LINEAR-TIME BLOCK NONCOHERENT DETECTION OF PSK

Robby G. McKilliam[1], *I. Vaughan L. Clarkson*[1], *Daniel J. Ryan*[2] *and Iain B. Collings*[3]

[1] School of Information Technology and Electrical Engineering, The University of Queensland, QLD 4067, AUSTRALIA,
{robertm,v.clarkson}@itee.uq.edu.au

[2] Dept. Elec. and Telecommuns. (IET), Norwegian Univ. of Science and Technology (NTNU), danryan@ieee.org

[3] Wireless Technologies Laboratory, CSIRO ICT Centre, NSW 2113, AUSTRALIA, iain.collings@csiro.au

ABSTRACT

We propose a new algorithm for noncoherent sequence detection of M-ary phase-shift-keying (M-PSK) symbols transmitted over a block fading channel. The algorithm is of complexity $O(T)$, where T is the sequence length, and is therefore computationally superior to existing maximum-likelihood (ML) detectors of complexity $O(T \log T)$. Our detector is based on a new approximation we propose to the noncoherent ML function. We show that by using this close approximation, the detection problem reduces to a nearest lattice point problem for the lattice A_n^*, from which we derive our $O(T)$ approach. Simulation results are provided that show the difference in bit error rate is negligibly small for a wide range of signal-to-noise ratios.

Index Terms— Differential phase shift keying, Mobile communication, Communication systems.

1. INTRODUCTION

We consider noncoherent detection of M-ary *phase shift keying* (M-PSK) symbols transmitted in the block fading channel. Noncoherent transmission is applicable to systems exhibiting small coherence intervals where regular transmission of pilot symbols is wasteful. Such situations typically occur in mobile communications [1, 2]. Moreover, as indicated by Chen *et al.* [1] standard coherent detection is, in a sense, inherently suboptimal because it only uses the energy of a small number of pilot symbols for channel estimation, rather than also exploiting the (typically larger) energy in the unknown data symbols. Other applications of noncoherent detection include recovery from deep fades in pilot-symbol assisted modulation based schemes, eavesdropping, and non-data-aided channel estimation [2].

A number of algorithms have been devised for the noncoherent detection of PSK. Wilson [3] and Makrakis and Feher [4] both propose algorithms of complexity $O(e^T)$ where T is the block length. Liu *et. al.* [5] describe a suboptimal algorithm that requires $O(T^2)$ arithmetic operations. Warrier and Madhow [6] describe an approximate ML algorithm that they claim to require $O(T)$ operations. It was shown by Sweldens [7] that the algorithm actually requires $O(T^2)$ operations in order for the approximation to remain valid as T increases.

Mackenthun [8] found an algorithm for ML noncoherent detection of M-PSK that required $O(T \log T)$ arithmetic operations. Later, Sweldens [7] rediscovered the same algorithm. More recently, low complexity algorithms for detection of multi-level modulation schemes such as PAM and QAM have been developed [2, 9].

Here we propose an approximation to the ML function for noncoherent detection of M-PSK. Allowing the approximation enables the detection problem to be represented as a nearest lattice point problem in the well studied lattice A_n^* [10–13]. Recently a linear-time nearest point algorithm for A_n^* was discovered [13]. We use this to create a noncoherent detector for M-PSK that requires $O(T)$ arithmetic operations. We refer to the new detector as the *lattice detector*.

Due to the approximation of ML function the lattice detector is not a ML detector. However, we show analytically that the approximation is close to the ML function for the range of signal-to-noise ratios of interest for M-PSK. We show by simulation that the lattice detector performs practically identically to the ML detector. The lattice detector is asymptotically less computationally intensive than the ML detector proposed by Mackenthun [8] and Sweldens [7].

2. NONCOHERENT BLOCK DETECTION

For M-PSK we define a codeword $\mathbf{u}$ as a vector of length T such $u_t \in \{0, 1, \cdots, M-1\}$. A block of M-PSK symbols is generated from a codeword by

$$x_t = \exp\left(\frac{2\pi j u_t}{M}\right) \tag{1}$$

where $j = \sqrt{-1}$ and $t \in \{0, 1, \ldots, T-1\}$. We write vectors and matrices in bold. The tth element in a vector is denoted by a subscript: x_t.

We consider transmitting a block of M-PSK symbols in the block fading channel

$$\mathbf{y} = h\mathbf{x} + \mathbf{n} \tag{2}$$

where h is a complex scalar representing the channel, $\mathbf{n}$ is white complex Gaussian noise and $\mathbf{y}$ is the received signal. The real and imaginary part of the n_t have variance σ^2.

The likelihood function derived from (2) is

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

where we recall that $\mathbf{x}$ is a function of $\mathbf{u}$. The ML estimate of h given $\mathbf{u}$ (or equivalently $\mathbf{x}$) can be found by differentiation and is given by [2]

$$\hat{h}_{\mathrm{ML}} = \frac{\mathbf{y}^\dagger\mathbf{x}}{\mathbf{x}^\dagger\mathbf{x}} = \frac{\mathbf{y}^\dagger\mathbf{x}}{T} \tag{4}$$

where † indicates the Hermitian transpose. Substituting (4) into (3) and simplifying we find that the ML estimate of $\mathbf{u}$, conditioned on the maximization w.r.t. h, is given by

$$\hat{\mathbf{u}}_{\mathrm{ML}} = \arg\max_{\mathbf{u}} |\mathbf{y}^\dagger\mathbf{x}|^2. \tag{5}$$

In the case that h is known then the ML estimate of $\mathbf{u}$ is

$$\hat{\mathbf{u}}_{\mathrm{ML}} = \left\lfloor \frac{M}{2\pi}(\angle\mathbf{y} - \mathbf{1}\angle h) \right\rceil \quad \bmod M \tag{6}$$

where $\angle(\cdot)$ denotes the complex argument and operates on vectors by taking the complex argument of each element and $\lfloor\cdot\rceil$ applied to a vector denotes the vector in which each element is rounded to a nearest integer[1] and $\mathbf{1} = (1,1,\dots,1)^\dagger$.

An important property of noncoherent detection of M-PSK is the ambiguity between the codewords $\mathbf{x}$ and $e^{2\pi kj/M}\mathbf{x}$ for $k \in \mathbb{Z}$. This is easily observed in (5) as

$$|\mathbf{y}^\dagger e^{2\pi kj/M}\mathbf{x}|^2 = |\mathbf{y}^\dagger\mathbf{x}|^2.$$

The ambiguities are typically resolved, for example, by using the phase of the last symbol from the previous codeword [1] or by differential encoding [8, 14]. We have chosen to use differential encoding in this paper. However, other schemes can be used.

We now briefly describe the ML detector found by Mackenthun [8] and Sweldens [7]. From (6) and the phase ambiguity of PSK constellations it is evident that the ML estimate of $\mathbf{u}$ is contained in the set

$$S = \left\{ \left\lfloor \frac{M}{2\pi}(\angle\mathbf{y} - \mathbf{1}\phi) \right\rceil \mid \phi \in [0, 2\pi/M] \right\}.$$

It can be shown that $|S| = T+1$. An ML estimator can then test each $\mathbf{u} \in S$ in turn and return the $\mathbf{u}$ that maximizes (5).

Both Mackenthun and Sweldens describe an algorithm that performs this procedure in $O(T\log T)$ operations. The algorithm sorts the $T+1$ elements so that the likelihood of each $\mathbf{u} \in S$ can be computed efficiently in a recursive manner. The complexity of the algorithm is asymptotically dominated by the sorting procedure that requires $O(T\log T)$ operations. The algorithm has many similarities with the nearest point algorithm for the lattice A_n^* described in [12].

[1] The direction of rounding for half-integers is not important. However, the authors have chosen to round up half-integers in their implementation.

3. THE LIKELIHOOD APPROXIMATION

In this section we derive an approximation to the ML function for the noncoherent detection of M-PSK (3). We show analytically that the approximate objective function is close to the ML function when σ^2 is sufficiently small. In Section 5 we show how maximizing the approximate function is equivalent to finding a nearest point in the lattice A_n^*.

Noting (6) define the approximate ML function

$$\begin{aligned} f(\mathbf{y};\hat{\mathbf{u}},\hat{h}) &= -\left\| \angle\mathbf{y} - \mathbf{1}\angle\hat{h} - \frac{2\pi\hat{\mathbf{u}}}{M} \right\|^2 \\ &= -\|\mathbf{z} - \mathbf{1}\theta - \hat{\mathbf{u}}\|^2 \end{aligned} \tag{7}$$

where $\mathbf{z} = {}^{M}\!/_{2\pi}\angle\mathbf{y}$ and $\theta = {}^{M}\!/_{2\pi}\angle\hat{h}$. We define the lattice detector to output

$$\hat{\mathbf{u}}_{\mathrm{lattice}} = \arg\max_{\hat{\mathbf{u}}} \max_{\hat{h}} f(\mathbf{y};\hat{\mathbf{u}},\hat{h}).$$

Whereas maximization of the ML function (3) amounts to choosing $\hat{\mathbf{u}}$ and $\hat{h}$ such that the Euclidean distance between $\mathbf{y}$ and $\hat{h}\hat{\mathbf{x}}$ is minimized, the lattice detector in (7) chooses $\hat{\mathbf{u}}$ and $\hat{h}$ such that the the Euclidean distance between the *complex arguments* of $\mathbf{y}$ and $\hat{h}\hat{\mathbf{x}}$ is minimized. Intuitively, we expect (3) and (7) to be closely related. We formally quantify this relationship in the remainder of this section.

Firstly note that (3) can be rewritten as

$$\begin{aligned} L(\mathbf{y};\hat{\mathbf{u}},\hat{h}) &= -\|\mathbf{y}\|^2 + 2\,\mathrm{Re}(\hat{h}\mathbf{y}^\dagger\hat{\mathbf{x}}) - |\hat{h}|^2\|\hat{\mathbf{x}}\|^2 \\ &= 2\,\mathrm{Re}\left(\hat{h}\mathbf{y}^\dagger\hat{\mathbf{x}}\right) - |\hat{h}|^2 T \\ &= 2|\hat{h}|\sum_{t=1}^{T}|y_t|\cos(\delta_t) - |\hat{h}|^2 T \\ &= 2|\hat{h}|\sum_{t=1}^{T}|y_t|\left(1 - \frac{\delta_t^2}{2} + O(\delta_t^4)\right) - |\hat{h}|^2 T \end{aligned}$$

by letting $\delta_t = \angle\hat{x}_t + \angle\hat{h} - \angle y_t$ and by taking the Taylor series expansion for cos and dropping the constant term $-\|\mathbf{y}\|^2$. At 'strong' peaks in $L(\mathbf{y};\hat{\mathbf{u}},\hat{h})$ the δ_t are small and $\delta_t^2 \gg O(\delta_t^4)$. Then the ML function is well approximated by

$$\begin{aligned} L(\mathbf{y};\hat{\mathbf{u}},\hat{h}) &\approx 2|\hat{h}|\sum_{t=1}^{T}|y_t|\left(1 - \frac{\delta_t^2}{2}\right) - |\hat{h}|^2 T \\ &= 2|\hat{h}|\sum_{t=1}^{T}|y_t|\left(1 - \frac{4\pi^2(\hat{u}_t + \theta - z_t)^2}{2M^2}\right) - |\hat{h}|^2 T. \end{aligned}$$

When σ^2 is small $|y_t| \approx |h|$ and we obtain

$$\begin{aligned} &\approx -\frac{4|\hat{h}|\pi^2}{M^2}\|\mathbf{z} - \mathbf{1}\theta - \hat{\mathbf{u}}\|^2 - |\hat{h}|^2 T + 2|\hat{h}|\sum_{t=1}^{T}|y_t| \\ &= \frac{4|\hat{h}|\pi^2}{M^2} f(\mathbf{y};\hat{\mathbf{u}},\hat{h}) - |\hat{h}|^2 T + 2|\hat{h}|\sum_{t=1}^{T}|y_t| = g(\mathbf{y};\hat{\mathbf{u}},\hat{h}). \end{aligned}$$

As $f(\mathbf{y};\mathbf{u},h)$ is independent of $|h|$ and because $g(\mathbf{y};\hat{\mathbf{u}},\hat{h})$ is an approximation to the ML function near 'strong' peaks and when σ^2 is small

$$\begin{aligned}\hat{\mathbf{u}}_{\mathrm{ML}} &\approx \arg\max_{\hat{\mathbf{u}}}\max_{\hat{h}} g(\mathbf{y};\hat{\mathbf{u}},\hat{h}) \\ &= \arg\max_{\hat{\mathbf{u}}}\max_{\hat{h}} f(\mathbf{y};\hat{\mathbf{u}},\hat{h}) = \hat{\mathbf{u}}_{\mathrm{lattice}}.\end{aligned}$$

We see that the lattice detector will be a close approximation to the ML detector when σ^2 is small. In Section 6 it is shown that the requirement that σ^2 is small is not very restrictive in practice. The lattice detector performs very similarly to the ML detector for the range of signal-to-noise ratios of interest for PSK.

4. THE LATTICE A_N^*

A lattice, L, is a set of points in $\mathbb{R}^n$ such that

$$L = \{\mathbf{v} \in \mathbb{R}^n | \mathbf{v} = \mathbf{B}\mathbf{w}, \mathbf{w} \in \mathbb{Z}^n\}$$

where $\mathbf{B}$ is termed the *generator matrix*. The cubic lattice $\mathbb{Z}^n$ is the set of n dimensional vectors with integer elements. The lattice A_n^* can be defined as the projection of the cubic lattice $\mathbb{Z}^{n+1}$ onto the hyperplane orthogonal to $\mathbf{1}$. This is,

$$A_n^* = \left\{\mathbf{Q}\mathbf{w} \mid \mathbf{w} \in \mathbb{Z}^{n+1}\right\} \tag{8}$$

where $\mathbf{Q}$ is the projection matrix

$$\mathbf{Q} = \left(\mathbf{I} - \frac{\mathbf{1}\mathbf{1}^\dagger}{n+1}\right) \tag{9}$$

and $\mathbf{I}$ is the $(n+1)\times(n+1)$ identity matrix. It follows that $\mathbf{Q}$ is the generator matrix for A_n^*.

The nearest lattice point problem is: Given $\mathbf{p} \in \mathbb{R}^n$ and some lattice L whose lattice points lie in $\mathbb{R}^n$, find the lattice point $\mathbf{v} \in L$ such that the Euclidean distance between $\mathbf{p}$ and $\mathbf{v}$ is minimized [10,15–17]. Van Emde Boas [18] and Ajtai [19] showed that the problem is NP-complete for general lattices. For certain lattices, the problem is considerably easier.

A number of algorithms to compute the nearest lattice point in the lattice A_n^* exist in the literature. Conway and Sloane [16] found an algorithm to compute the nearest point in $O(n^2 \log n)$ arithmetic operations. Later they improved this algorithm so that it required only $O(n^2)$ operations [17]. Clarkson [11] found an algorithm that required only $O(n \log n)$ operations and another algorithm requiring $O(n \log n)$ operation was found by some of the authors and Quinn [12]. Recently, a linear time algorithm was found by some of the authors and Smith and Quinn [13].

5. A_N^* AND THE LIKELIHOOD APPROXIMATION

For fixed $\mathbf{u}$, maximizing (7) with respect to θ we obtain $\hat{\theta} = \mathbf{1}^\dagger(\mathbf{z}-\mathbf{u})/T$. Substituting this estimate into (7) the likelihood function becomes

$$f(\mathbf{y};\hat{\mathbf{u}}) = -\|\mathbf{Q}\mathbf{z} - \mathbf{Q}\hat{\mathbf{u}}\|^2 \tag{10}$$

where $\mathbf{Q}$ is the projection matrix defined in (9). Since $\mathbf{Q}$ is the generator matrix for the lattice A_{T-1}^*, the maximization of (10) is achieved by choosing $\hat{\mathbf{u}}$ such that $\mathbf{Q}\hat{\mathbf{u}}$ is the nearest point in A_{T-1}^* to $\mathbf{Q}\mathbf{z}$. We can calculate $\hat{\mathbf{u}}$ in linear-time by using the nearest point algorithm for the lattice A_{T-1}^* described in [13] which we now discuss.

Like the $O(T\log T)$ algorithm of [7, 8] for noncoherent detection, the nearest lattice point problem for A_{T-1}^* can be solved using a sorting procedure of $O(T)$ elements [12, 13]. The complexity of sorting $O(T)$ elements is well-known to be $O(T\log T)$. However, for the nearest A_{T-1}^* lattice point problem it was shown in [13] that only a partial sort is required, where the elements are allocated into $O(T)$ 'buckets'. It was shown in [13] that due to the geometric properties of the lattice the nearest point can be found without further sorting each bucket. The complexity of this partial sort is only $O(T)$, and this results in a nearest lattice point algorithm of complexity $O(T)$. Therefore the complexity of our proposed algorithm is only $O(T)$. Note that this approach is in contrast to a standard bucket sort [20], where pathological cases of $\mathbf{z}$ may occur that result in a complexity of $O(T^2)$.

6. RESULTS

Simulations were run to compare the bit error rate (BER) of the lattice detector and the ML detector as the signal to noise ratio per bit (E_b/N_0) was varied from 2 dB to 10 dB. The block length was set to 4, 8 and 64 and $M = 4$. The channel, h, was generated such that $h = e^{j\phi}$ where ϕ is uniformly distributed in the range $[0, 2\pi)$.

Results are plotted in Figure 1. It is evident that there is negligible difference in performance between the lattice detector and the ML detector. Both detectors perform better than conventional 2 symbol differential detection. As T increases both detectors approach the performance of differentially encoded 4-PSK when perfect channel state information (CSI) is available.

Table 1 shows the practical computational performance of the lattice detector and the Mackenthun/Sweldens ML detector. The lattice detector appears to be be roughly twice as fast as the Mackenthun/Sweldens detector. This performance gap is expected to increase as T increases to reflect that the that lattice detector requires $O(T)$ operations whereas the Mackenthun/Sweldens detector requires $O(T\log T)$ operations. The computer used is an Intel Core2 running at 2.4GHz. The software is written in Java.

7. CONCLUSION

In this paper we have derived a linear-time noncoherent detector for M-PSK signals. We propose an objective func-

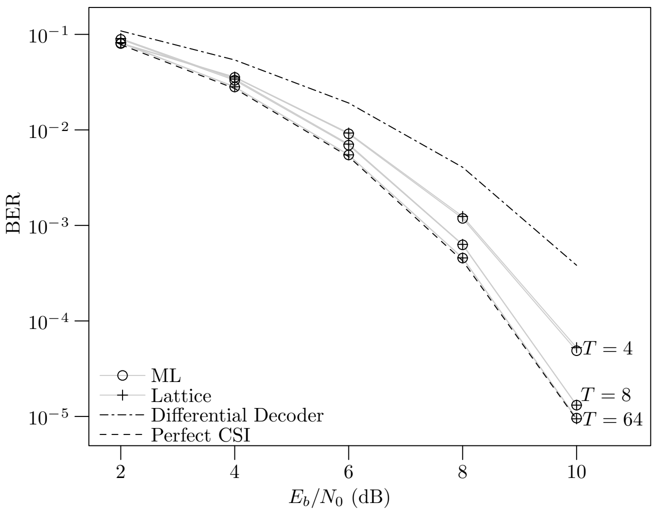

Fig. 1. Bit Error Rate (BER) versus E_b/N_0.

Table 1. Computation Time in seconds for 10^5 trials

Estimator	T=8	T=64	T=256
Lattice	2.77	9.67	33.62
ML Mac/Swe	3.87	17.16	63.72

tion that is an approximation to the ML function. We show that maximization of the objective function amounts to finding the nearest lattice point in the lattice A_n^*. Using a linear-time nearest point algorithm for A_n^* [13] we derive an algorithm for noncoherent detection of M-PSK that requires only $O(T)$ arithmetic operations where T is the block length. We show analytically that the objective function is a close approximation to the ML function. We show by simulation that the lattice detector performs practically identically to the ML detector. The lattice detector is computationally superior to existing ML detectors that require $O(T \log T)$ arithmetic operations [7, 8].

8. REFERENCES

[1] 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.

[2] D. J. Ryan, I. V. L. Clarkson, and I. B. Collings, "GLRT-optimal noncoherent lattice decoding," *IEEE Trans. Signal Process.*, vol. 55, pp. 3773–3786, July 2007.

[3] S. G. Wilson, J. Freebersyser, and C. Marshall, "Multi-symbol detection of MPSK," *Proc. IEEE GLOBECOM*, pp. 1692–1697, Nov. 1989.

[4] D. Makrakis and K. Feher, "Optimal noncoherent detection of PSK signals," *Electronics Letters*, vol. 26, no. 6, pp. 398–400, Mar. 1990.

[5] J. Liu, J. Kim, S. C. Kwatra, and G. H. Stevens, "An analysis of the MPSK scheme with differential recursive detection (DRD)," *Proc. IEEE Conf. on Veh. Tech.*, pp. 741–746, May 1991.

[6] D. Warrier and U. Madhow, "Spectrally efficient noncoherent communication," *IEEE Trans. Inform. Theory*, vol. 48, no. 3, pp. 651–668, Mar. 2002.

[7] W. Sweldens, "Fast block noncoherent decoding," *IEEE Comms. Letters*, vol. 5, no. 4, pp. 132–134, Apr. 2001.

[8] K.M. Mackenthun, "A fast algorithm for multiple-symbol differential detection of MPSK," *IEEE Trans. Commun.*, vol. 42, pp. 1471–1474, Feb/Mar/Apr 1994.

[9] R. G. McKilliam, D. J. Ryan, I. V. L. Clarkson, and I. B. Collings, "An improved algorithm for optimal noncoherent QAM detection," *Proc. Australian Commun. Theory Workshop*, pp. 64–68, Jan. 2008.

[10] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer, 3rd edition, 1998.

[11] I. V. L. Clarkson, "An algorithm to compute a nearest point in the lattice A_n^*," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, Eds., vol. 1719 of *Lecture Notes in Computer Science*, pp. 104–120. Springer, 1999.

[12] R. G. McKilliam, I. V. L. Clarkson, and B. G. Quinn, "An algorithm to compute the nearest point in the lattice A_n^*," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4378–4381, Sep. 2008.

[13] R. G. McKilliam, I. V. L. Clarkson, W. D. Smith, and B. G. Quinn, "A linear-time nearest point algorithm for the lattice A_n^*," *International Symposium on Information Theory and its Applications*, 2008.

[14] W. J. Weber, "Differential encoding for multiple amplitude and phase shift keying systems," *IEEE Trans. Commun.*, vol. 26, pp. 385–391, Mar. 1978.

[15] 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.

[16] J. H. Conway and N. J. A. Sloane, "Fast quantizing and decoding and algorithms for lattice quantizers and codes," *IEEE Trans. Inform. Theory*, vol. 28, no. 2, pp. 227–232, Mar. 1982.

[17] J. H. Conway and N. J. A. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 41–50, Jan. 1986.

[18] P. van Emde Boas, "Another NP-complete partition problem and the complexity of computing short vectors in a lattice," Tech. Rep., Mathematisch Instituut, Roetersstraat 15, 1018 WB Amsterdam, The Netherlands, Apr. 1981.

[19] M. Ajtai, "The shortest vector problem in L^2 is NP-hard for randomized reductions," *in Proc. 30th ACM Symposium on Theory of Computing*, pp. 10–19, May 1998.

[20] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, MIT Press. and McGraw-Hill, 2nd edition, 2001.