of possible sequences. Therefore when a constellation increases in size, e.g., from 8-ary to 16-ary PAM, if the new constellation points are prime numbers then $\Pr\{E\}$ will go down, whereas if the new points are divisible by existing points then new ambiguous sequences will be introduced, as well as new unambiguous sequences, and $\Pr\{E\}$ will go up or down depending on the ratio.

It is worth noting that each of the expressions in this section can be numerically evaluated with a complexity which is independent of the block length.

VI. SIMULATION RESULTS

In this section we show that the asymptotic expressions match the Monte Carlo simulated performance of the exhaustive-search based ML noncoherent receiver. To avoid phase ambiguities we use differential encoding [5] within each block. We do not assume any knowledge of the fading distribution and therefore the SNR is taken as instantaneous, i.e., $\text{SNR} = |h|^2 \mathbb{E}[|x|^2] / \sigma^2$. Fig. 5 shows results for 64-ary square DEQAM, and sequence lengths of $n = 3$ to $n = 7$. Observe that for each value of n the analytic finite-size constellation values from Section V match the simulated BLER curves at high SNR. Note that

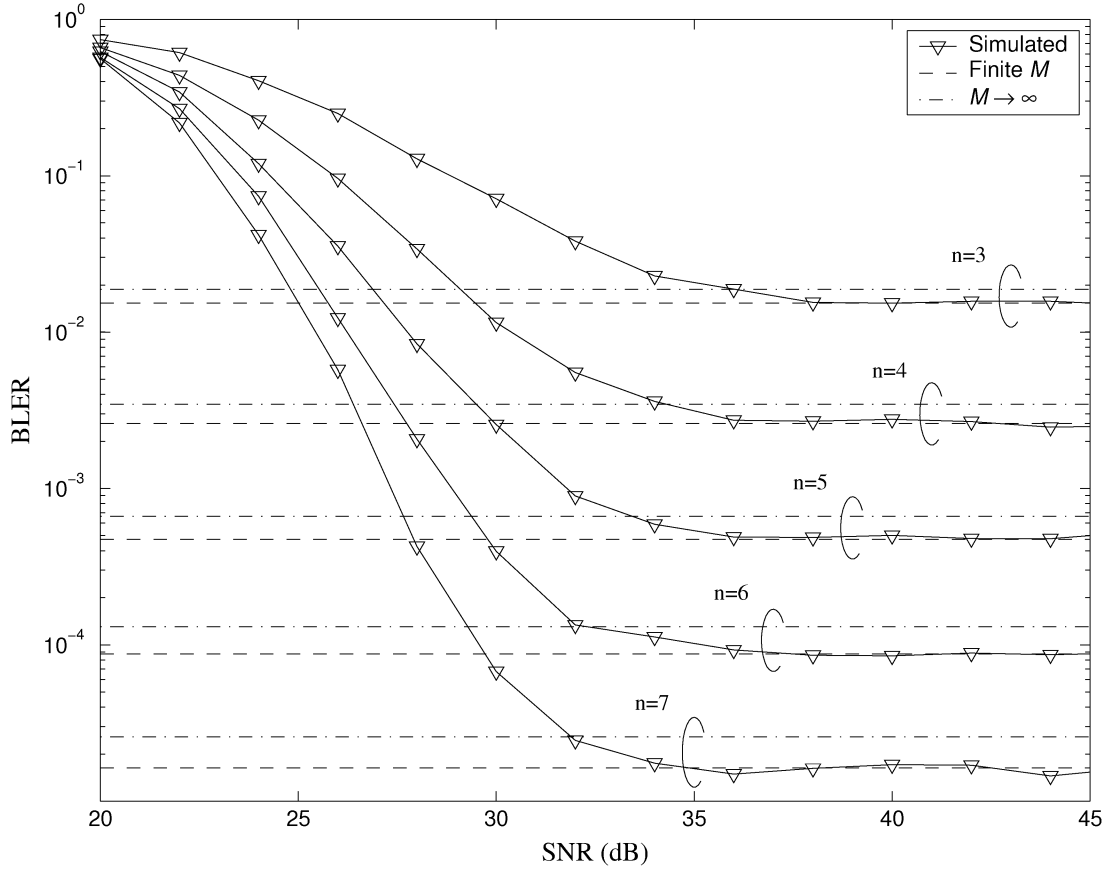


Fig. 5. Blind detection performance for 64-ary square DEQAM. The “ $M \rightarrow \infty$ ” curves are from Theorem 3, and the “Finite M ” curves are from Lemma 2.

the asymptotic BLERs decrease approximately exponentially for small increases in block length n . Although not shown, similar plots have confirmed the accuracy of the analysis for PAM and hexagonal QAM.

VII. CONCLUSION

This correspondence considered blind block detection for PAM and QAM. Fundamentally the performance is limited by the inherent ambiguities associated with jointly estimating the channel and the data, even in high SNR. Analytic expressions were derived for the BLER as the SNR tends to infinity, and were shown to be in terms of a Dedekind zeta function. We also presented BLER expressions for finite constellations which can be evaluated independent of the block length.

APPENDIX

A. Weierstrass M -Test for PAM Case

For PAM, we can calculate $D_{\mathbf{c}}$ for a given M using a simple counting argument, which gives

$$\Pr\{D_{\mathbf{c}}\} = \begin{cases} \left(\frac{2}{M} \left\lfloor \frac{M-1+|\mathbf{c}|}{2|\mathbf{c}|} \right\rfloor\right)^n, & \text{if } \langle 2 \rangle \nmid \mathbf{c} \\ 0, & \text{otherwise} \end{cases}$$

where we have set $a = |\mathbf{c}|$. Observe that

$$|\mu(\mathbf{c})\Pr\{D_{\mathbf{c}}\}| \leq \left(\frac{2}{M} \left\lfloor \frac{M-1+a}{2a} \right\rfloor\right)^n \leq \left(\frac{2}{a}\right)^n.$$

Now, when $n > 1$

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

Therefore, the Weierstrass M -test is passed and thus limits and summation can be swapped.

B. Weierstrass M -Test for QAM Case

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

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

For QAM, we have that

$$\Pr\{D_{\mathbf{c}}\} = \left[\frac{\sum_{x \in \mathbf{c} \setminus \langle 1+i \rangle} \Phi(\lambda \mathcal{S}, x)}{\sum_{x \in \mathbb{Z}[i] \setminus \langle 1+i \rangle} \Phi(\lambda \mathcal{S}, x)} \right]^n. \quad (24)$$

We seek simple expressions that bound the numerator of the fraction from above and its denominator from below. Consider the denominator. We have

$$\begin{aligned} & \sum_{x \in \mathbb{Z}[i] \setminus \langle 1+i \rangle} \Phi(\lambda \mathcal{S}, x) \\ & \geq \sum_{x \in \mathbb{Z}[i] \setminus \langle 1+i \rangle} \Phi\left(\left\{x \in \mathbb{C} \mid |x| \leq \frac{\lambda}{\sqrt{2}}\right\}, x\right) \\ & \geq \sum_{x \in \mathbb{Z}[i] \setminus \langle 1+i \rangle} \Phi\left(\left\{x = a + bi \in \mathbb{C} \mid |a| + |b| \leq \frac{\lambda}{\sqrt{2}}\right\}, x\right) \\ & = 4 \left[\frac{\lambda}{\sqrt{2}} + \frac{1}{2} \right]^2. \end{aligned}$$

It can easily be shown that for $v \geq 1$

$$\left[\frac{v}{2} + \frac{1}{2} \right] \geq \frac{v}{3}. \quad (25)$$

Therefore, since for any nonempty constellation $\lambda \geq 1/\sqrt{2}$ is valid

$$\sum_{x \in \mathbb{Z}[i] \setminus \langle 1+i \rangle} \Phi(\lambda \mathcal{S}, x) \geq 4 \left(\frac{\lambda}{3\sqrt{2}} \right)^2.$$

On the other hand, for the numerator, we have

$$\begin{aligned}
 & \sum_{x \in \mathcal{C} \setminus \{1+i\}} \Phi(\lambda \mathcal{S}, x) \\
 &= \sum_{x \in \mathbb{Z}[i] \setminus \{1+i\}} \Phi(\lambda \mathcal{S}, |c|x) \\
 &\leq \sum_{x \in \mathbb{Z}[i] \setminus \{1+i\}} \Phi\left(\left\{x \in \mathbb{C} \mid |x| \leq \frac{\lambda}{|c|}\right\}, x\right) \\
 &\leq \sum_{x \in \mathbb{Z}[i] \setminus \{1+i\}} \Phi\left(\left\{x = a + bi \mid |a| + |b| \leq \frac{\sqrt{2}\lambda}{|c|}\right\}, x\right) \\
 &= 4 \left[\frac{\frac{\sqrt{2}\lambda}{|c|}}{2} + \frac{1}{2} \right]^2 \\
 &\leq 4 \left(\frac{\sqrt{2}\lambda}{|c|} \right)^2
 \end{aligned}$$

where we used the fact that for $v \geq 0$

$$\left[\frac{v}{2} + \frac{1}{2} \right] \leq v$$

to obtain the final inequality. Hence, we have

$$\Pr\{D_{\mathbf{c}}\} \leq \left(\frac{6}{|c|} \right)^{2n} = \left(\frac{36}{N(\mathbf{c})} \right)^n.$$

Now, when $n > 1$, the limits and summation can be swapped, since

$$\begin{aligned}
 \sum_{\mathbf{c} \subseteq \mathbb{Z}[i]} \left(\frac{36}{N(\mathbf{c})} \right)^n &= 36^n \sum_{\mathbf{c} \subseteq \mathbb{Z}[i]} N(\mathbf{c})^{-n} \\
 &= 36^n \beta(n) \zeta(n) < \infty.
 \end{aligned}$$

C. Weierstrass M-Test for Hexagonal QAM

For hexagonal QAM, we have that

$$\Pr\{D_{\mathbf{c}}\} = \left[\frac{\frac{1}{3} \sum_{x \in \mathcal{C} \setminus \{2\}} \Phi(\lambda \mathcal{S}, x)}{\frac{1}{3} \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi(\lambda \mathcal{S}, x)} \right]^n$$

where the factor of $\frac{1}{3}$ comes about because for any $x \in \mathcal{C}$, exactly two of its six associates are in \mathcal{C} . As in the previous section, we seek simple expressions that bound the numerator of the fraction from above and its denominator from below. Consider the summation in the denominator. We have

$$\begin{aligned}
 & \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi(\lambda \mathcal{S}, x) \\
 &\geq \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi\left(\left\{x \in \mathbb{C} \mid |x| \leq \frac{\lambda}{\sqrt{2}}\right\}, x\right) \\
 &= \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi\left(\left\{x = a + b\omega \in \mathbb{C} \mid \sqrt{a^2 - ab + b^2} \leq \frac{\lambda}{\sqrt{2}}\right\}, x\right) \\
 &\geq \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi\left(\left\{x = a + b\omega \in \mathbb{C} \mid |a| + |b| \leq \frac{\lambda}{\sqrt{2}}\right\}, x\right) \\
 &= 2 \left[\frac{\frac{\lambda}{\sqrt{2}}}{2} + \frac{1}{2} \right]^2 \\
 &\geq 2 \left(\frac{\lambda}{3\sqrt{2}} \right)^2.
 \end{aligned}$$

On the other hand, for the numerator, we have

$$\begin{aligned}
 & \sum_{x \in \mathcal{C} \setminus \{2\}} \Phi(\lambda \mathcal{S}, x) \\
 &= \sum_{x \in \mathbb{Z}[\omega] \setminus \{w\}} \Phi(\lambda \mathcal{S}, |c|x) \\
 &\leq \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi\left(\left\{x \in \mathbb{C} \mid |x| \leq \frac{\lambda}{|c|}\right\}, x\right) \\
 &= \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi\left(\left\{x = a + b\omega \mid \sqrt{a^2 - ab + b^2} \leq \frac{\lambda}{|c|}\right\}, x\right) \\
 &\leq \sum_{x \in \mathbb{Z}[\omega] \setminus \{2\}} \Phi\left(\left\{x = a + b\omega \mid |a| + |b| \leq \frac{2\lambda}{|c|}\right\}, x\right) \\
 &= 2 \left[\frac{\frac{2\lambda}{|c|}}{2} + \frac{1}{2} \right]^2 \\
 &\leq 2 \left(\frac{2\lambda}{|c|} \right)^2.
 \end{aligned}$$

Hence, we have

$$\Pr\{D_{\mathbf{c}}\} \leq \left(\frac{6\sqrt{2}}{|c|} \right)^{2n} = \left(\frac{72}{N(\mathbf{c})} \right)^n.$$

Now, when $n > 1$, the limits and summation can be swapped, since

$$\begin{aligned}
 \sum_{\mathbf{c} \subseteq \mathbb{Z}[\omega]} \left(\frac{72}{N(\mathbf{c})} \right)^n &= 72^n \sum_{\mathbf{c} \subseteq \mathbb{Z}[\omega]} N(\mathbf{c})^{-n} \\
 &= 72^n \zeta_{\mathbb{Z}[\omega]}(n) < \infty.
 \end{aligned}$$

REFERENCES

- [1] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 139–157, Jan. 1999.
- [2] L. Zheng and D. N. C. Tse, "Communication on the Grassmann manifold: A geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 359–383, Feb. 2002.
- [3] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.
- [4] R.-R. Chen, R. Koetter, D. Agrawal, and U. Madhow, "Joint demodulation and decoding for the noncoherent block fading channel: A practical framework for approaching Shannon capacity," *IEEE Trans. Commun.*, vol. 51, no. 10, pp. 1676–1689, Oct. 2003.
- [5] W. E. Weber, "Differential encoding for multiple amplitude and phase shift keying systems," *IEEE Trans. Commun.*, vol. COM-26, no. 3, pp. 385–391, Mar. 1978.
- [6] K. M. Chugg, "Blind acquisition characteristics of PSP-based sequence detectors," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1518–1529, Oct. 1998.
- [7] D. Warrior and U. Madhow, "Spectrally efficient noncoherent communication," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 652–668, Mar. 2002.
- [8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. Oxford, U.K.: Oxford Univ. Press, 1975.
- [9] 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.
- [10] G. E. Collins and J. R. Johnson, "The probability of relative primality of Gaussian integers," in *Symbolic and Algebraic Computation (Lecture Notes in Computer Science)*. New York: Springer-Verlag, 1988, vol. 358, pp. 252–258.
- [11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed. New York: Springer-Verlag, 1993, p. 7.

- [12] G. D. Forney Jr., R. Gallager, G. Lang, F. Longstaff, and S. Qureshi, "Efficient modulation for band-limited channels," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 5, pp. 632–647, Sep. 1984.
- [13] H. L. Van Trees, *Detection, Estimation, and Modulation Theory: Part I*. New York: Wiley, 1968.
- [14] D. E. Knuth, *The Art of Computer Programming Volume 2: Seminumerical Algorithms*. Reading, MA: Addison-Wesley, 1969.
- [15] 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, Sep. 1996.

Robust Minimax Detection of a Weak Signal in Noise With a Bounded Variance and Density Value at the Center of Symmetry

Georgy Shevlyakov, *Member, IEEE*, and
Kiseon Kim, *Senior Member, IEEE*

Abstract—In practical communication environments, it is frequently observed that the underlying noise distribution is not Gaussian and may vary in a wide range from short-tailed to heavy-tailed forms. To describe partially known noise distribution densities, a distribution class characterized by the upper-bounds upon a noise variance and a density dispersion in the central part is used. The results on the minimax variance estimation in the Huber sense are applied to the problem of asymptotically minimax detection of a weak signal. The least favorable density minimizing Fisher information over this class is called the Weber–Hermite density and it has the Gaussian and Laplace densities as limiting cases. The subsequent minimax detector has the following form: i) with relatively small variances, it is the minimum L_2 -norm distance rule; ii) with relatively large variances, it is the L_1 -norm distance rule; iii) it is a compromise between these extremes with relatively moderate variances. It is shown that the proposed minimax detector is robust and close to Huber's for heavy-tailed distributions and more efficient than Huber's for short-tailed ones both in asymptotics and on finite samples.

Index Terms—Huber's M -estimators, least favorable distributions, non-Gaussian noise, robust minimum distance detection.

I. INTRODUCTION

Consider the problem of detection of a known signal θ in the additive independent and identically distributed (i.i.d.) noise $\{n_i\}_1^N$ with pdf f from a certain class \mathcal{F} . Given $\{x_i\}_1^N$, it is necessary to decide whether the signal θ is observed. This problem of binary detection is set up as the problem of hypotheses testing: $H_0 : x_i = n_i$ versus $H_1 : x_i = \theta + n_i$, $i = 1, \dots, N$. Given a pdf f , the classical theory of hypotheses testing yields various optimal (in the Bayesian, minimax, Neyman-Pearson senses) algorithms for the solution of this problem: all the optimal algorithms are based on the value of the likelihood ratio (LR) statistic $T_N(\mathbf{x}) = \prod_{i=1}^N f(x_i - \theta) / f(x_i)$ that must be compared with a certain threshold. The differences between the aforementioned approaches result only in the values of a threshold.

Manuscript received June 10, 2004; revised November 10, 2005. The material in this correspondence was presented in part at Nordic Radio Symposium 2004, Oulu, Finland, August 2004.

The authors are with the Department of Information and Communications, Gwangju Institute of Science and Technology, Gwangju 500-712, Korea (e-mail: shev@gist.ac.kr; kskim@gist.ac.kr).

Communicated by X. Wang, Associate Editor for Detection and Estimation. Digital Object Identifier 10.1109/TIT.2005.864462

In this correspondence, we consider the asymptotic weak signal approach when the useful signal θ decreases with sample size as $\theta = \theta_N = A/\sqrt{N}$ given some constant $A > 0$. For reasonable decision rules, the error probability then converges as $N \rightarrow \infty$ to a nonzero limit [6]. Moreover, within this approach, the error probability is closely related to the Pitman efficacy of the detector test statistic, and therefore, Huber's minimax theory can be used to analyze the detector [10]–[12]. Finally, since weak signals are on the border of not be distinguishable, and therefore, it is especially important to know the error probabilities.

In what follows, we deal with the following minimum distance detection rule [6]:

$$\sum_{i=1}^N \rho(x_i) \underset{H_0}{\overset{H_1}{\gtrless}} \sum_{i=1}^N \rho(x_i - \theta) \quad (1)$$

where $\rho(z)$ is a loss function characterizing the assumed form of a distance. This choice of a detection rule is mainly determined by the fact that it allows for the direct and simple use of Huber's minimax theory on M -estimators of location [7], [8]. Further, it can be seen that the choice $\rho(z) = -\log f(z)$ makes the optimal LR test statistic minimizing the Bayesian risk with equal costs and prior probabilities of hypotheses. Note, that in this case, it is necessary to know exactly the shape of pdf f to figure out the distance function, and the LR-statistics usually behave poorly under the departures from the assumed pdf model.

In many practical problems of radio-location, acoustics, and communications, noise distributions are only partially known. For instance, it may be known that either the underlying pdf is approximately Gaussian, or there is some information on its behavior in the central zone and on the tails, or an impulsive noise may distort the observed signal, etc. For these detection problems, some robust alternatives to the classical methods have been proposed in [8], [5], [10]–[12], [6], [4]. Recently, some of these approaches have been extended to more complicated static models of signals under the assumptions of the approximately Gaussian character of noise distributions [3], [18]. Heavy-tailed non-Gaussian noise models with finite and infinite variances both for static and dynamic systems are considered in many works, for example, in [2], [13], [16]. However, we are interested in a static model containing short-tailed noise pdfs with small variances as well as the heavy-tailed ones with large or even with infinite variances.

Within the minimax approach, the choice of a distribution class \mathcal{F} determines all the subsequent stages and the qualitative character of the corresponding robust procedure. In its turn, the choice of a distribution class depends either on the available prior information about data distributions, or on the possibilities of getting this information from the data sample.

Being historically the first [7], various ε -neighborhoods of the Gaussian distribution are not the only models of interest. In practice there often exists a prior information about the distribution dispersion in its central part and/or its tails, about the moments and/or subranges of a distribution. The empirical distribution function and relative estimators of a distribution shape (quantile functions and their approximations, histograms, kernel estimators) along with their confidence boundaries give other examples. In order to enhance efficiency of robust minimax procedures, it is reasonable to use such information in minimax settings by introducing the corresponding distribution classes. In Section II, we describe such a class.

We now dwell on the contributions of this paper. In [15], the distribution class with a bounded variance and density value at the center of symmetry, as well as some other classes with bounded distribution