In the Proc. of IEEE ISOC ITW2005 on Coding and Complexity; editor M.J. Dinneen; co-chairs U. Speidel and D. Taylor; pages 47-51

Bounds on the Performance of Sphere Decoding of Linear Block Codes

Mostafa El-Khamy, Haris Vikalo and Babak Hassibi
Electrical Engineering Department
California Institute of Technology
Pasadena, CA 91125, USA
E-mail: mostafa, hvikalo, hassibi @systems.caltech.edu

***Abstract*— A sphere decoder searches for the closest lattice point within a certain search radius. The search radius provides a tradeoff between performance and complexity. We derive tight upper bounds on the performance of sphere decoding of linear block codes. The performance of soft-decision sphere decoding on AWGN channels as well as that of hard-decision sphere decoding on binary symmetric channels is analyzed.**

I. Introduction

Maximum likelihood (ML) decoding of linear block codes is known to be NP-hard [1]. Fincke and Pohst (FP) [2] described a 'sphere decoder' algorithm for closest point search in lattices which could find the closest lattice point to the received vector without actually searching all the lattice points. A fast variation of it was given by Schnorr and Euchner [3]. Other efficient closest point search algorithms exist (for a survey see [4]). The sphere decoder algorithm was proposed for decoding lattice codes [5]. Recently, a *soft-decision* (SD) sphere decoder was used for joint detection and decoding of linear block codes [6]. A *hard decision* (HD) sphere decoder was proposed for decoding linear block codes over the binary symmetric channel (BSC) [7]. The decoding radius of the sphere decoder provides a tradeoff between performance and complexity.

Tight upper bounds on the performance of SD-ML decoding of linear block codes over additive white Gaussian noise (AWGN) channels were derived in the literature (e.g., [8], [9], [10] and references therein). A tight bound on the performance of the HD-ML decoder on the BSC is the Poltyrev bound [8].

In this paper, we find tight upper bounds on the performance of HD and SD sphere decoding of linear block codes when transmitted over the BSC and AWGN channels respectively. This is done in sections II and III respectively. The performance of sphere decoding of Reed Solomon codes is analyzed in section IV. In section V, the analytic bounds are compared to simulations. In section VI, we conclude the paper.

II. Upper bounds on the performance of soft decision Sphere Decoding

Through out this paper, $\mathbb{C}$ will denote an (n,k) binary linear code. Assuming that a codeword $\boldsymbol{c} \in \mathbb{C}$ is transmitted over a binary input AWGN channel, the received word is $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z}$, where $\boldsymbol{x} = \mathcal{M}(\boldsymbol{c})$, $\mathcal{M}(\boldsymbol{c}) \stackrel{\Delta}{=} 1 - 2\boldsymbol{c}$ is the BPSK modulation of $\boldsymbol{c}$ and $\boldsymbol{z} = [z_i]_{i=1}^n$ is the AWGN vector with variance σ^2.

A soft-decision sphere decoder with an Euclidean radius D, SSD(D), solves the following optimization problem,

$$\begin{aligned} \hat{\boldsymbol{c}} = \arg\min_{\boldsymbol{v}\in\mathbb{C}} \quad & \|\boldsymbol{y} - \mathcal{M}(\boldsymbol{v})\|^2 \\ \text{subject to} \quad & \|\boldsymbol{y} - \mathcal{M}(\boldsymbol{v})\|^2 \le D^2, \end{aligned} \tag{1}$$

where $\|\boldsymbol{x}\|$ is the Euclidean norm of $\boldsymbol{x}$. Such decoders include *list-decoders* that list all codewords whose modulated image is within an Euclidean distance D from the received vector y and choose the closest one.

Let $\mathcal{E}_D$ denote the event of error or failure of SSD(D), then the error plus failure probability, $P(\mathcal{E}_D)$ [1] is

$$P(\mathcal{E}_D) = P(\mathcal{E}_D|\mathcal{E}_{ML})P(\mathcal{E}_{ML}) + P(\mathcal{E}_D|\mathcal{S}_{ML})P(\mathcal{S}_{ML}), \tag{2}$$

where $\mathcal{E}_{ML}$ and $\mathcal{S}_{ML}$ denote the events of an ML error and an ML success respectively. Let $\epsilon = \|\boldsymbol{y} - \mathcal{M}(\boldsymbol{c})\|$, then an ML error results if there exists another codeword $\hat{\boldsymbol{c}} \in \mathbb{C}$ such that $\|\boldsymbol{y} - \mathcal{M}(\hat{\boldsymbol{c}})\| \le \epsilon$. Since limiting the decoding radius to D will not do better than ML decoding, then $P(\mathcal{E}_D|\mathcal{E}_{ML}) = 1$. Since $P(\mathcal{S}_{ML}) \le 1$, it follows that an upper bound on the decoding performance is

$$P(\mathcal{E}_D) \le P(\mathcal{E}_{ML}) + P(\mathcal{E}_D|\mathcal{S}_{ML}). \tag{3}$$

Let Ω_D be the Euclidean sphere of radius D centered around the transmitted codeword. The probability that the added white Gaussian noise will not lie in the sphere Ω_D is

$$P(\boldsymbol{z} \notin \Omega_D) = P\left(\chi_n > D^2\right) = 1 - \Gamma_r(n/2, D^2/2\sigma^2) \tag{4}$$

where $\chi_n = \sum_{i=1}^n z_i^2$ is a Chi-squared distributed random variable with n degrees of freedom. Let $\Gamma(x)$ denote the Gamma function, then the cumulative distribution function (CDF) of χ_v is given by the regularized Gamma function Γ_r [11],

$$\Gamma_r(v/2, w/2) = \begin{cases} \int_0^w \frac{t^{v/2-1}e^{-t/2}}{2^{v/2}\Gamma(v/2)}\mathrm{d}t, & w \ge 0; \\ 0, & w < 0. \end{cases} \tag{5}$$

Define $\bar{P}(\mathcal{E}_{ML})$ to be an upper bound on the SD-ML decoder error probability, then we have the following lemma,

Lemma 1: $P(\mathcal{E}_D) \le \bar{P}(\mathcal{E}_{ML}) + P(\boldsymbol{z} \notin \Omega_D)$.

[1] Through out this paper, $P(X)$ will denote the probability that the event X occurs.

Proof: Given an ML success, $\mathcal{E}_D$ will only be due to failures of the SSD(D) decoder, i.e.,

$$P(\mathcal{E}_D|\mathcal{S}_{ML}) = P(\|\boldsymbol{y} - \mathcal{M}(\boldsymbol{c})\| > D) = P(\boldsymbol{z} \notin \Omega_D),$$

where the last equality follows from the linearity of the code and without loss of generality one could assume that the all zero codeword was transmitted. By definition, $P(\mathcal{E}_{ML}) \leq \bar{P}(\mathcal{E}_{ML})$. By substituting in (3) we are done. ■

Lemma 1 provides a way to bound the performance of sphere decoding of linear block codes on a variety of channels where additive white Gaussian noise is added and for a variety of modulation schemes. (In this paper, we will concentrate on the case that a binary linear block code is BPSK modulated and transmitted over an AWGN channel.) If $\bar{P}(\mathcal{E}_{ML})$ is the union upper bound on the codeword error probability [12, Ch.8] for BPSK modulation on an AWGN channel, then

$$P(\mathcal{E}_D) \leq \sum_{w \geq 1} G_w Q(\sqrt{2\gamma R w}) + P(\boldsymbol{z} \notin \Omega_D), \qquad (6)$$

where G_w is the number of codewords with (binary) Hamming weight w, γ is the signal to noise ratio (SNR) and R is the rate of the code. Eq. 6 was used in [13] to bound the performance of a suboptimum decoder, used for soft decoding of Reed Solomon codes when their binary image is used for transmission. Lemma 1 implies that one could obtain a tighter upper bound on $P(\mathcal{E}_D)$ by tightening the bound on the ML error probability, $\bar{P}(\mathcal{E}_{ML})$.

Shannon's sphere packing bound [14] is a lower bound on the error probability where he showed that the Voronoi region of a codeword can be bounded by a right circular n-dimensional cone with the codeword on its axis. The Poltyrev tangential sphere bound (TSB) on the performance of the SD-ML decoder is calculated by,

$$P(\mathcal{E}_{ML}) \leq \min_{\theta} \left\{ P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\theta) + P(\boldsymbol{z} \notin V_\theta) \right\}, \qquad (7)$$

where V_θ is an n-dimensional right circular cone with a half angle θ whose central line passes through the transmitted codeword and whose apex is at an Euclidean distance $\sqrt{n}$ from the transmitted codeword. Let the minimum of the optimization problem in (7) be achieved at $\theta = \phi$, then the following upper bound is tighter than (6),

$$P(\mathcal{E}_D) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) + P(\boldsymbol{z} \notin V_\phi) + P(\boldsymbol{z} \notin \Omega_D). \quad (8)$$

For the TSB, the optimum angle ϕ is related to the radius $\sqrt{r_\phi}$ (see Fig. 1 or Fig. 2) by $\sqrt{r_\phi/n} = \tan(\phi)$, such that r_ϕ is the root of

$$\sum_{b=1}^{n} G'_b(r_o) \int_0^{\theta_b(r_o)} \sin^{n-3}(\vartheta) \mathrm{d}\vartheta = \mathcal{B} \qquad (9)$$

when solved for r_o [8], $\mathcal{B} \triangleq \frac{\sqrt{\pi}\Gamma(\frac{n-2}{2})}{\Gamma(\frac{n-1}{2})}$ and $\theta_b(r_o) \triangleq \cos^{-1}\left(\sqrt{\frac{b/r_o}{1-b/n}}\right)$. Define $\alpha_b(r_o) \triangleq r_o(1-b/n)$, $G'_b(r_o) = G_b$ if $b < \alpha_b(r_o)$ and $G'_b(r_o) = 0$ otherwise. Let z_1 be the component of the noise along the central axis of the cone with a probability distribution function (PDF) $\mathcal{N}(z_1) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-{z_1}^2/2\sigma^2}$ and z_2 be the noise component orthogonal to z_1. Define $\beta_{z_1}(b) \triangleq \frac{\sqrt{n}-z_1}{\sqrt{\frac{n}{b}-1}}$ and $r_{z_1}(\phi) \triangleq \sqrt{r_\phi}\left(1 - \frac{z_1}{\sqrt{n}}\right)$, then the ML error probability given that the noise $\boldsymbol{z}$ is in the cone V_ϕ is [8]

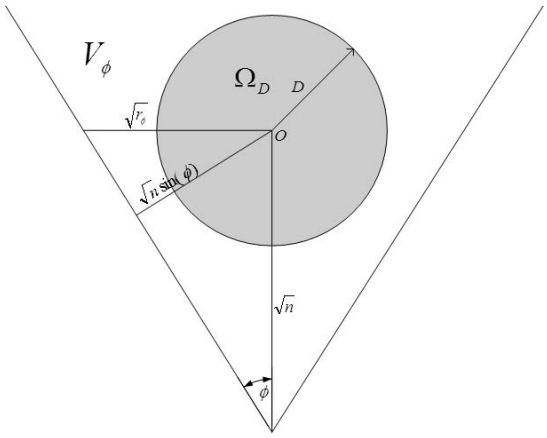

Fig. 1. *Case A:* The sphere Ω_D lies totally inside the Cone V_ϕ

$$P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) = \int_{-\infty}^{\infty} \mathcal{N}(z_1) \left[\sum_{b=1}^{n-1} G'_b(r_\phi) \int_{\beta_{z_1}(b)}^{r_{z_1}(\phi)} \mathcal{N}(z_2)\, \Gamma_r\left(\frac{n-2}{2}, \frac{r^2_{z_1}(\phi) - z_2^2}{2\sigma^2}\right) \mathrm{d}z_2 \right] \mathrm{d}z_1. \qquad (10)$$

A. A tight upper bound on the performance of SDD(D)

We observe that instead of directly substituting the TSB of (7) for $\bar{P}(\mathcal{E}_{ML})$ in Lem. 1 as we did in (8), a tighter upper bound than (8) could be found by noticing that the events $\{\boldsymbol{z} \notin V_\theta\}$ and $\{\boldsymbol{z} \notin \Omega_D\}$ are not in general mutually exclusive. This is shown in the following lemma.

Lemma 2: $P(\mathcal{E}_D)$ is upper bounded by $P(\mathcal{E}_D) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) + P(\boldsymbol{z} \notin \Omega_D) + P\left(\{\boldsymbol{z} \notin V_\phi\} \cap \{\boldsymbol{z} \in \Omega_D\}\right)$.

Proof: Using Bayes' rule and defining the region $\Lambda(\theta, D) \triangleq \{V_\theta \cap \Omega_D\}$ we get

$$\begin{aligned} P(\mathcal{E}_D) \leq \quad & \min_{\theta} \{ P(\mathcal{E}_D|\boldsymbol{z} \in \Lambda(\theta, D)) P(\boldsymbol{z} \in \Lambda(\theta, D)) \\ & + P(\mathcal{E}_D|\boldsymbol{z} \notin \Lambda(\theta, D)) P(\boldsymbol{z} \notin \Lambda(\theta, D)) \}. \end{aligned} \qquad (11)$$

From the definition of $\Lambda(\theta, D)$, it follows that $P(\mathcal{E}_D, \boldsymbol{z} \in \Lambda(\theta, D)) = P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Lambda(\theta, D)) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\theta)$, where the last inequality follows from that $\Lambda(\theta, D) \subseteq V_\theta$. Using $P(\mathcal{E}_D|\boldsymbol{z} \notin \Lambda(\theta, D)) \leq 1$, it follows that

$$\begin{aligned} P(\mathcal{E}_D) \quad & \leq \quad \min_{\theta} \left\{ P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\theta) + P(\boldsymbol{z} \notin \Lambda(\theta, D)) \right\} \\ & \leq \quad P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) + P(\boldsymbol{z} \notin \{V_\phi \cap \Omega_D\}). \end{aligned} \qquad (12)$$

The last inequality is due to the observation that ϕ does not necessarily minimize (12). By de Morgan's law, $\{V_\phi \cap \Omega_D\}^c = \{\Omega_D\}^c \cup \{\{V_\phi\}^c \cap \Omega_D\}$, $\{.\}^c$ is the complement of $\{.\}$. ■

We consider two cases;

Case A: The sphere Ω_D lies totally inside the cone V_ϕ. (See Fig. 1). This case is equivalent to the event $\mathbb{A} \triangleq \{D \leq D_\phi\}$, where

$$D_\phi = \sqrt{n}\sin(\phi), \tag{13}$$

and will be called the critical decoding radius. It follows that $P\left(\{\boldsymbol{z} \notin V_\phi\} \cap \{\boldsymbol{z} \in \Omega_D\}|\mathbb{A}\right) = 0$, which could be substituted in Lem. 2. Furthermore, since $\Lambda(\theta, D) = \Omega_D$, it follows from (11) that a tighter upper bound is

$$P(\mathcal{E}_D|\mathbb{A}) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_D) + P(\boldsymbol{z} \notin \Omega_D), \tag{14}$$

$P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_D) =$
$\sum_{\sqrt{b}<D} G_b \int_{\sqrt{b}}^{D} \mathcal{N}(z_o)\Gamma_r(\frac{n-1}{2}, \frac{D^2-z_o^2}{2\sigma^2})\mathrm{d}z_o.$

Let δ be the half angle at which the cone V_δ is tangential to the sphere Ω_D, $\delta = \sin^{-1}(D/\sqrt{n})$ (see Fig. 1), then another tight upper bound is

$$P(\mathcal{E}_D|\mathbb{A}) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\delta) + P(\boldsymbol{z} \notin \Omega_D). \tag{15}$$

Case B: The sphere Ω_D intersects the cone V_ϕ. (see Fig. 2). This could be divided into two cases depending on the position of the apex of the cone. The apex of the cone does not lie in the sphere when $\sqrt{n}\sin(\phi) < D < \sqrt{n}$ (see Fig. 2a), and lies in the sphere when $D \geq \sqrt{n}$ (see Fig. 2b). In both cases the following analysis holds. Let the origin, O, of the n-dimensional space be at the transmitted codeword which is also the center of Ω_D. Since the cone and the sphere are symmetrical around the central axis, we project on a two dimensional plane as in Fig. 2. The radial component of the noise (along the axis of the cone) is z_1. The altitudes $y_a(\phi, D)$ and $y_b(\phi, D)$ at which the (double) cone intersects the sphere are found by substituting the line equation $P = P_1 + u(P_2 - P1)$, where $P = (x, y)$, $P_1 = (0, \sqrt{n})$ and $P_2 = (2\sqrt{n}\tan(\phi), -\sqrt{n})$ into the quadratic equation of the sphere. Solving for u, it follows that

$$u_{a,b} = \frac{4n \pm \sqrt{16n^2 - 16n\sec^2(\phi)(n - D^2)}}{8n\sec^2(\phi)}, \tag{16}$$

and $y_{a,b}(\phi, D) = y_1 + u_{a,b}(y_2 - y_1) = \sqrt{n}(1 - 2u_{a,b})$. It is easy to check that at $D = \sqrt{n}$, $u_b = 0$ and y_b is at the apex of V_ϕ. If $D > \sqrt{n}$ then the intersection at y_b is in the lower nappe of the cone. It is also observed that V_ϕ and Ω_D do not intersect ($\Omega_D \subset V_\phi$) if $16n^2 < 16n\sec^2(\phi)(n - D^2)$ or equivalently $D < \sqrt{n}sin(\phi)$ which is Case A.

Define $\mathbb{B}$ to be the event $\mathbb{B} \triangleq \{D > \sqrt{n}\sin(\phi)\}$, $f_{n-1}(t)$ to be the PDF of $\chi_{n-1} = \sum_{i=2}^{n} z_i^2$, and $\omega_{z_1}^2 = D^2 - z_1^2$ (see Fig. 2). From Lem. 2 and (4), the error probability is upper bounded by $P(\mathcal{E}_D|\mathbb{B}) \leq$

$$P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) + P(\boldsymbol{z} \notin \Omega_D) + P\left(\{\boldsymbol{z} \notin V_\phi\} \cap \{\boldsymbol{z} \in \Omega_D\}|\mathbb{B}\right),$$

such that $P\left(\{\boldsymbol{z} \notin V_\phi\} \cap \{\boldsymbol{z} \in \Omega_D\}|\mathbb{B}\right) =$

$$\int_{y_a(\phi,D)}^{y_b(\phi,D)} \mathcal{N}(z_1) \int_{r_{z_1}^2(\phi)}^{\omega_{z_1}^2} f_{n-1}(t)\mathrm{d}t\mathrm{d}z_1.$$

To summarize the tight upper bound is given in the following theorem,

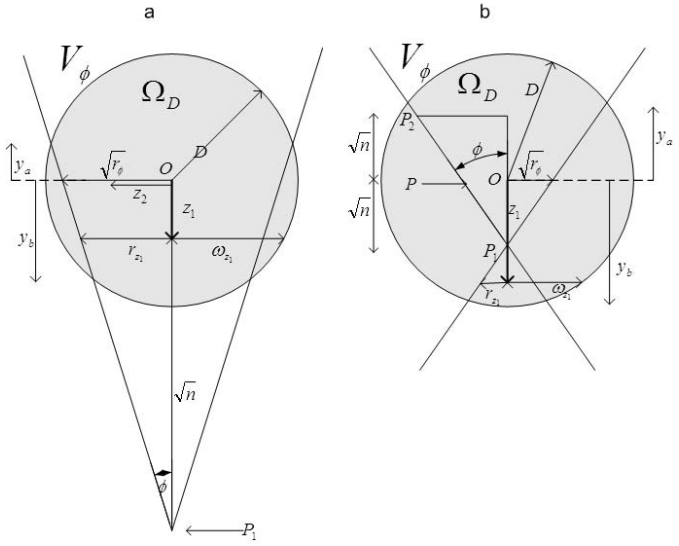

Fig. 2. *Case B:* The sphere Ω_D intersects the cone V_ϕ; the apex of the cone V_ϕ lies (a) outside the sphere Ω_D, (b) inside the sphere Ω_D.

Theorem 3: The performance of the soft decision sphere decoder with an Euclidean decoding radius D on an AWGN channel with noise variance σ^2 is upper bounded by:

A) *If $D \leq \sqrt{n}\sin(\phi)$:*
$P(\mathcal{E}_D) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\delta) + 1 - \Gamma_r(n/2, D^2/2\sigma^2)$;

B) *If $D > \sqrt{n}\sin(\phi)$:*
$P(\mathcal{E}_D) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) + 1 - \Gamma_r(n/2, D^2/2\sigma^2) +$
$\int_{y_a(\phi,D)}^{y_b(\phi,D)} \left(\Gamma_r\left(\frac{n-1}{2}, \frac{\omega_{z_1}^2}{2\sigma^2}\right) - \Gamma_r\left(\frac{n-1}{2}, \frac{r_{z_1}^2(\phi)}{2\sigma^2}\right)\right)\mathcal{N}(z_1)\mathrm{d}z_1,$
where $P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\theta)$ is given by (10), r_ϕ is the solution of (9), $r_\delta = n\tan^2(\delta)$ and $\delta = \sin^{-1}(D/\sqrt{n})$.

III. Upper bound on the performance of hard-decision Sphere Decoding

In this section, an upper bound on the performance of the hard-decision sphere decoder, when the code is transmitted over the BSC, is derived. Transmitting a binary codeword over an AWGN channel followed by hard decisions is equivalent to transmitting it on a BSC with a cross over probability $p = Q(\sqrt{2R\gamma})$ where γ is the bit signal to noise ratio. Let $\boldsymbol{y}$ be the received word when the codeword $\boldsymbol{c}$ is transmitted over an BSC channel. The HD sphere decoder with radius m, HSD(m), finds the codeword $\hat{\boldsymbol{c}}$, if it exists, such that

$$\begin{aligned} \hat{\boldsymbol{c}} = \arg\min_{\boldsymbol{v} \in \mathbb{C}} \quad & d\left(\boldsymbol{y}, \boldsymbol{v}\right) \\ \text{subject to} \quad & d(\boldsymbol{y}, \boldsymbol{v}) \leq m, \end{aligned} \tag{17}$$

where $d\left(\boldsymbol{y}, \boldsymbol{v}\right)$ is the Hamming distance between $\boldsymbol{y}$ and $\boldsymbol{v}$. Let $\zeta = d(\boldsymbol{y}, \boldsymbol{c})$, then, from the linearity of the code, the probability that the received word is outside a Hamming sphere (ball) of radius $m - 1$ centered around the transmitted codeword is

$$P(\zeta \geq m) = \sum_{t=m}^{n} \binom{n}{t} p^t (1-p)^{n-t}. \tag{18}$$

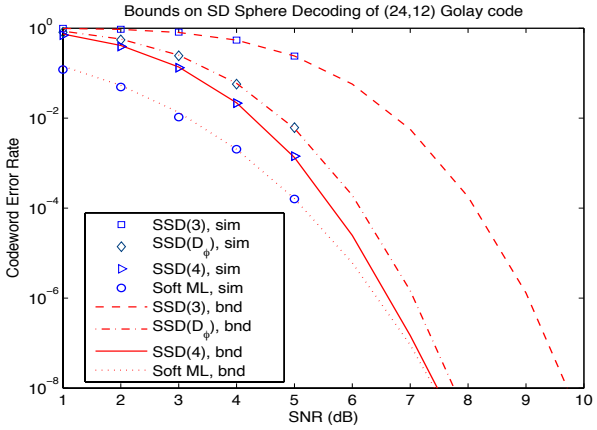

Fig. 3. Bounds on the performance of soft-decision sphere decoding of the (24,12) Golay code BPSK modulated over an AWGN channel.

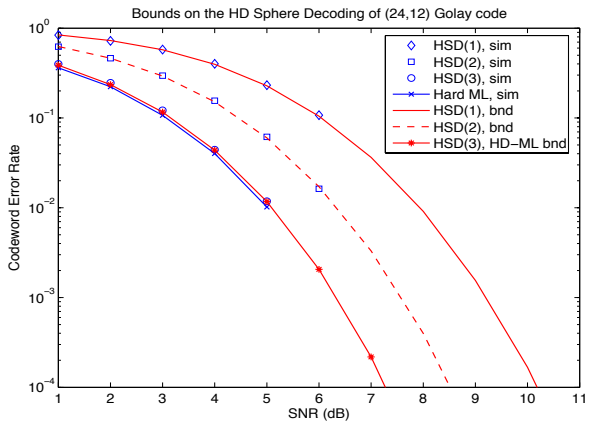

Fig. 4. Bounds on the performance of hard-decision sphere decoding of the (24,12) Golay code BPSK modulated over an AWGN channel.

Poltyrev [8] derived a tight bound on the performance of the HD-ML decoder based on,

$$P(\mathcal{E}_{ML}) \leq \min_{m} \{P(\mathcal{E}_{ML}, \zeta < m) + P(\zeta \geq m)\}. \quad (19)$$

The minimum of the above equation is at m_o where m_o is the smallest integer m such that [8]

$$\sum_{b=1}^{2m} G_b \sum_{r=\lceil \frac{w}{2} \rceil}^{m} \binom{b}{r}\binom{n-b}{m-r} \geq \binom{n}{m}. \quad (20)$$

The joint HD-ML error probability given that $\zeta < m$ is upper bounded by the union bound [8],

$$P(\mathcal{E}_{ML}, \zeta < m) \leq \sum_{b=1}^{2(m-1)} G_b \sum_{r=\lceil \frac{w}{2} \rceil}^{m-1} \left[\binom{b}{r} p^r (1-p)^{b-r} \sum_{s=0}^{m-r-1} \binom{n-b}{s} p^s (1-p)^{n-b-s}\right]. \quad (21)$$

We now turn our attention to the HD sphere decoder with an arbitrary decoding radius. Let $P(\Sigma_m)$, be the error plus failure probability of HSD($m-1$), then $P(\Sigma_m)$ could be written as

$$\begin{aligned} P(\Sigma_m) &= P(\Sigma_m, \zeta < m) + P(\Sigma_m | \zeta \geq m) P(\zeta \geq m) \\ &= P(\mathcal{E}_{ML}, \zeta < m) + P(\zeta \geq m), \end{aligned} \quad (22)$$

where we used the fact that $P(\Sigma_m | \zeta \geq m) = 1$ and the observation that given that $\zeta < m$, the conditional error probability of the HSD($m-1$) and the HD-ML decoders are the same. The last term in the above equation is equal to the failure probability of the HSD($m-1$) decoder. To develop a tight upper bound on $P(\Sigma_m)$, we consider two cases;

Case I: The decoding radius $m \geq m_o$. The upper bound of (22) could be written as

$P(\Sigma_m | m \geq m_o) = P(\mathcal{E}_{ML}, \zeta < m_o) + P(\mathcal{E}_{ML}, m_o \leq \zeta < m) + P(\zeta \geq m)$.

It follows that

$$P(\Sigma_m | m \geq m_o) \leq P(\mathcal{E}_{ML}, \zeta < m_o) + P(\zeta \geq m_o). \quad (23)$$

We observe that the upper bound reduces to that of the HD-ML case (19). By recalling that the minimum of (19) is achieved at m_o, the bound of (22) is looser than (23) when $m > m_o$. The intuition behind this is that the performance of a sphere decoder with a decoding radius $m_o - 1$ or greater approaches that of the ML decoder. Moreover, it was shown in [8] that m_o is a lower bound on the covering radius of the code.

Case II: The decoding radius $m < m_o$. Noticing that the sphere $\{\zeta < m\} \subset \{\zeta < m_o\}$, $P(\Sigma_m | m < m_o)$ is indeed given by (22).

Thus, we have proved the following theorem,

Theorem 4: The performance of a hard-decision sphere decoder with a decoding radius $m-1$ when used over an BSC channel with a cross-over probability p is upper bounded by

$$P(\Sigma_m) \leq \begin{cases} P(\mathcal{E}_{ML}, \zeta < m_o) + P(\zeta \geq m_o), & m \geq m_o; \\ P(\mathcal{E}_{ML}, \zeta < m) + P(\zeta \geq m), & m < m_o, \end{cases}$$

where m_o is radius that minimizes (19) and is the solution of (20). $P(\zeta \geq m)$ is given by (18) and $P(\mathcal{E}_{ML}, \zeta < m)$ is upper bounded by (21).

IV. Sphere Decoding of RS codes

We study the performance of Reed Solomon (RS) codes defined over F_{2^m} when their binary image is transmitted over an AWGN channel and the decoder is either a HD or SD sphere decoder. Tight upper bounds on the performance of the HD and SD maximum likelihood decoders were developed in [15] by averaging the Poltyrev bounds over all possible binary representations of the RS code. We use the same technique here to analyze the performance of the sphere decoders, where the average binary weight enumerator of the RS code (see [15]) would be used in conjunction with theorems 3 and 4 to derive averaged bounds on the performance of decoding RS codes with the SSD and HSD respectively.

V. Numerical Results

In this section, the bounds developed for SD and HD sphere decoding are evaluated and compared with the performance of

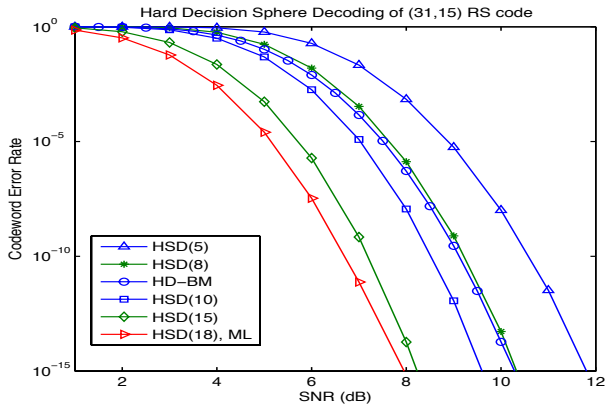

Fig. 5. Bounds on the performance of hard-decision sphere decoding of the $(31, 15)$ RS code BPSK modulated over an AWGN channel.

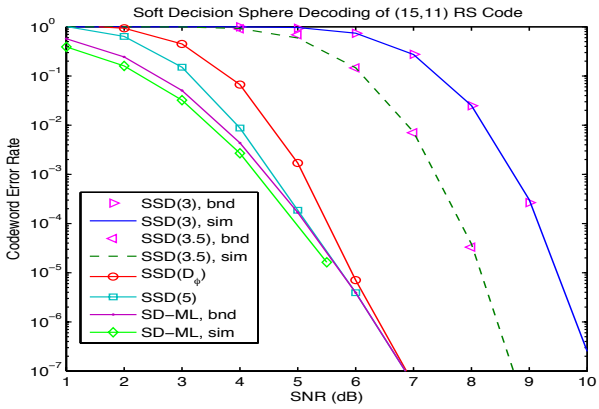

Fig. 6. Bounds on the performance of soft-decision sphere decoding of the $(15, 11)$ RS code BPSK modulated over an AWGN channel.

the corresponding sphere decoders, [6] and [7] respectively. The simulation curves and the analytical bounds will be labeled by 'sim' and 'bnd' respectively.

In figures 3 and 4, the performance of the soft and hard decision sphere decoders of the $(24, 12)$ Golay code is shown respectively. The minimum distance of the $(24, 12)$ Golay code is 8. For the SD sphere decoder, the critical decoding radius is $D_\phi = 3.772$ (see (13)). At a codeword error rater (CER) of 10^{-8}, the SSD with an Euclidean radius of 4 has a near ML performance. The optimum Hamming radius for the HSD bound is $m_o = 4$. As expected, a sphere decoder with radius $m_o - 1$ or greater has a near ML performance. It is observed that the analytical bounds are very tight. Similar results were also observed for BCH codes.

In Fig. 5, we show bounds on the performance of HD decoding of the near half rate $(31, 15)$ RS code over F_{32} when its binary image is transmitted over an AWGN channel. The HD-ML decoder has more than 2 dB coding gain over the Berlekamp Massey (BM) decoder [16], which can correct 8 symbol errors. We observe that the average performance of an HD sphere decoder with a (binary Hamming) radius 8 closely upper bounds that of the HD-BM decoder. The optimum decoding radius is 18 and the HSD has a competitive performance with a radius of 15. In Fig. 6, the performance of SD decoding of the $(15, 11)$ RS code over F_{16} are shown. The critical decoding radius is $D_\phi = 4.588$. As expected, the performance of a SSD with a larger decoding radius approaches that of the SD-ML decoder at a lower SNR.

VI. Conclusions

Bounds on the error plus failure probability of hard-decision and soft-decision sphere decoding of linear block codes were derived. By comparing with the simulations of the corresponding decoders these bounds are tight. The performance of sphere decoding of binary images of Reed Solomon codes was analyzed. Moreover, the bounds are extremely useful in predicting the performance of the sphere decoders at the tail of error probability when simulations are prohibitive.

Acknowledgment

This research was supported by NSF grant no. CCR-0118670 and grants from Sony, Qualcomm, and the Lee Center for Advanced Networking.

References

[1] Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inform. Theory*, vol. 24, pp. 384–386, May 1978.

[2] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of Computation*, vol. 44, pp. 463–471, 1985.

[3] C. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Programming*, vol. 66, pp. 181–191, 1994.

[4] E. Agrell, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.

[5] E. Viterbo and J. Boutros, "A universal lattice decoder for fading channels," *IEEE Trans. Inform. Theory*, vol. 45, p. 1639.

[6] H. Vikalo and B. Hassibi, "On joint ML detection and decoding on gaussian vector channels," submitted to *IEEE Trans. Signal Processing*.

[7] ——, "Statistical approach to ML decoding of linear block codes on symmetric channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2004.

[8] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.

[9] D. Divsalar, "A simple tight bound on error probability of block codes with application to turbo codes," TMO Progress Report, NASA,JPL, Tech. Rep. 42–139, 1999.

[10] S. Shamai and I. Sason, "Variations on the Gallager bounds, connections and applications," *IEEE Trans. Inform. Theory*, vol. 48, pp. 3029–3051, Dec. 2002.

[11] E. W. Weisstein, *Mathworld–A Wolfram Web Resource*. http://mathworld.wolfram.com.

[12] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2001.

[13] V. Ponnampalam and B. Vucetic, "Soft decision decoding of Reed-Solomon codes," *IEEE Trans. Commun.*, vol. 50, pp. 1758–1768, Nov. 2002.

[14] C. E. Shannon, "Probability of error for optimal codes in a gaussian channel," *Bell Syst. Tech. J.*, vol. 38, pp. 611–656, 1959.

[15] M. El-Khamy and R. J. McEliece, "Bounds on the average binary minimum distance and the maximum likelihood performance of Reed Solomon codes," in *42nd Allerton Conf. on Communication, Control and Computing*, 2004.

[16] R. J. McEliece, *The Theory of Information and Coding*, 2nd ed. Cambridge: Cambridge U. Press, 2002.