On the Sphere-Decoding Algorithm II. Generalizations, Second-Order Statistics, and Applications to Communications

Haris Vikalo and Babak Hassibi

***Abstract*—In Part I, we found a closed-form expression for the expected complexity of the sphere-decoding algorithm, both for the infinite and finite lattice. We continue the discussion in this paper by generalizing the results to the complex version of the problem and using the expected complexity expressions to determine situations where sphere decoding is practically feasible. In particular, we consider applications of sphere decoding to detection in multiantenna systems. We show that, for a wide range of signal-to-noise ratios (SNRs), rates, and numbers of antennas, the expected complexity is polynomial, in fact, often roughly cubic. Since many communications systems operate at noise levels for which the expected complexity turns out to be polynomial, this suggests that maximum-likelihood decoding, which was hitherto thought to be computationally intractable, can, in fact, be implemented in real-time—a result with many practical implications. To provide complexity information beyond the mean, we derive a closed-form expression for the variance of the complexity of sphere-decoding algorithm in a finite lattice. Furthermore, we consider the expected complexity of sphere decoding for channels with memory, where the lattice-generating matrix has a special Toeplitz structure. Results indicate that the expected complexity in this case is, too, polynomial over a wide range of SNRs, rates, data blocks, and channel impulse response lengths.**

***Index Terms*—Expected complexity, frequency-selective channels, multiple-antenna systems, polynomial-time complexity, sphere decoding, wireless communications.**

I. Introduction

INTEGER least-squares problems of the form

$$\min_{s} ||x - Hs||^2 \tag{1}$$

appear in a host of applications. In communications, when the channel is linear and the noise independent, identically distributed (i.i.d.) Gaussian, maximum-likelihood (ML) decoding leads to a least-squares cost. When the transmitted symbols are from a finite set, this can be often cast as an integer least-squares problem. Applications where the sphere-decoding algorithm is employed for solving the integer least-squares problem (1) include lattice codes [1]–[4], CDMA systems [5], and multiantenna systems [6]–[8]. In all these applications, the unknown vector s represents the transmitted signal, the matrix H represents the channel, and the vector x represents the received signal. For example, in the multiantenna context of V-BLAST [6], where we have M transmit and N receive antennas, H is the $(m = 2M) \times (n = 2N)$ real channel matrix, and for linear space–time codes (such as those in [8]), it is the equivalent channel matrix. The integer least-squares problem also arises in the detection of signals transmitted over frequency-selective finite impulse response channels [9]. Other applications include global positioning systems (GPSs) [10] and cryptography. In fact, there is a whole family of public-key cryptosystems based on the NP-hardness of the integer least-squares problem [11]–[13].

In this paper, we continue with the study of complexity of sphere decoding started in Part I. In Sections II and IV, we demonstrate the use of the expressions for expected complexity to determine situations where sphere decoding is practically feasible, i.e., we use those expressions to search for the transition from polynomial to exponential expected complexity. In particular, in Section II, the expected complexity of sphere decoding for an infinite lattice, relevant for GPS applications, is examined over a range of values of the system parameters. In Section IV, we study the complexity of sphere decoding employed for ML detection in multiantenna wireless communication systems. Since in this application, the underlying optimization problem is complex valued, we first generalize the expected complexity results to the complex version of the integer least-squares problem in Section III. Using these expressions, we show in Section IV that over a wide range of rates, signal-to-noise ratios (SNRs), and dimensions (in fact, those that are typically encountered in communications problems), the expected complexity of the sphere-decoding algorithm is polynomial, often cubic. In order to provide complexity information beyond the first-order statistics that we found in Part I, in Section V, we calculate the variance of complexity of sphere decoding. Application of the sphere-decoding algorithm to frequency-selective channels and the complexity of the algorithm therein are studied in Section VI. The complexity of the algorithm for the case when the system of equations in (1) is overdetermined and some variations of the basic sphere-decoding algorithm are discussed in Section VII, while the conclusion is in Section VIII. Many of the results of this paper and various extensions can be found in the first author's Ph.D. dissertation [14].

Manuscript received June 25, 2003; revised September 19, 2004. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Zhi Ding.

The authors are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: hvikalo@systems.caltech.edu; hassibi@systems.caltech.edu).

Digital Object Identifier 10.1109/TSP.2005.850350

1053-587X/$20.00 © 2005 IEEE

II. Expected Complexity Exponent of Sphere Decoding in Infinite Lattice

As a measure of complexity, instead of the complexity itself, it is often useful to look at the *complexity exponent*, defined as

$$e_c = \frac{\log C(m, \sigma^2, d^2)}{\log m}. \tag{2}$$

In other words, for the particular complexity exponent e_c, the expected complexity of sphere decoding is

$$C(m, \sigma^2, d^2) = m^{e_c}.$$

When plotted, e_c is more visually appealing since the complexity exponent approaches a constant if the expected complexity is polynomial and grows like $m/\log m$ if $C(m, \sigma^2, d^2)$ is exponential.

Using the closed-form expression for the expected complexity of sphere decoding in an infinite lattice given by (28) in Part I, the complexity exponent is plotted as a function of m for different values of σ^2 in Fig. 1. As can be seen from the figure, for small enough noise, the expected complexity is polynomial, as indicated by the constant e_c over a wide range of m. On the other hand, for large noise, e_c clearly exhibits the $m/\log m$ behavior, and the computational complexity of the algorithm is exponential. Thus, we see the transition from polynomial time to exponential complexity, which, for a wide range of m, takes place at $\sigma^2 \approx 1$.

III. Generalization of Complexity Results to the Complex Case

In many applications, one is confronted with a complex version of the integer least-squares problem. In this case, we may generally assume that the model is

$$\mathbf{x} = \mathbf{H}\mathbf{s} + \mathbf{v} \tag{3}$$

where now $\mathbf{v} \in \mathcal{C}^{N\times 1}$ is comprised of i.i.d. $\mathcal{CN}(0, \sigma^2)$ (circularly-symmetric complex normal) entries, $\mathbf{H} \in \mathcal{C}^{N\times M}$ is comprised of i.i.d. $\mathcal{CN}(0, 1)$ entries, and $\mathbf{s} \in \mathcal{CZ}^M$ is an M-dimensional complex vector whose entries have real and imaginary parts that are integers. As before, we are interested in the problem

$$\min_{\mathbf{s}\in\mathcal{CZ}^M} \|\mathbf{x} - \mathbf{H}\mathbf{s}\|^2. \tag{4}$$

The standard sphere-decoding algorithm given in Section 3.1 of Part I can be applied, provided that we use the complex QR decomposition and modify the algorithm to accommodate for complex inputs. In particular, the algorithm now runs over complex dimensions $k = 1, 2, \ldots, M$. Therefore, instead of finding points that belong to an interval on a real line, steps 2 and 3 of the algorithm in Section 3.1 of Part I need to be modified so that they compute coordinates of the points within a disc in a complex plane. In the other steps of the algorithm, all that one needs to do is replace the real operations with appropriate complex ones. We are omitting the details of the algorithm and its complexity analysis for brevity and because they closely parallel the real case and state the complexity results below.

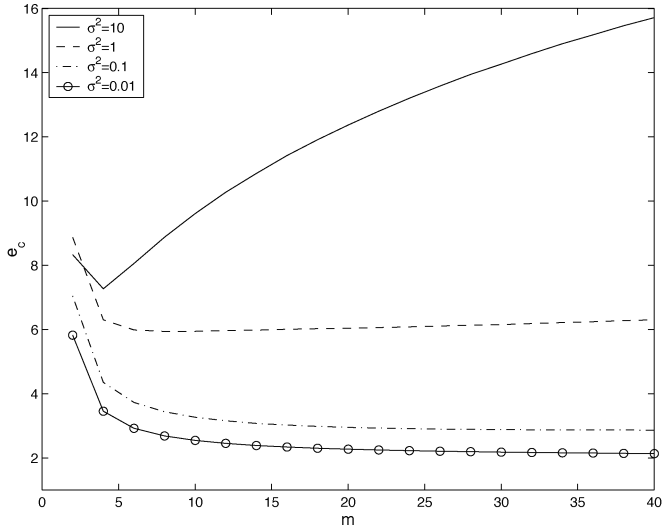

Fig. 1. Complexity exponent as a function of dimension m for the noise variance $\sigma^2 = 0.01, 0.1, 1, 10$ with $\epsilon = .1$ chosen for the sphere decoder applied to an infinite lattice.

Corollary 1. [Expected Complexity of Sphere Decoding Over Infinite Lattice]: Consider the model

$$\mathbf{x} = \mathbf{H}\mathbf{s} + \mathbf{v}$$

where $\mathbf{v} \in \mathcal{C}^{N\times 1}$ is comprised of i.i.d. $\mathcal{CN}(0, \sigma^2)$ entries, $\mathbf{H} \in \mathcal{C}^{N\times M}$ is comprised of i.i.d. $\mathcal{CN}(0, 1)$ entries, and $\mathbf{s} \in \mathcal{CZ}^M$ is an M-dimensional vector whose entries are complex vectors with integer numbers for real and imaginary parts. Then, the expected complexity of the sphere-decoding algorithm with a search radius d for solving the integer least-squares problem

$$\min_{\mathbf{s}\in\mathcal{CZ}^M} \|\mathbf{x} - \mathbf{H}\mathbf{s}\|^2$$

is given by

$$C(M, \sigma^2, d^2) = \sum_{k=1}^{M} F_p(k) \sum_{l=0}^{\infty} \gamma\left(\frac{d^2}{\sigma^2 + l}, N - M + k\right) r_{2k}(l) \tag{5}$$

where the number of elementary operations per visited point in complex dimension k is $F_p(k) = 8k + 24$, and $r_{2k}(l)$ is the number of ways l can be represented as the sum of $2k$ squared integers.

Corollary 2. [Expected Complexity for Finding the Optimal Solution]: Consider the setting of Corollary 1 in Part I. Given any $0 < \epsilon \ll 1$, consider a strategy where we first choose a radius such that we find a lattice point with probability $1-\epsilon$, and then increase it to a probability of $1 - \epsilon^2$, and so on, if no point is found. Then, the expected complexity of the sphere-decoding algorithm to find the optimal solution is given by

$$C(M, \sigma^2, \epsilon) = \sum_{i=1}^{\infty} (1-\epsilon)\epsilon^{i-1} \sum_{k=1}^{M} F_p(k) \times \sum_{l=0}^{\infty} \gamma\left(\frac{\alpha_i N\sigma^2}{\sigma^2 + l}, N - M + k\right) r_{2k}(l) \tag{6}$$

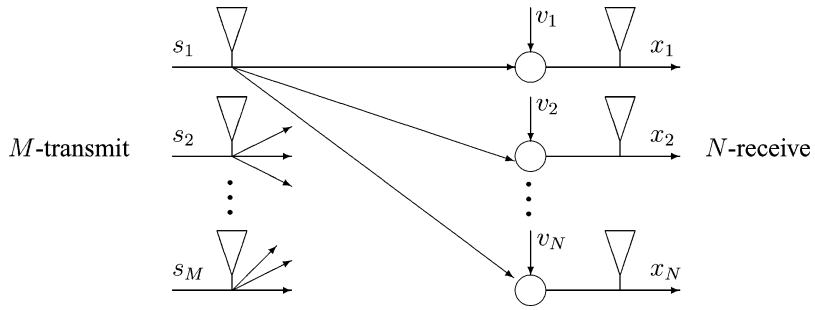

Fig. 2. Multiple antenna system.

where $F_p(k) = 8k + 24$, $r_{2k}(l)$ is the number of ways l can be represented as the sum of $2k$ squared integers, $\gamma(\cdot,\cdot)$ denotes a normalized gamma function, and α_i is chosen such that

$$\gamma(\alpha_i N, N) = 1 - \epsilon^i, \quad i = 1, 2, \ldots \tag{7}$$

When confronted with a complex integer least-squares problem over a finite lattice, similar results hold.

The next corollary is the complex analog of Theorem 2 in Part I.

Corollary 3. [Expected Complexity of the Sphere Decoding Over a Finite Lattice]: Consider the model

$$\mathbf{x} = \mathbf{H}\mathbf{s} + \mathbf{v}$$

where $\mathbf{v} \in \mathcal{C}^{N\times 1}$ is comprised of i.i.d. $\mathcal{CN}(0,\sigma^2)$ entries, $\mathbf{H} \in \mathcal{C}^{N\times M}$ is comprised of i.i.d. $\mathcal{CN}(0,1)$ entries, and $\mathbf{s} \in \mathcal{CD}_L^M$ is an M-dimensional vector whose entries are complex-valued elements of an L^2-QAM constellation. Define the SNR as

$$\rho = \frac{M(L^2-1)}{6\sigma^2}.$$

Then, the expected complexity of the sphere-decoding algorithm with a search radius d, chosen such that $d^2 = \alpha N(M(L^2-1)/6\rho)$, for solving the integer least-squares problem

$$\min_{\mathbf{s}\in\mathcal{CD}_L^M} \|\mathbf{x} - \mathbf{H}\mathbf{s}\|^2$$

1) for a 4-QAM constellation

$$C(M,\rho,d^2) = \sum_{k=1}^{M} F_p(k) \sum_{l=0}^{2k} \binom{2k}{l} \gamma\left(\frac{\alpha N}{1+\frac{6\rho l}{M(L^2-1)}}, N-M+k\right) \tag{8}$$

2) for a 16-QAM constellation

$$C(M,\rho,d^2) = \sum_{k=1}^{M} F_p(k) \sum_{q} \frac{1}{2^{2k}} \times \sum_{l=0}^{2k} \binom{2k}{l} g_{2kl}(q)\gamma\left(\frac{\alpha N}{1+\frac{6\rho q}{M(L^2-1)}}, N-M+k\right) \tag{9}$$

where $g_{2kl}(q)$ is the coefficient of x^q in the polynomial

$$(1 + x + x^4 + x^9)^l (1 + 2x + x^4)^{2k-l}.$$

3) for a 64-QAM constellation, the expected complexity is

$$C(M,\rho,d^2) = \sum_{k=1}^{M} F_p(k) \sum_{q} \frac{1}{4^{2k}} \times \sum_{j_0,j_1,j_2,j_3} g_{2kj_0j_1j_2j_3}(q)\gamma\left(\frac{\alpha N}{1+\frac{6\rho q}{M(L^2-1)}}, N-M+k\right) \tag{10}$$

where $g_{2kj_0j_1j_2j_3}(q)$ is the coefficient of x^q in the polynomial

$$\binom{2k}{j_0, j_1, j_2, j_3} \psi_0^{j_0}(x)\psi_1^{j_1}(x)\psi_2^{j_2}(x)\psi_3^{j_3}(x)$$

where $j_0 + j_1 + j_2 + j_3 = 2k$ and $\binom{2k}{j_0,j_1,j_2,j_3} = (2k)!/(j_0!j_1!j_2!j_3!)$, and

$$\begin{aligned}
\psi_0(x) &= 1 + x + x^4 + x^9 + x^{16} + x^{25} + x^{36} + x^{49} \\
\psi_1(x) &= 1 + 2x + x^4 + x^9 + x^{16} + x^{25} + x^{36} \\
\psi_2(x) &= 1 + 2x + 2x^4 + x^9 + x^{16} + x^{25} \\
\psi_3(x) &= 1 + 2x + 2x^4 + 2x^9 + x^{16}.
\end{aligned}$$

4) similar expressions can be obtained for 256-QAM, etc., constellations.

The number of elementary operations per visited point in (8)–(10) is $F_p(k) = 8k + 20 + 4L$, while $\gamma(\cdot,\cdot)$ in (8)–(10) denotes a normalized gamma function.

IV. Expected Complexity Exponent of Sphere Decoding in Finite Lattices: ML Detection in Multiantenna Systems

In this section, we use the expressions from Section III to study the expected complexity of sphere decoding employed for ML detection in multiantenna systems. Fig. 2 shows a multiantenna system with M-transmit and N-receive antennas.

The received signal $\mathbf{x}$ is related to the transmitted symbol $\mathbf{s}$ via

$$\mathbf{x} = \mathbf{H}\mathbf{s} + \mathbf{v} \tag{11}$$

where $\mathbf{H} \in \mathcal{C}^{N\times M}$ is the known channel matrix comprised of i.i.d. complex-Gaussian entries $\mathcal{CN}(0,1)$, and $\mathbf{v} \in \mathcal{C}^{N\times 1}$ is the additive noise vector, comprised of i.i.d. complex-Gaussian entries $\mathcal{CN}(0,\sigma^2)$. Furthermore, entries in the symbol vector $\mathbf{s}$

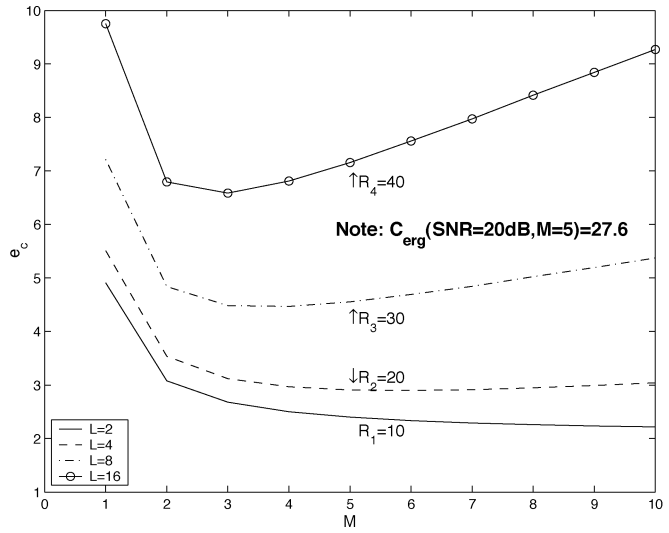

Fig. 3. Complexity exponent as a function of M for $\rho = 20$ dB and $L = 2, 4, 8, 16$.

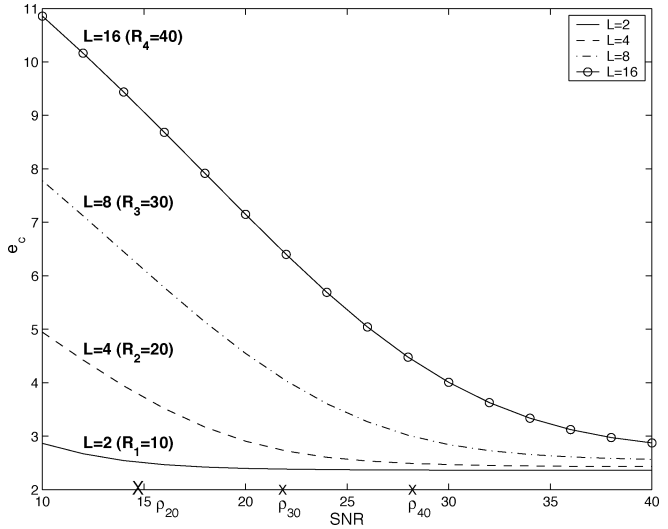

Fig. 4. Complexity exponent as a function of ρ for $M = N = 5$ and $L = 2, 4, 8, 16$.

are chosen from a complex-valued L^2-QAM constellation, i.e., both the real and the imaginary components of $\mathbf{s}$ are elements of an L-PAM constellation $\mathcal{D}_L$. As in Section III, the SNR ρ is given by

$$\rho = \frac{E\{\text{tr}(\mathbf{H}\mathbf{s}\mathbf{s}^*\mathbf{H}^*)\}}{E\{\text{tr}(\mathbf{v}\mathbf{v}^*)\}} = \frac{M(L^2-1)}{6\sigma^2}$$

where $\text{tr}(\cdot)$ denotes trace of its argument. The transmission rate is defined as the number of bits transmitted per channel use

$$R = M \log L^2 = 2M \log L.$$

We consider the expected complexity of the sphere-decoding algorithm for signal detection in the system shown in Fig. 2 with equal $(M = N)$ number of transmit and receive antennas, for various QAM modulation schemes. The expected complexity $C(M, \rho, \epsilon)$ is a function of both the symbol vector size M and the SNR ρ.[1] We shall consider "snapshots" in each dimension, i.e., we keep either M or ρ variable fixed and examine the expected complexity as a function of the other variable. Fig. 3 shows the complexity exponent, defined as

$$e_c = \frac{\log C(M, \rho, \epsilon)}{\log 2M}$$

as a function of M for a fixed SNR $\rho = 20$ dB and L^2-QAM constellations with $L = 2, 4, 8, 16$. For low rates (i.e., small constellations), the expected complexity is polynomial, whereas for high rates (i.e., large constellations), it is exponential. Simulation results suggest that the complexity is polynomial as long as the rate is sufficiently—but not necessarily all that much—below the Shannon capacity corresponding to the SNR. Since this is the regime at which most communication systems operate, it suggests that ML decoding can be feasible. For instance, the complexity exponents curves in Fig. 3 that correspond to $L = 8$ and $L = 16$ modulation schemes appear to be in the exponential regime. However, as is illustrated in Fig. 3 for $M = 5$, the data rates corresponding to the points on those two curves are larger than the corresponding ergodic capacity

$$C_{\text{erg}} = E\{\log \det(I_M + \mathbf{H}^*\mathbf{H})\}.$$

For instance, when $M = 5$ (and SNR 20 dB), ergodic capacity is $C_{\text{erg}} = 27.6$. For the same system parameters, only the rates provided by the modulation schemes corresponding to $L = 2$ and $L = 4$ ($R_1 = 10$ and $R_2 = 20$, respectively, as denoted in Fig. 3) can be supported by the channel. The other two modulation schemes cannot be employed (we assume uncoded transmission). Note that the expected complexity exponent in the data transmission regime that is supportable by the channel complexity is roughly cubic—which, in fact, is the complexity of the heuristic techniques. For comparison, exhaustive search in $M = N = 5$, 16-QAM system requires examining $k = 4^{10} \approx 10^6$ points, which is roughly of sixth order.

Fig. 4 shows the complexity as a function of SNR for $M = 5$ and L^2-QAM constellations with $L = 2, 4, 8, 16$. A particular modulation scheme can be used only in the range of SNRs that supports transmission at the rate corresponding to that modulation scheme. We note that in such a range, the complexity exponent is roughly cubic. For instance, although the complexity for $L = 16$ appears to be high over a wide range of SNR, it is only for $\rho > \rho_{40} = 27.9$ dB that this modulation scheme can be employed [ρ_{40} is the SNR for which the capacity $C_{\text{erg}} = 40 = R_4(L = 16)$]. The complexity exponent at ρ_{40} and $L = 16$ is $e_c \approx 4.4$. The other SNRs marked on Fig. 4, $\rho_{30} = 21.6$ dB and $\rho_{20} = 14.9$ dB, have similar meanings (only for $L = 8$ and $L = 4$, respectively).

Figs. 3 and 4 show the analytically obtained expected complexity, that is, the first-order statistics. In Fig. 5, the empirical distribution of the complexity exponent $p(e_c)$ is shown for $M = N = 5$ transmit and receive antennas, 16-QAM modulation scheme, and for four different SNR values. From Fig. 4, we

[1]In all of the simulations presented, the complexities are for the scheme that finds the optimal solution. In other words, our initial radius is determined so that we find a lattice point with probability .9 (i.e., $\epsilon = .1$). If no lattice point is found, we increase the radius so that this probability increases to .99, and so on.

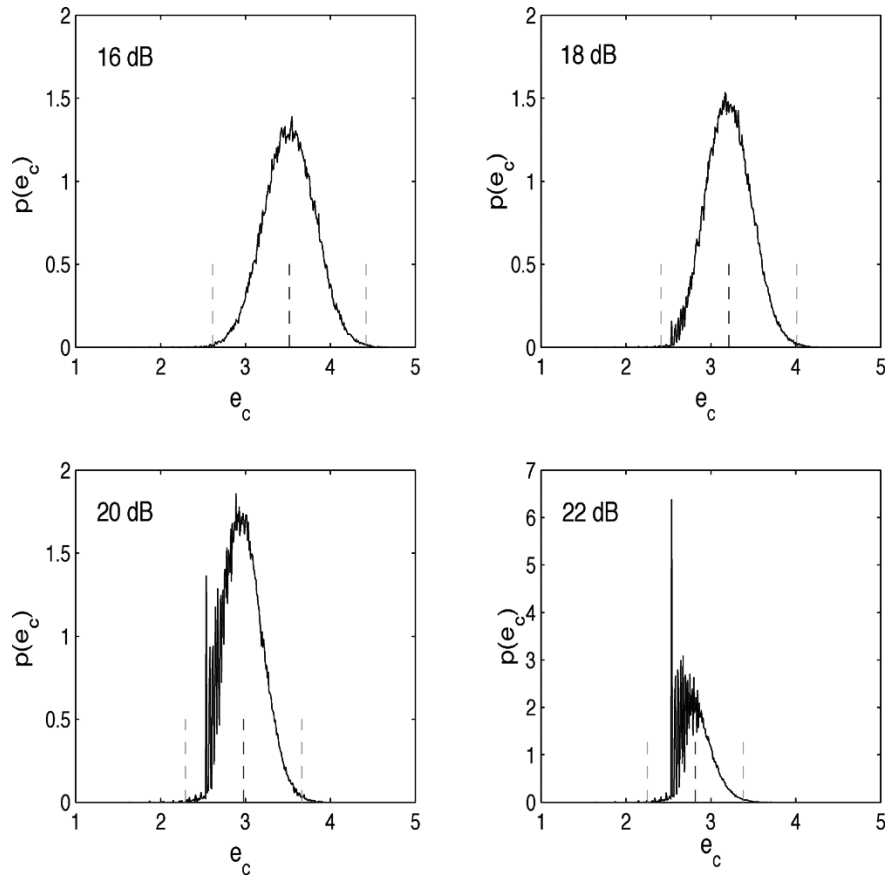

Fig. 5. Complexity exponent distribution for $M = N = 5$, $L = 4$, and SNR $= 16, 18, 20, 22$ dB.

see that the lowest SNR in Fig. 5 (16 dB) roughly corresponds to the minimum SNR required for transmission on the particular system with the modulation scheme of choice. The outer dashed lines in each graph of Fig. 5 denote the complexity exponents that are three standard deviations away from the mean. The middle dashed line denotes the mean itself, i.e., the expected complexity. We can make the following observations in relation to the distributions as the SNR increases.

- The expected complexity decreases, which was already implied by the results illustrated in Fig. 4.
- The variance of the complexity decreases, as illustrated with the tightening of the standard deviation.
- The "point-mass" segments become more pronounced. This is expected: For large SNRs, the radius of the sphere will be small, and only a small (discrete) number of lattice points are found inside.

More discussion on the variance of sphere decoding will follow in the next section of the paper.

Finally, Fig. 6 shows the improvement in performance of sphere decoding over the minimum mean-squared error (MMSE) nulling and cancelling with optimal ordering for a multiantenna system employing $M = N = 5$ transmit and receive antennas and 16-QAM modulation scheme. The complexity of ML decoding for a single frame via sphere decoding here is comparable to that of nulling and cancelling, whereas the performance improvement is significant. The range of SNRs in Fig. 6 is typical for indoor applications ([6]).

V. Variance of Computational Complexity of Sphere Decoding

Recall the basic real-valued integer least-squares problem that we focused on in Part I. As argued there, the complexity of sphere decoding is a random variable that depends upon the realization of the generator matrix H and the noise vector v. So far, we have considered its first moment, i.e., the expected complexity. In this section, we find the variance of the complexity of sphere decoding for a finite lattice. Using the results derived in Part I of the paper, we can express the variance as

$$\begin{aligned}\text{Var} &= E\left\{\sum_{k=1}^{m}\left[N_p(k)f_p(k) - E_p(k,\rho,d^2)f_p(k)\right]\right\}^2 \\ &= E\left\{\sum_{k=1}^{m}\left[N_p(k)f_p(k) - E_p(k,\rho,d^2)f_p(k)\right]\right. \\ &\qquad \left.\times\sum_{l=1}^{m}\left[N_p(l)f_p(l) - E_p(l,\rho,d^2)f_p(l)\right]\right\} \\ &= \sum_{k=1}^{m}\sum_{l=1}^{m}\left[E\left\{N_p(k)N_p(l)\right\} - E_p(k,\rho,d^2)E_p(l,\rho,d^2)\right] \\ &\quad \times f_p(k)f_p(l) \end{aligned} \tag{12}$$

where $N_p(i)$ is the number of points in a sphere of dimension i and radius d, and $f_p(i)$ is the number of operations (flop count) per visited point in dimension i. The average number of points

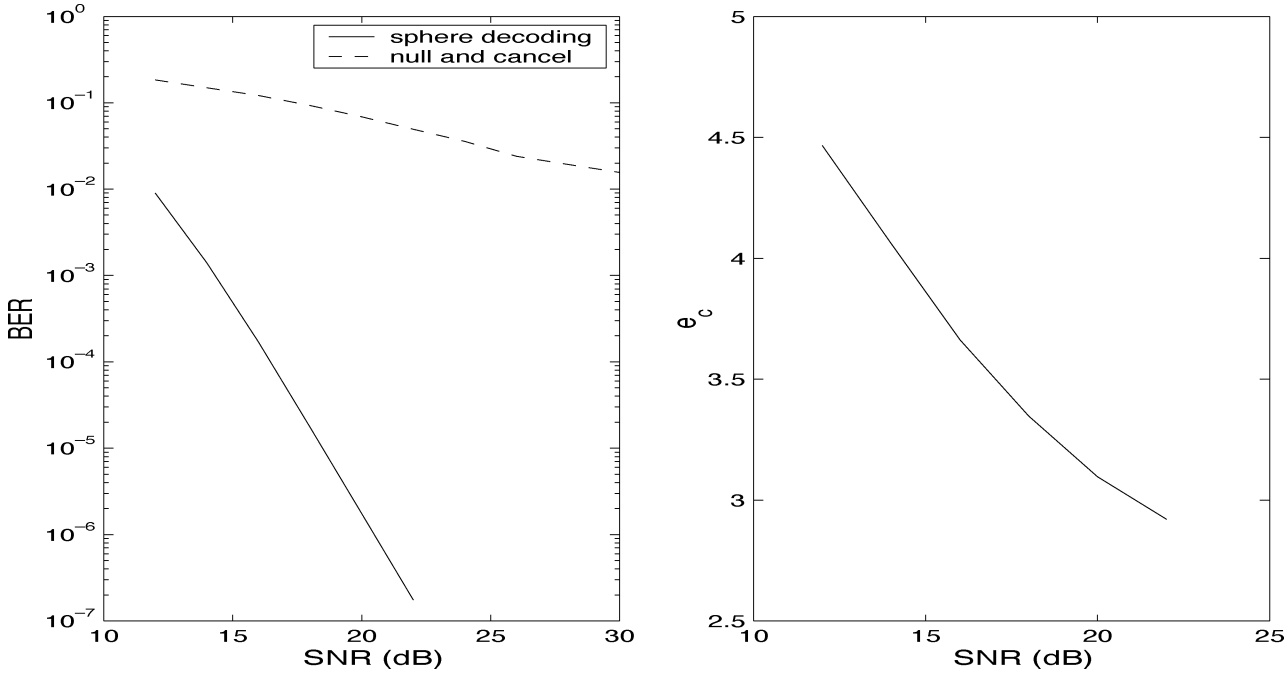

Fig. 6. Sphere decoder versus nulling and cancelling, $M = N = 5$, $L = 4$, and corresponding e_c.

per dimension, $E_p(i, \rho, d^2) = EN_p(i)$, $i = 1, 2, \ldots, m$, has been given in Theorem 2 in Part I of the paper. What remains to be determined in (12) is the correlation $E\{N_p(k)N_p(l)\}$, i.e., the expected number of pairs of points that fall inside the spheres of radius d and dimensions k and l, centered at the received vector. To this end, recall that a skewed lattice point Hs belongs to a sphere of radius d around the received vector x iff

$$d^2 \geq \|x - Hs\|^2 = \|x - QRs\|^2 = \|Q^*x - Rs\|^2 = \|y - Rs\|^2$$

where we denoted $y = Q^*x$, and $H = QR$. Therefore, for any pair of points (s_B, s_C), where s_B and s_C are k-dimensional and l-dimensional vectors in $\mathcal{D}_L^k$ and $\mathcal{D}_L^l$, respectively, we wish to calculate

$$\begin{aligned} &E\{N_p(k)N_p(l)\} \\ &\quad = \sum_{(s_B, s_C)} p\left(\underbrace{\|y^k - R_{k,k}s_B\|^2}_{=t_b} \leq d^2, \underbrace{\|y^l - R_{l,l}s_C\|^2}_{=t_c} \leq d^2\right) \\ &\quad = \sum_{(s_B, s_C)} p(t_b \leq d^2,\ t_c \leq d^2) \end{aligned} \tag{13}$$

where the vectors y^k and y^l are k-dimensional and l-dimensional, respectively, and the upper-triangular matrices $R_{k,k}$ and $R_{l,l}$ are $k \times k$ and $l \times l$, respectively, and are defined by the following partitioning of the vector y and the matrix R:

$$y = \begin{bmatrix} y^{n-k} \\ y^k \end{bmatrix} = \begin{bmatrix} y^{n-l} \\ y^l \end{bmatrix} \quad \text{and}$$
$$R = \begin{bmatrix} R_{m-k,m-k} & R_{m-k,k} \\ 0_{k\times(m-k)} & R_{k,k} \end{bmatrix} = \begin{bmatrix} R_{m-l,m-l} & R_{m-l,l} \\ 0_{l\times(m-l)} & R_{l,l} \end{bmatrix}.$$

Assume that s_t has been transmitted. Then, we can write

$$\begin{aligned} t_b &= \|y^k - R_{k,k}s_B\|^2 = \|u^k + R_{k,k}s_t - R_{k,k}s_B\|^2 \\ &= \left\| u^k + R_{k,k}\underbrace{(s_t - s_B)}_{=s_b} \right\|^2 \end{aligned}$$

and

$$\begin{aligned} t_c &= \|y^l - R_{l,l}s_C\|^2 = \|u^l + R_{l,l}s_t - R_{l,l}s_C\|^2 \\ &= \left\| u^l + R_{l,l}\underbrace{(s_t - s_C)}_{=s_c} \right\|^2 \end{aligned}$$

where $u = Q^*v$, and u^k and u^l are k-dimensional and l-dimensional vectors, respectively, obtained by partitioning u as

$$u = \begin{bmatrix} u^{n-k} \\ u^k \end{bmatrix} = \begin{bmatrix} u^{n-l} \\ u^l \end{bmatrix}.$$

Without loss of generality, we will assume that $k \leq l$. Let s_c^k denote the vector comprised of the last k entries of s_c. Then, one can show (see Appendix A) the following.

1) If $s_b = s_c^k$

$$p(t_b \leq d^2, t_c \leq d^2) = \gamma\left(\frac{d^2}{2(\sigma^2 + \|s_c\|^2)}, \frac{l}{2}\right). \tag{14}$$

2) If $s_b \neq s_c^k$

$$p(t_b \leq d^2, t_c \leq d^2) = \int_{t_b=0}^{d^2}\int_{t_c=0}^{d^2} \phi(t_b, t_c)dt_b dt_c \tag{15}$$

where

$$\phi(t_b,t_c) = \frac{1}{4\pi^2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{d\omega_b d\omega_c e^{-j\omega_b t_b - j\omega_c t_c}}{\Delta^{\frac{k}{2}}\left[\left(\frac{a_{bb}}{\Delta}-2j\omega_c\right)\left(\frac{a_{cc}}{\Delta}-2j\omega_b\right)-\frac{a_{bc}^2}{\Delta^2}\right]^{\frac{k}{2}}} \times \frac{\left(1-2j\omega_c\left(\sigma^2+\left\|s_c^k\right\|^2\right)\right)^{\frac{k}{2}}}{\left(1-2j\omega_c\left(\sigma^2+\|s_c\|^2\right)\right)^{\frac{l}{2}}}$$

and

$$a_{bb}=\|s_b\|^2+\sigma^2,\quad a_{cc}=\left\|s_c^k\right\|^2+\sigma^2$$
$$a_{bc}=s_b^* s_c^k+\sigma^2,\quad \text{and } \Delta=a_{bb}a_{cc}-a_{bc}^2.$$

The summation in (13) is over all possible pairs of points (s_b,s_c). This is a formidable task for even small to moderate (k,l). To ease the calculation, we count the number of pairs of points (s_b,s_c) that give the same $p(t_b\le d^2,t_c\le d^2)$. From (14) and (15), it follows that the probability is completely determined by the quadruplet $(\|s_b\|^2,\|s_c^k\|^2,s_b^*s_c^k,\|s_c\|^2)$. Therefore, we can enumerate all pairs of lattice points (s_b,s_c) by counting the number of solutions to the system of equations

$$\|s_b\|^2=\beta,\quad \left\|s_c^k\right\|^2=\gamma,\quad s_b^*s_c^k=\delta,\quad \text{and}\quad \|s_c\|^2=\eta$$

where β, γ, δ, and η are integer numbers that satisfy the constraints imposed by dimensions k and l and by the span of the constellation L.

We will show the enumeration for a 2-PAM constellation. Since the constellation is symmetric, and all points are equally likely to be transmitted, we can assume that the point s_t comprised of all $-1/2$ has been sent. Let us first count the number of pairs (s_b,s_c^k) that give a particular triplet $(\|s_b\|^2,\|s_c^k\|^2,s_b^*s_c^k)$. Since the transmitted vector has all entries equal to $-1/2$, the entries of s_b and s_c^k can only be 0 and 1. Therefore, each entry of s_b, s_c^k, and $s_b^*s_c^k$ can simultaneously only take on the values (0,0,0), (1,0,0), (0,1,0), and (1,1,1). So, we form a multinomial in three variables, where each variable represents one of the components in an admissible triplet

$$g_1(x,y,z)=(x^0y^0z^0+x^1y^0z^0+x^0y^1z^0+x^1y^1z^1)=1+x+y+xyz.$$

Therefore, the polynomial

$$g_k(x,y,z)=g_1^k(x,y,z)=(1+x+y+xyz)^k=\sum_{k_1+k_2+k_3+k_4=k,k_1\ge0,k_2\ge0,k_3\ge0,k_4\ge0}\binom{k}{k_1,k_2,k_3,k_4}\times x^{k_2+k_4}y^{k_3+k_4}z^{k_4}=\sum_{\beta+\gamma\le k+\delta,\delta\le\beta,\delta\le\gamma}\frac{k!}{(k+\delta-\beta-\gamma)!(\beta-\delta)!(\gamma-\delta)!\delta!}\times x^\beta y^\gamma z^\delta \quad (16)$$

counts all possible triplets $(\|s_b\|^2,\|s_c^k\|^2,s_b^*s_c^k)$ in the following manner: There are $k!/((k+\delta-\beta-\gamma)!(\beta-\delta)!(\gamma-\delta)!\delta!)$ pairs of points (s_b,s_c^k) such that

$$\|s_b\|^2=\beta,\quad \left\|s_c^k\right\|^2=\gamma,\quad s_b^*s_c^k=\delta.$$

The number of vectors s_c that, in addition to satisfying the above, have $\|s_c\|^2=\eta$ is given by $\binom{l-k}{\eta-\gamma}$.

Combining the above, we conclude that

$$\frac{k!}{(k+\delta-\beta-\gamma)!(\beta-\delta)!(\gamma-\delta)!\delta!}\binom{l-k}{\eta-\gamma}$$

is the number of pairs of points (s_b,s_c) such that $\|s_b\|^2=\beta$, $\|s_c^k\|^2=\gamma$, $s_b^*s_c^k=\delta$, and $\|s_c\|^2=\eta$, which gives us the full enumeration for which we were seeking.

The results of this section can be summarized in the following theorem.

Theorem 1. [Variance of Complexity of the Sphere Decoding Algorithm Over $\mathcal{D}_2^m$ Lattice]: Consider the model

$$x=Hs+v$$

where $v\in\mathcal{R}^{n\times1}$ is comprised of i.i.d. $\mathcal{N}(0,\sigma^2)$ entries, $H\in\mathcal{R}^{n\times m}$ is comprised of i.i.d. $\mathcal{N}(0,1)$ entries, and $s\in\mathcal{D}_2^m$ is an m-dimensional vector whose entries are elements of an 2-PAM constellation. Then, the variance of the complexity of the sphere-decoding algorithm with a search radius of d for solving the integer least-squares problem

$$\min_{s\in\mathcal{D}_2^m}\|x-Hs\|^2$$

is given by

$$\text{Var}=\sum_{k=1}^{m}\sum_{l=1}^{m}\left[E\left\{N_p(k)N_p(l)\right\}-E_p(k,\rho,d^2)E_p(l,\rho,d^2)\right]f_p(k)f_p(l)$$

where

$$E\left\{N_p(k)N_p(l)\right\}=\sum_{\beta,\gamma,\delta,\eta}p(t_b\le d^2,t_c\le d^2)\times\frac{r!}{(r+\delta-\beta-\gamma)!(\beta-\delta)!(\gamma-\delta)!\delta!}\binom{q-r}{\eta-\gamma}$$

where $E_p(i,\rho,d^2)$ is computed in Section 4.4 in Part I, where $r=\min(k,l)$, $q=\max(k,l)$, $\beta+\gamma\le r+\delta$, $\delta\le\beta$, $\delta\le\gamma$, $\eta-\gamma\le q-r$, and $p(t_b\le d^2,t_c\le d^2)$ is given by expressions (14) and (15) wherein $\|s_b\|^2=\beta$, $\|s_c^k\|^2=\gamma$, $s_b^*s_c^k=\delta$, and $\|s_c\|^2=\eta$.

Proof: Follows from the above discussions. □

Though we do not give enumeration for $L>2$, the variance of complexity of the sphere-decoding algorithm for those cases can, in principle, be found by calculating summation (13) over all possible pairs of points (s_b,s_c).

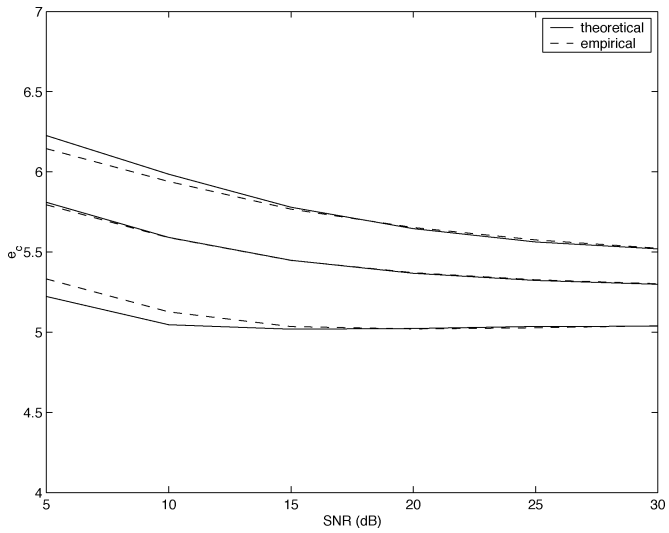

Fig. 7. Example with $m = n = 2$, $L = 2$. The curves from the top to the bottom are the exponents for the expected complexity, the expected complexity plus one standard deviation, and the expected complexity minus one standard deviation, respectively. The solid lines are obtained theoretically, and the dashed lines are obtained empirically from the flop count in MATLAB 5.

We illustrate the variance results summarized in Theorem 1 on an example with $m = n = 2$, $L = 2$. The middle curve in Fig. 7 is the expected complexity exponent. The top curve in Fig. 7 corresponds to the exponent of the expected complexity plus one standard deviation, and the bottom curve corresponds to the exponent of the expected complexity minus one standard deviation. The variance is computed using Theorem 1, where the integral in (15) is computed numerically, using *Mathematica*.

VI. Sphere Decoding for Detection in Frequency-Selective Channels

The sphere-decoding algorithm that we considered in Part I assumes no special structure on the channel matrix H and requires computing its QR factorization. In this section, we describe how the sphere-decoding idea can be employed for detection on frequency-selective channels directly, without performing the QR factorization of the corresponding (banded Toeplitz) channel matrix. This observation was first made in [9]. Furthermore, we consider the expected complexity of the algorithm for this special case of the lattice-generating matrix. To this end, consider the frequency-selective channel model in Fig. 8, with the input/output relation given by

$$x_i = \sum_{j=1}^{l} h_j s_{i-j+1} + v_i$$

where h_i, $i = 1, \ldots, l$ are the coefficients of the channel impulse response assumed to be Gaussian $\mathcal{N}(0,1)$, s_i is the ith

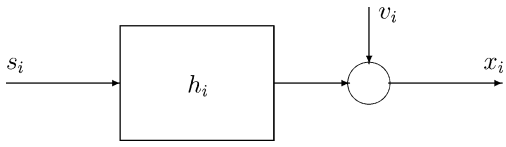

Fig. 8. Frequency-selective channel.

symbol in a transmitted sequence (chosen from an L-PAM constellation), and v_i denotes Gaussian $\mathcal{N}(0, \sigma^2)$ noise.[2] The data is assumed to be transmitted in blocks of T symbols, which are separated by guard intervals of $l-1$ symbols. To employ the sphere-decoding algorithm, we write the channel model as

$$x = Hs + v \tag{17}$$

where $s = [s_1 s_2 \ldots s_T]^* \in \mathcal{D}_L^T$ is the vector of the transmitted data sequence, $x = [x_1 x_2 \ldots x_{T+l-1}]^*$ is the vector of the received sequence, and $v = [v_1 v_2 \ldots v_{T+l-1}]^*$ is the vector of an additive white Gaussian noise. The matrix $H \in \mathcal{R}^{(T+l-1)\times T}$ is given by

$$H = \begin{bmatrix} h_1 & & & \\ h_2 & h_1 & & \\ \vdots & \ddots & \ddots & \\ h_l & \ddots & \ddots & h_1 \\ & h_l & \ddots & h_2 \\ & & \ddots & \vdots \\ & & & h_l \end{bmatrix}.$$

Here is where the banded Toeplitz structure of H comes in handy. Recall that the lattice point Hs lies in a sphere of radius d if and only if

$$d^2 \geq \|x - Hs\|^2. \tag{18}$$

The right-hand side of (18) can be expanded as

$$d^2 \geq (x_{T+l-1} - h_l s_T)^2 + (x_{T+l-2} - h_l s_{T-1} - h_{l-1} s_T)^2 + \ldots \tag{19}$$

where the first term depends only on s_T, the second term on $\{s_T, s_{T-1}\}$, and so on. Therefore, considering the first term only, a necessary condition for Hs to lie inside the sphere is that

$$d^2 \geq (x_{T+l-1} - h_l s_T)^2.$$

This condition is equivalent to s_T belonging to the interval[3]

$$\left\lceil \frac{-d + x_{T+l-1}}{h_l} \right\rceil \leq s_T \leq \left\lfloor \frac{d + x_{T+l-1}}{h_l} \right\rfloor. \tag{20}$$

[2]We have assumed a real model to follow [9]. Both the algorithm, as well as the complexity analysis, can be easily extended to the (perhaps more realistic) complex model. However, in the interest of space, we shall refrain from considering also the complex case. The complexity analysis in the real case is already quite involved (including a certain enumeration of integer-entried Toeplitz matrices), and the interested reader should be able to extend our results in a straightforward fashion.

[3]We assume that $h_l > 0$. Note that the boundaries of intervals here and below change when dividing by $h_l < 0$.

Of course, (20) is by no means sufficient. For every s_T satisfying (20), defining

$$d_{T-1}^2 = d^2 - (x_{T+l-1} - h_l s_T)^2$$

and

$$x_{T-1|T} = x_{T+l-2} - h_{l-1} s_T$$

a stronger necessary condition can be found by looking at the first two terms in (19), which leads to s_{T-1} belonging to the interval

$$\left\lceil \frac{-d_{T-1} + x_{T-1|T}}{h_l} \right\rceil \le s_{T-1} \le \left\lfloor \frac{d_{T-1} + x_{T-1|T}}{h_l} \right\rfloor. \quad (21)$$

One can continue in a similar fashion for s_{T-2} and so on until s_1. However, these T conditions used to find s are necessary but still not sufficient. Only if an additional constraint

$$\begin{aligned} d_0^2 &= d_1^2 - (x_{1|2} - h_l s_1)^2 \\ &\ge (x_{l-1} - h_{l-1}s_1 - \ldots - h_1 s_{l-1})^2 + \ldots \\ &\quad + (x_1 - h_1 s_1)^2 \end{aligned} \quad (22)$$

is satisfied will the point s indeed belong to the sphere, i.e., satisfy condition (18).

We can summarize the algorithm as follows.

Input: H, x, d.

1) Set $k = T$, $d_T^2 = d^2$, $x_{T|T+1} = x_{T+l-1}$
2) (Bounds for s_k) Set $UB(s_k) = \lfloor (d_k + x_{k|k+1})/h_l \rfloor$, $s_k = \lceil (-d_k + x_{k|k+1})/h_l \rceil - 1$
3) (Increase s_k) $s_k = s_k + 1$. If $s_k \le UB(s_k)$ go to 5, else to 4.
4) (Increase k) $k = k + 1$; if $k = T + 1$, terminate algorithm, else go to 3.
5) (Decrease k) If $k = 1$ go to 6. Else $k = k - 1$, $x_{k|k+1} = x_{k+l-1} - \sum_{j=k+1}^{\min(k+l,T)} h_{l+k-j} s_j$, $d_k^2 = d_{k+1}^2 - (x_{k+1|k+2} - h_l s_{k+1})^2$.
6) If $d_0^2 = d_1^2 - (x_{1|2} - h_l s_1)^2 \ge (x_{l-1} - h_{l-1}s_1 - \ldots - h_1 s_{l-1})^2 + \ldots + (x_1 - h_1 s_1)^2$, solution found. Save s and its distance from x, $d_T^2 - d_0^2 + (x_{l-1} - h_{l-1}s_1 - \ldots - h_1 s_{l-1})^2 + \ldots + (x_1 - h_1 s_1)^2$, and go to 3.

Remark: One can immediately notice a potential drawback to the aforementioned algorithm. The additional constraint (22) means that the T previously considered constraints might have not been particularly stringent. This would clearly have negative impact on the complexity. Indeed, as we shall argue shortly, we observe that there are scenarios where performing the QR factorization and then employing sphere decoding may, in fact, be the more favorable approach.

A. Expected Complexity of Sphere Decoding Algorithm for Frequency-Selective Channels

For simplicity, we will assume that $T \ge l$ (the case $T < l$ is treated similarly). To find the expected complexity of sphere decoding for a banded Toeplitz matrix H, we follow the procedure outlined in Part I. First, note that (18) can be written as

$$\begin{aligned} d^2 \ge \|x^T - H_{T,T} s\|^2 \\ + \left\| x - \begin{bmatrix} 0_{(l-1)\times 1} \\ x^T \end{bmatrix} - \left(H - \begin{bmatrix} 0_{(l-1)\times T} \\ H_{T,T} \end{bmatrix} \right) s \right\|^2 \end{aligned}$$

where x^T is the T-dimensional vectors comprised of the last T entries of the vector x, and $H_{T,T}$ is the matrix comprised of the last T rows of H. Then, the algorithm described in the previous section visits all T-dimensional points s such that

$$d^2 \ge \|x^T - H_{T,T} s\|^2$$

while the additional constraint in step 6 of the pseudo-code ensures that the stricter condition (18) is satisfied. Suppose that the lattice point s_t was transmitted and that the vector $x = Hs_t + v$ was observed. To find the expected number of the T-dimensional points tested in step 6 of the code, we need to compute the probability that for an arbitrary lattice point s_a

$$\|x^T - H_{T,T} s_a\|^2 = \left\| v^T + H_{T,T}(s_t - s_a) \right\|^2 \le d^2$$

where v^T is a T-dimensional vector comprised of the last T entries of the vector v. The expected number of points in a T-dimensional sphere of radius d can now be found as

$$E_p(T, d^2) = \sum_{(s_t, s_a)} p\left(\left\| v^T + H_{T,T}(s_t - s_a) \right\|^2 \le d^2 \right)$$

where the summation is over all pairs of points (s_t, s_a).

A similar expression holds for an expected number of points in a k-dimensional sphere $k < T$. In particular

$$E_p(k, d^2) = \sum_{(s_t^k, s_a^k)} p\left(\left\| v^k + H_{k,k}\left(s_t^k - s_a^k\right) \right\|^2 \le d^2 \right)$$

where v^k, s_t^k, and s_a^k are k-dimensional vectors, and $H_{k,k}$ is a $k \times k$ matrix obtained by the partitions

$$v = \begin{bmatrix} v^{T+l-1-k} \\ v^k \end{bmatrix}, \quad s_t = \begin{bmatrix} s_t^{T-k} \\ s_t^k \end{bmatrix}, \quad s_a = \begin{bmatrix} s_a^{T-k} \\ s_a^k \end{bmatrix}$$

$$H = \begin{bmatrix} H_{T-k+l-1,T-k} & H_{T-k+l-1,k} \\ H_{k,T-k} & H_{k,k} \end{bmatrix}.$$

In Appendix B, we show that the probability that a point $H_{k,k} s_a^k$ belongs to the k-dimensional sphere of radius d is

$$\begin{aligned} p\left(\left\| v^k + H_{k,k}\left(s_t^k - s_a^k\right) \right\|^2 \le d^2 \right) \\ = \frac{1}{2\pi} \int_{t=0}^{d^2} \int_{\omega=-\infty}^{\infty} \Phi_{k,l}(\omega) e^{-j\omega t} d\omega dt \end{aligned} \quad (23)$$

where

$$\Phi_{k,l}(\omega) = \frac{\sqrt{2^{k+q}}}{\sqrt{(1+j\omega 2\sigma^2)^{k-q}\prod_{i=1}^{q}[1+j\omega 2(\sigma^2+\lambda_i)]}} \tag{24}$$

is the characteristic function of $\|v^k + H_{k,k}(s_t^k - s_a^k)\|^2$, and $q = \min(k,l)$. Furthermore, λ_i, $i = 1,\ldots,q$ are the eigenvalues of the matrix $(\mathcal{S}_t - \mathcal{S}_a)^*(\mathcal{S}_t - \mathcal{S}_a)$, where, for $k \le l$, $\mathcal{S}_t$ and $\mathcal{S}_a$ are $k \times k$ matrices defined as

$$\mathcal{S}_t = \begin{bmatrix} s_{t,T} & \cdots & & s_{t,T-k+1} \\ & s_{t,T} & & \vdots \\ & & \ddots & s_{t,T-1} \\ & & & s_{t,T} \end{bmatrix}$$

$$\mathcal{S}_a = \begin{bmatrix} s_{a,T} & \cdots & & s_{a,T-k+1} \\ & s_{a,T} & & \vdots \\ & & \ddots & s_{a,T-1} \\ & & & s_{a,T} \end{bmatrix} \tag{25}$$

while for $k > l$, they are $k \times l$ matrices defined as

$$\mathcal{S}_t = \begin{bmatrix} s_{t,T-k+l} & \cdots & & s_{t,T-k+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{t,T} & \cdots & & s_{t,T-l+1} \\ & s_{t,T} & & \vdots \\ & & \ddots & s_{t,T-1} \\ & & & s_{t,T} \end{bmatrix}$$

$$\mathcal{S}_a = \begin{bmatrix} s_{a,T-k+l} & \cdots & & s_{a,T-k+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{a,T} & \cdots & & s_{a,T-l+1} \\ & s_{a,T} & & \vdots \\ & & \ddots & s_{a,T-1} \\ & & & s_{a,T} \end{bmatrix}. \tag{26}$$

The expected complexity of the sphere-decoding algorithm is given by [cf. (18), Part I]

$$C(T,\sigma^2,d^2) = \sum_{k=1}^{T} (\text{expected \# of points in } k-\text{dim sphere of radius } d) \cdot f_{p,\text{Toep}}(k).$$

From the pseudo-code of the sphere-decoding algorithm for a banded Toeplitz lattice-generating matrix H given in the previous section, we find that the number of elementary operations per point in a k-dimensional sphere is

$$f_{p,\text{Toep}}(k) = \begin{cases} 2\cdot\min(T-k+l+1,T) \\ \quad -2(T-k)+9+2L, & k<T \\ l(l-1)+11+2L, & k=T. \end{cases}$$

Note that $f_{p,\text{Toep}}(T)$ includes the number of operations for testing the additional constraint in step 6 of the code. Combining all of the above, we can write the expression for the expected complexity as

$$C(T,\sigma^2,d^2) = \sum_{k=1}^{T} f_{p,\text{Toep}}(k) \times \sum_{(s_t^k,s_a^k)} \frac{1}{2\pi} \int_{t=0}^{d^2} \int_{\omega=-\infty}^{\infty} \Phi_{k,l}(\omega) e^{-j\omega t} d\omega dt \tag{27}$$

where $\Phi_{k,l}(\omega)$ is given by (24).

For given l and k, one can often find the closed-form expression for the probability (23). [In many cases, (23) is a linear combination of a number of incomplete gamma functions.] Alternatively, one can compute (23) by means of numerical integration (with, e.g., *Mathematica* or *MATLAB*). However, the more pressing problem is one of finding an efficient enumeration of the eigenvalues of the matrix $(\mathcal{S}_t - \mathcal{S}_a)^*(\mathcal{S}_t - \mathcal{S}_a)$ over the lattice, i.e., counting the number of pairs of points (s_t, s_a) that yield the particular set of eigenvalues of $(\mathcal{S}_t - \mathcal{S}_a)^*(\mathcal{S}_t - \mathcal{S}_a)$. Unfortunately, unlike the enumeration via generating functions in Part I of the paper, this enumeration appears to be difficult to obtain. Thus, we leave the expression for the expected complexity of sphere decoding for a banded Toeplitz H in the form (27). Note that for small dimensional problems (i.e., problems with small l and T), one can compute (27) by actually going over all possible pairs of points (s_t^k, s_a^k), $k = 1,2,\ldots,T$.

B. Some Comments

In the previous section, we considered the expected complexity of sphere decoding that exploits the banded Toeplitz structure of the channel matrix H. However, there is a range of system parameters l, T, and L, for which it is more efficient to first perform the QR factorization of H. This is due to the fact that the sphere decoding that directly uses H may impose less strict conditions on lattice points than the sphere decoding that uses the upper-triangular matrix R from the QR factorization—as implied by the need to impose additional conditions (22) when doing the former. The matrices Q and R obtained from the QR factorization of the banded Toeplitz H do not have as nice statistical properties as Q and R obtained from the factorization of the full, Gaussian i.i.d. matrix H. Hence, we illustrate the previous point by means of simulations.

For illustration, consider an example with $l = 12$, $T = 20$, and $L = 2$. In Fig. 9, we plot the (empirically calculated) complexity exponent e_c as a function of SNR. Note that in the range of SNRs where the bit-error rate (BER) performance is $< 10^{-3}$, the complexity of the sphere-decoding algorithm that exploits the Toeplitz structure of the matrix H is always less than the combined complexity of the QR factorization and the standard sphere decoding that makes use of the matrix R.

On the other hand, consider the case with $l = 8$, $T = 16$, and $L = 4$. As Fig. 10 shows, the range of SNRs where the sphere decoding with QR factorization is more preferable than the sphere decoding that exploits the Toeplitz structure of H is quite wide. In fact, only in the range of BER that are $< 10^{-4}$ does the algorithm that exploits the Toeplitz structure of H become preferable.

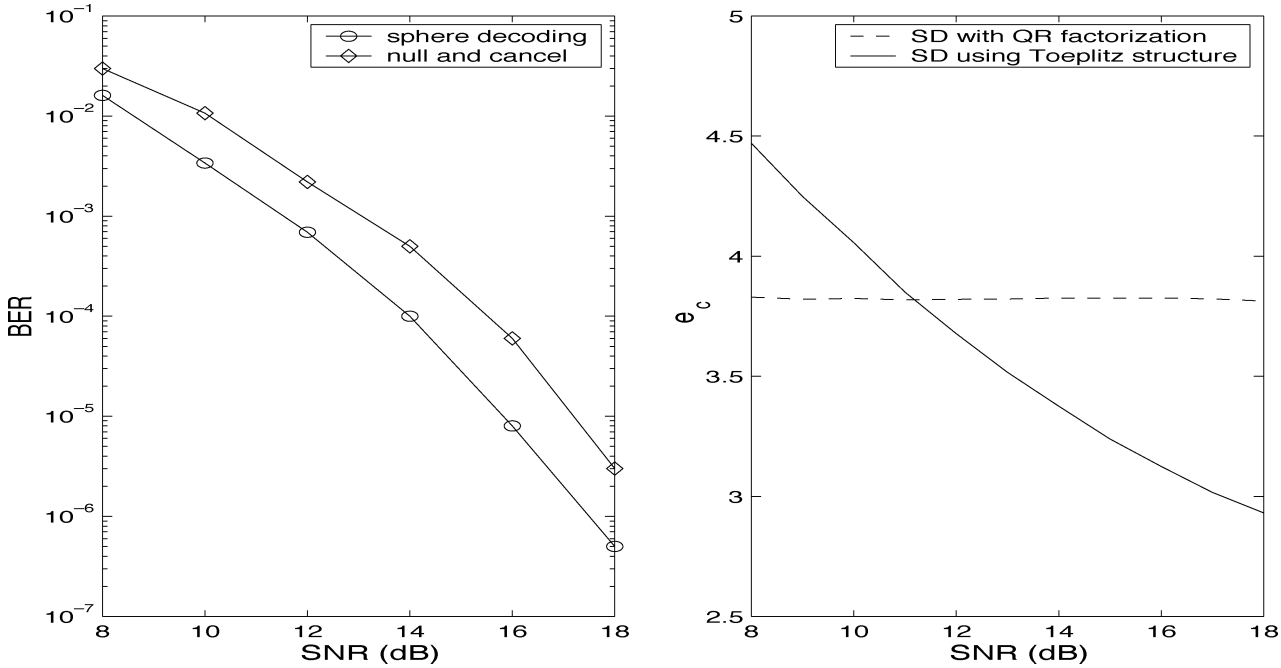

Fig. 9. BER performance and the expected complexity exponent of sphere decoding, $T = 20, l = 12, L = 2$. The plot on the right-hand side shows both the complexity exponent of the algorithm that uses the Toeplitz structure of H and the exponent of the algorithm that uses QR factorization (for the latter, the complexity of the QR factorization is included).

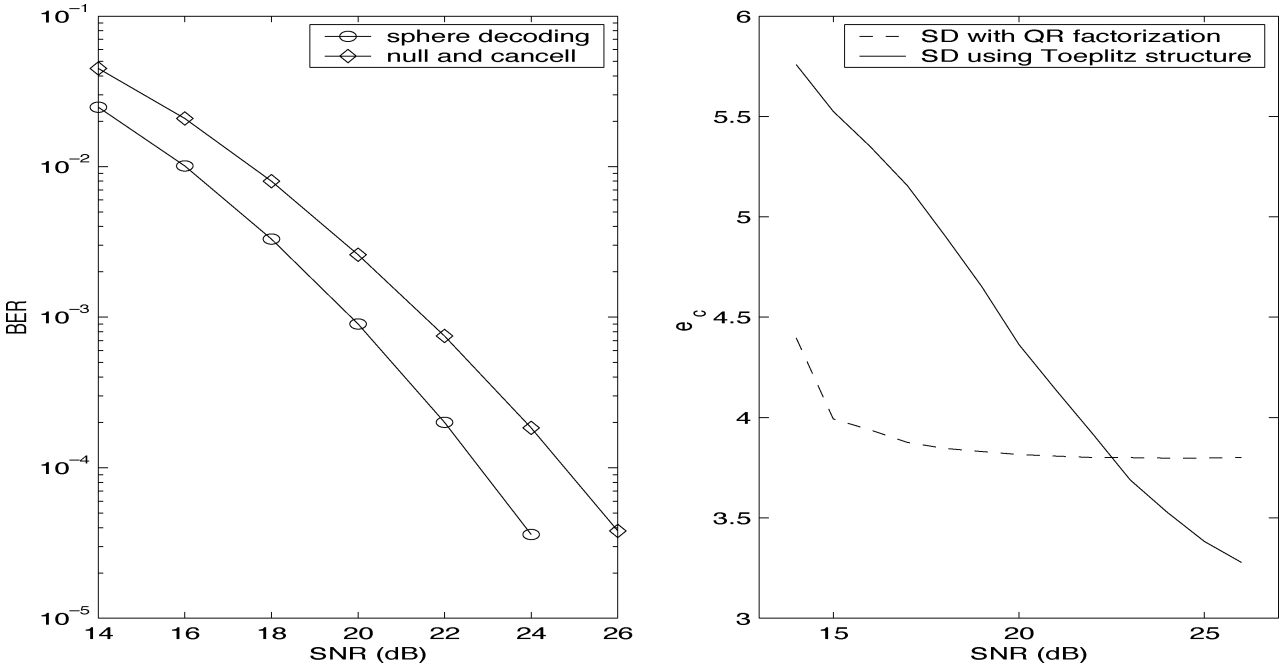

Fig. 10. BER performance and the expected complexity exponent of sphere decoding, $T = 16, l = 8, L = 4$. The plot on the right-hand side shows both the complexity exponent of the algorithm that uses the Toeplitz structure of H and the exponent of the algorithm that uses QR factorization (for the latter, the complexity of the QR factorization is included).

Note that the Viterbi algorithm, which has the same performance as sphere decoding permitting a guard interval, has the complexity that is exponential in the channel length and is linear in the block length T. Therefore, for the example in Fig. 10, the complexity of the Viterbi algorithm is on the order of $TL^l \sim 10^6$ flops. On the other hand, the sphere-decoding algorithm solves the same ML detection problem with $T^{e_c} \sim 10^4$ flops on average, which is a considerable computational saving. Sphere decoding offers computational savings over the Viterbi algorithm for this particular set of parameters and, in general, for the cases where the length of the channel is large. However, for short channels, low modulation schemes, and very long block lengths, the Viterbi algorithm has lower (essentially linear in the data block length) complexity than the sphere decoding.

VII. Remarks

In this and in Part I of the paper, we studied the complexity of sphere decoding for finding an m-dimensional vector s so that Hs is the closest lattice point to the given n-dimensional vector x, i.e., we studied the complexity of sphere decoding employed for solving

$$\min_{s\in\mathcal{D}_L^m} ||x - Hs||^2$$

when $n \geq m$. On the other hand, for a finite lattice $\mathcal{D}_L^m$, one can employ sphere decoding for solving the same problem, even when $n < m$, provided that one performs an additional partial exhaustive search over the remaining $m - n$ dimensions. We omit the details for brevity. However, it is easy to see that the expected complexity of this scheme is given by

$$C(n, m, \rho, d^2) = C(m, \rho, d^2) \cdot L^{m-n}$$

where $C(m, \rho, d^2)$ is given by Theorem 2 in Part I.

On another note, the expected complexity that we discussed in this paper accounts for finding all the lattice points in the sphere. The point among those found that is closest to x is the solution to the integer least-squares problem. There are some more efficient variations on the basic sphere-decoding algorithm that potentially avoid having to search all lattice points inside the sphere. We briefly mention two variations here.

- *Sphere decoding with radius update*

  Whenever the algorithm finds a point s_{in} inside the sphere (note that Hs_{in} is not necessarily the closest point to x), we set the new radius of the sphere $d^2 = ||x - Hs_{in}||^2$ and restart the algorithm. The radius update may be particularly useful at lower SNRs, where the number of points in the initial sphere is relatively large. However, it may not be beneficial at high SNR, since restarting the sphere decoder may be costly. In any event, computing the expected complexity for this modification of sphere decoding appears to be complicated, since it requires the calculation of the distribution of the radii that are updated.
- *Schnorr–Euchner version of sphere decoding*

  This strategy was proposed in [15]. The likelihood that the point will be found early is maximized if the search at each dimension k is performed from the middle of the allowed interval for s_k and if the radius update strategy (as described above) is used. In particular, recall step 2 of the sphere-decoding algorithm in Section 3.1 of Part I. There, we set the upper and the lower bounds on s_k

$$LB(s_k) = \left\lceil \frac{-d'_k + y_{k|k+1}}{r_{k,k}} \right\rceil - 1, \quad UB(s_k) = \left\lfloor \frac{d'_k + y_{k|k+1}}{r_{k,k}} \right\rfloor$$

  and the search for s_k was performed by examining the points

$$LB(s_k),\ LB(s_k) + 1,\ \ldots,\ UB(s_k).$$

  In the Schnorr–Euchner version of the sphere-decoding algorithm, however, one starts from

$$[\hat{s}_k] = \left[\frac{y_{k|k+1}}{r_{k,k}} \right]$$

  where $[\cdot]$ denotes rounding to the nearest element in the set spanning the lattice and performs the search in the order of, say,

$$[\hat{s}_k],\ [\hat{s}_k] - 1,\ [\hat{s}_k] + 1, \ldots$$

  The expected complexity of the Schnorr–Euchner version of the sphere-decoding algorithm is no greater than the expected complexity of the basic algorithm that we derived in Part I. However, computing its expected complexity in a closed form appears to be formidable. More details about the Schnorr–Euchner version of the sphere decoding, and some improvements thereof, can be found in [3].

VIII. Conclusion

In this paper, we generalized the results on the expected complexity of sphere decoding to the complex version of the problem. We also calculated second-order statistics, i.e., we found the variance of the complexity of sphere decoding. Moreover, we studied applications of sphere decoding to communication systems. In particular, we considered the application to ML detection in multiantenna systems. Furthermore, we studied the expected complexity of the sphere-decoding algorithm for frequency-selective channels. In both cases, it turns out that over a wide range of SNRs, rates, and dimensions, the expected complexity is often cubic or subcubic. Since many communications systems operate at noise levels for which this is the case, this suggests that ML decoding, which was hitherto thought to be computationally intractable, can, in fact, be implemented with complexity similar to heuristic methods but with significant performance gains—a result with many practical implications.

There are quite a few open problems that remain and possible directions for further work and research. With regards to finite impulse response (FIR) channels, there is a need for an efficient (number-theoretic) enumeration technique that would result in a more explicit complexity expression. Second-order statistics for the FIR case also need to be computed. On a different note, for FIR channels, the sphere-decoding algorithm does not at all exploit the Markovian property of the channel, which is precisely what the Viterbi algorithm does. Practical algorithms that combine both structures (the lattice and the Markovian property) are highly desirable, and some steps in this direction have been taken in [16]. In this paper, we have considered only real- (or complex-) valued lattices. ML decoding of linear error-correcting codes can be viewed as finding closet lattice points (in a Hamming distance sense) generated in Galois field. Moreover, when error-correcting codes are coupled with analog channels (through some modulation scheme), problems of joint detection and decoding arise. Some preliminary work using the ideas of this paper appear in [17].

Finally, we should remark that an important message of this two-part paper is that, for problems where there is an underlying statistical model, the complexity of any algorithm is best viewed as a random variable (see also [18] and the references therein). A methodology for how to determine the statistics for one such algorithm has been presented in this paper; however, we believe that the general approach may find applications in other areas (other than closest point searches) as well.

APPENDIX A
CALCULATION OF THE PROBABILITY $p(t_b \le d^2, t_c \le d^2)$

Recall that

$$t_b = \|u^k + R_{k,k}s_b\|^2 \quad \text{and} \quad t_c = \|u^l + R_{l,l}s_c\|^2.$$

We distinguish between the following two cases: $s_b = s_c^k$ and $s_b \neq s_c^k$, where s_c^k denotes a vector comprised of the last k entries of s_c.

1) $s_b = s_c^k$: Since $k \le l$, if $R_{l,l}s_c$ belongs to the l-dimensional sphere of radius d, then it must be that $R_{k,k}s_b$ belongs to the k-dimensional sphere of radius d and, therefore

$$p(t_b \le d^2, t_c \le d^2) = p(t_c \le d^2).$$

However, from (20) in Part I of the paper

$$p(t_c \le d^2) = \gamma\left(\frac{d^2}{2(\sigma^2 + \|s_c\|^2)}, \frac{l}{2}\right).$$

2) $s_b \neq s_c^k$: To find $p(t_b \le d^2, t_c \le d^2)$, we consider the characteristic function of (t_b, t_c)

$$\Phi(\omega_b, \omega_c) = Ee^{j\omega_b t_b + j\omega_c t_c}.$$

Denote

$$\nu_b = u^k + R_{k,k}s_b, \quad \nu_c = u^l + R_{l,l}s_c.$$

Consider two entries $\nu_{b,i}$ and $\nu_{c,j}$ of the vectors ν_b and ν_c

$$\nu_{b,i} = u_{m-k+i} + r_{m-k+i,m-k+i}s_{b,i} + \sum_{q=i+1}^{k} r_{m-k+i,m-k+q}s_{b,q} \tag{28}$$

and

$$\nu_{c,j} = u_{m-l+j} + r_{m-l+j,m-l+j}s_{c,j} + \sum_{q=j+1}^{l} r_{m-l+j,m-l+q}s_{c,q} \tag{29}$$

where $r_{i,j}$ is the (i,j) entry of matrix R. The $r_{i,i}^2$ are independent, with χ^2-distribution of $m-i+1$ degrees of freedom, while the nondiagonal entries $r_{i,j}$ are independent Gaussian (see, e.g., [19]). Therefore, $\nu_{b,i}$ and $\nu_{c,j}$ are independent for $m-k+i \neq m-l+j$. So, ν_c^{l-k} is independent from ν_b, where ν_c^{l-k} is defined by the partition

$$\nu_c = \begin{bmatrix} \nu_c^{l-k} \\ \nu_c^k \end{bmatrix}.$$

Hence, we can write

$$\begin{aligned}\Phi(\omega_b, \omega_c) &= Ee^{j\omega_b t_b + j\omega_c t_c} \\ &= Ee^{j\omega_b\|\nu_b\|^2 + j\omega_c\|\nu_c^k\|^2} \cdot Ee^{j\omega_c\|\nu_c - \nu_c^k\|^2} \\ &= \Phi_1(\omega_b, \omega_c)\Phi_2(\omega_c).\end{aligned} \tag{30}$$

Furthermore

$$\begin{aligned}\Phi_2(\omega_c) &= Ee^{j\omega_c\|\nu_c - \nu_c^k\|^2} \\ &= Ee^{j\omega_c(\nu_{c,1}^2 + \ldots + \nu_{c,l-k}^2)} \frac{Ee^{j\omega_c(\nu_{c,l-k+1}^2 + \ldots + \nu_{c,l}^2)}}{Ee^{j\omega_c(\nu_{c,l-k+1}^2 + \ldots + \nu_{c,l}^2)}} \\ &= \frac{Ee^{j\omega_c\|\nu_c\|^2}}{Ee^{j\omega_c\|\nu_c^k\|^2}}.\end{aligned} \tag{31}$$

To calculate $\Phi_1(\omega_b, \omega_c)$, we need to find joint distribution for $(\nu_{b,i}, \nu_{c,j})$. However, for $\nu_{b,i}$ and $\nu_{c,j}$ given by (28) and (29), it is difficult to do so. Instead, we can consider an equivalent problem that is quite easier to solve. To this end, recall Lemma 1 in Part I, which asserts that $R_{k,k}$ has the same distribution as the upper triangular matrix obtained from the QR factorization of a $k \times k$ matrix G comprised of i.i.d. Gaussian entries. This implies that if we choose any isotropically random unitary matrix Q, independent of $R_{k,k}$, the matrix $QR_{k,k}$ will have a Gaussian distribution with i.i.d. $\mathcal{CN}(0,1)$ entries. In particular, if Q_b is an isotropically distributed unitary matrix, we can write

$$z_b = Q_b^*\nu_b = Q_b^*u^k + Q_b^*R_{k,k}s_b = w + Gs_b$$

where $w = Q_b^*u^k$ and $G = Q_b^*R_{k,k}$ have i.i.d. Gaussian entries. Similarly

$$z_c = Q_b^*\nu_c^k = w + Gs_c^k. \tag{32}$$

Thus, the ith entry of z_b and the jth entry of z_c can be written as

$$z_{b,i} = w_i + \sum_{q=1}^{k} g_{i,q}s_{b,q}$$

and

$$z_{c,j} = w_j + \sum_{q=1}^{k} g_{j,q}s_{c,q}.$$

We note that $z_{b,i}$ and $z_{c,j}$ are independent for $i \neq j$ and jointly Gaussian otherwise, i.e.,

$$(z_{b,i}, z_{c,j}) \sim \mathcal{N}\left(\begin{bmatrix}0\\0\end{bmatrix}, \Sigma_{bc}\right)\delta_{ij}$$

where

$$\Sigma_{bc} = \begin{bmatrix} \|s_b\|^2 + \sigma^2 & s_b^*s_c^k + \sigma^2 \\ s_a^*s_b^k + \sigma^2 & \|s_c^k\|^2 + \sigma^2 \end{bmatrix} = \begin{bmatrix} a_{bb} & a_{bc} \\ a_{bc} & a_{cc} \end{bmatrix}$$

is the covariance matrix of the joint Gaussian probability density function $f(z_{b,i}, z_{c,j})$. Therefore, the characteristic function $\Phi_1(\omega_b, \omega_c)$ can be written as

$$\begin{aligned}\Phi_1(\omega_b,\omega_c) &= Ee^{j\omega_b\|z_b\|^2+j\omega_c\|z_c\|^2}\\ &= Ee^{j\omega_b\left(z_{b,1}^2+\ldots+z_{b,k}^2\right)+j\omega_c\left(z_{c,1}^2\ldots+z_{c,k}^2\right)}\\ &= Ee^{j\omega_b z_{b,1}^2+j\omega_c z_{c,1}^2}Ee^{j\omega_b z_{b,2}^2+j\omega_c z_{c,2}^2}\cdots\\ &\quad Ee^{j\omega_b z_{b,k}^2+j\omega_c z_{c,k}^2}\\ &= \left(Ee^{j\omega_b z_{b,1}^2+j\omega_c z_{c,1}^2}\right)^k.\end{aligned}$$

Recall that we denoted $\det\Sigma_{bc} = a_{bb}a_{cc} - a_{bc}^2 = \Delta$. Therefore, we can write

$$\begin{aligned}&Ee^{j\omega_b z_{b,1}^2+j\omega_c z_{c,1}^2}\\ &\quad= \iint e^{j\omega_b z_{b,1}^2+j\omega_c z_{c,1}^2} f(z_{b,1}, z_{c,1})dz_{b,1}dz_{c,1}\\ &\quad= \frac{1}{\sqrt{(2\pi)^2\Delta}}\iint e^{j\omega_b z_{b,1}^2+j\omega_c z_{c,1}^2}\\ &\qquad\cdot e^{-\frac{1}{2}[z_{b,1}\ \ z_{c,1}]\Sigma_{bc}^{-1}\begin{bmatrix}z_{b,1}\\ z_{c,1}\end{bmatrix}}dz_{b,1}dz_{c,1}\\ &\quad= \frac{1}{\sqrt{(2\pi)^2\Delta}}\\ &\qquad\times\iint e^{-\frac{1}{2}[z_{b,1}\ \ z_{c,1}]\begin{bmatrix}\frac{a_{cc}}{\Delta}-2j\omega_b & -\frac{a_{bc}}{\Delta}\\ -\frac{a_{bc}}{\Delta} & \frac{a_{bb}}{\Delta}-2j\omega_c\end{bmatrix}\begin{bmatrix}z_{b,1}\\ z_{c,1}\end{bmatrix}}\\ &\qquad\times dz_{b,1}dz_{c,1}\\ &\quad= \frac{1}{\sqrt{\Delta\left[\left(\frac{a_{bb}}{\Delta}-2j\omega_c\right)\left(\frac{a_{cc}}{\Delta}-2j\omega_b\right)-\frac{a_{bc}^2}{\Delta^2}\right]}}\end{aligned}$$

and thus, we have

$$\Phi_1(\omega_b,\omega_c) = \frac{1}{\sqrt{\Delta^k\left[\left(\frac{a_{bb}}{\Delta}-2j\omega_c\right)\left(\frac{a_{cc}}{\Delta}-2j\omega_b\right)-\frac{a_{bc}^2}{\Delta^2}\right]^k}}. \tag{33}$$

On the other hand, using (32), the denominator of (31) can be written as

$$\begin{aligned}Ee^{j\omega_c\left\|\nu_c^k\right\|^2} &= Ee^{j\omega_c\|z_c\|^2} = Ee^{j\omega_c\left(z_{c,1}^2+\ldots+z_{c,k}^2\right)}\\ &= \left(Ee^{j\omega_c z_{c,1}^2}\right)^k.\end{aligned}$$

Note that $Ez_{c,1}^2 = \sigma^2 + \|s_c^k\|^2 = a_{cc}$, and hence, we can write

$$\begin{aligned}Ee^{j\omega_c z_{c,1}^2} &= \frac{1}{\sqrt{2\pi a_{cc}}}\int e^{j\omega_c z_{c,1}^2-\frac{z_{c,1}^2}{2a_{cc}}}dz_{c,1}\\ &= \frac{1}{\sqrt{1-2j\omega_c\left(\sigma^2+\|s_c^k\|^2\right)}}\end{aligned}$$

and thus, we have

$$Ee^{j\omega_c\|\nu_c^k\|^2} = \frac{1}{\sqrt{\left(1-2j\omega_c\left(\sigma^2+\|s_c^k\|^2\right)\right)^k}}.$$

Similarly, the numerator of (31) can be written as

$$Ee^{j\omega_c\|\nu_c\|^2} = \frac{1}{\sqrt{\left(1-2j\omega_c\left(\sigma^2+\|s_c\|^2\right)\right)^l}}.$$

Combining the two expressions above, we obtain

$$\Phi_2(\omega_c) = \frac{\sqrt{\left(1-2j\omega_c\left(\sigma^2+\|s_c^k\|^2\right)\right)^k}}{\sqrt{\left(1-2j\omega_c\left(\sigma^2+\|s_c\|^2\right)\right)^l}}. \tag{34}$$

Finally, combining (33) and (34), we obtain

$$\begin{aligned}\Phi(\omega_b,\omega_c) = &\frac{1}{\Delta^{\frac{k}{2}}\left[\left(\frac{a_{bb}}{\Delta}-2j\omega_c\right)\left(\frac{a_{cc}}{\Delta}-2j\omega_b\right)-\frac{a_{bc}^2}{\Delta^2}\right]^{\frac{k}{2}}}\\ &\times\frac{\left(1-2j\omega_c\left(\sigma^2+\left\|s_c^k\right\|^2\right)\right)^{\frac{k}{2}}}{\left(1-2j\omega_c\left(\sigma^2+\|s_c\|^2\right)\right)^{\frac{l}{2}}}.\end{aligned} \tag{35}$$

The probability density function can be found by taking the inverse Fourier transform of the characteristic function in (35)

$$\begin{aligned}\phi(t_b,t_c) &= \mathcal{F}^{-1}\left[\Phi(\omega_b,\omega_c)\right]\\ &= \frac{1}{4\pi^2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{d\omega_b d\omega_c e^{-j\omega_b t_b-j\omega_c t_c}}{\Delta^{\frac{k}{2}}\left[\left(\frac{a_{bb}}{\Delta}-2j\omega_c\right)\left(\frac{a_{cc}}{\Delta}-2j\omega_b\right)-\frac{a_{bc}^2}{\Delta^2}\right]^{\frac{k}{2}}}\\ &\quad\times\frac{\left(1-2j\omega_c\left(\sigma^2+\left\|s_c^k\right\|^2\right)\right)^{\frac{k}{2}}}{\left(1-2j\omega_c\left(\sigma^2+\|s_c\|^2\right)\right)^{\frac{l}{2}}}\end{aligned}$$

and thus, the probability $p(t_b \le d^2, t_c \le d^2)$ can be found as

$$p(t_b\le d^2, t_c\le d^2) = \int_{t_b=0}^{d^2}\int_{t_c=0}^{d^2}\phi(t_b,t_c)dt_b dt_c.$$

Appendix B
Calculation of the Characteristic Function $\Phi(\omega)$ in Section VI-A

Note that we can write the random variable $\left\|v^k + H_{k,k}(s_t^k - s_a^k)\right\|^2$ as

$$\left\|v^k + H_{k,k}\left(s_t^k - s_a^k\right)\right\|^2 = \|v^k + \Lambda h^q\|^2 = \left\|[I_k \quad \Lambda]\begin{bmatrix}v^k\\ h^q\end{bmatrix}\right\|^2 \tag{36}$$

where $q = \min(k, l)$, the q-dimensional vector h^q, is defined as

$$h^q = [h_{l-q+1} h_{l-q+2} \dots h_l]^*$$

the $k \times q$ matrix Λ is defined as

$$\Lambda = \mathcal{S}_t - \mathcal{S}_a$$

and the matrices $\mathcal{S}_t$, $\mathcal{S}_a$ are given by (25) and (26).

The characteristic function of $\|v^k + H_{k,k}(s_t^k - s_a^k)\|^2$ can be found as

$$\begin{aligned}\Phi(\omega) &= E e^{j\omega \left\| v^k + H_{k,k}\left(s_t^k - s_a^k\right)\right\|^2} \\ &= \int_{-\infty}^{\infty} e^{j\omega \begin{bmatrix} v^{k*} & h^{q*} \end{bmatrix} \begin{bmatrix} I_k & \Lambda \\ \Lambda^* & \Lambda^*\Lambda \end{bmatrix} \begin{bmatrix} v^k \\ h^q \end{bmatrix}} \phi \\ &\quad \times e^{-\begin{bmatrix} v^{k*} & h^{q*} \end{bmatrix} \begin{bmatrix} \frac{1}{2\sigma^2} I_k & 0 \\ 0 & \frac{1}{2} I_q \end{bmatrix} \begin{bmatrix} v^k \\ h^q \end{bmatrix}} dh^q dv^k \quad (37)\end{aligned}$$

where

$$\phi = \frac{1}{\sqrt{(2\pi)^{k+q}\sigma^{2k}}}.$$

By simplifying the integrand in (37), we obtain

$$\begin{aligned}\Phi(\omega) &= \frac{1}{\sqrt{(2\pi)^{k+q}\sigma^{2k}}} \\ &\quad \times \int e^{-\begin{bmatrix} v^{k*} & h^{q*} \end{bmatrix} \underbrace{\begin{bmatrix} \left(\frac{1}{2\sigma^2} + j\omega\right) I_k & j\omega\Lambda \\ j\omega\Lambda^* & \frac{1}{2} I_q + j\omega\Lambda^*\Lambda \end{bmatrix}}_{=\mathcal{I}} \begin{bmatrix} v^k \\ h^q \end{bmatrix}} dv^k dh^q\end{aligned}$$

and, finally

$$\Phi(\omega) = \frac{1}{\sqrt{\sigma^{2k} \det \mathcal{I}}}$$

where the determinant of $\mathcal{I}$ is found as

$$\begin{aligned}\det \mathcal{I} &= \left(\frac{1}{2\sigma^2} + j\omega\right)^k \\ &\quad \times \det\left[\frac{1}{2} I_q + j\omega\Lambda^*\Lambda - j\omega\Lambda^* \frac{1}{\frac{1}{2\sigma^2} + j\omega} j\omega\Lambda\right] \\ &= \left(\frac{1 + j\omega 2\sigma^2}{2\sigma^2}\right)^k \det\left[\frac{1}{2} I_q + \frac{j\omega}{1 + j\omega 2\sigma^2}\Lambda^*\Lambda\right] \\ &= \frac{1}{2^{k+q}\sigma^{2k}} (1 + j\omega 2\sigma^2)^{k-q} \prod_{i=1}^{q} \left[1 + j\omega 2(\sigma^2 + \lambda_i)\right]\end{aligned}$$

where λ_i, $i = 1, \dots, q$ are the eigenvalues of the matrix $\Lambda^*\Lambda$. In evaluating $\det \mathcal{I}$, we used the matrix inversion lemma

$$\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det A \det(D - CA^{-1}B).$$

Combining all of the above, we obtain (24), i.e.,

$$\Phi(\omega) = \frac{\sqrt{2^{k+q}}}{\sqrt{(1 + j\omega 2\sigma^2)^{k-q} \prod_{i=1}^{q} \left[1 + j\omega 2(\sigma^2 + \lambda_i)\right]}}.$$

ACKNOWLEDGMENT

The authors would like to thank R. Gowaikar for useful discussions on simplifying the derivation in Appendix A.

REFERENCES

[1] E. Viterbo and E. Biglieri, "A universal decoding algorithm for lattice codes," in *Proc. Quatorzieme Colloque GRETSI*, 1993, pp. 611–614.
[2] A. Banihashemi and A. Khandani, "On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 162–171, Feb. 1998.
[3] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2001–2214, Aug. 2002.
[4] E. Viterbo and J. Boutros, "A universal lattice decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 1639–1642, Jul. 1999.
[5] L. Brunel and J. Boutros, "Euclidean space lattice decoding for joint detection in CDMA systems," in *Proc. IEEE Inf. Theory Commun. Workshop*, 1999, p. 129.
[6] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs. Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.
[7] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.
[8] B. Hassibi and B. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804–1824, Jul. 2002.
[9] W. H. Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," *IEEE Trans. Inf. Theory*, vol. 40, no. 9, pp. 1591–1600, Sep. 1994.
[10] A. Hassibi and S. Boyd, "Integer parameter estimation in linear models with applications to GPS," *IEEE Trans. Signal Process.*, vol. 46, no. 11, pp. 2938–2952, Nov. 1998.
[11] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.
[12] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Proc. 17th Annu. Int. Cryptography Conf.*, 1997, pp. 112–131.
[13] R. Fischlin and J. Seifert, "Tensor-based trapdoors for CVP and their application to public key cryptography," in *Proc. 7th IMA Int. Conf.*, 1999, pp. 244–257.
[14] H. Vikalo, "Sphere decoding algorithms for digital communications," Ph.D. dissertation, Stanford Univ., Stanford, CA, 2003.
[15] C. P. Schnorr and M. Euchner, "Lattice basis reduction: improved practical algorithms and solving subset sum problems," *Math. Programming*, vol. 66, pp. 181–191, 1994.
[16] H. Vikalo, B. Hassibi, and U. Mitra, "Sphere-constrained ML detection for channels with memory," in *Proc. 37th Asilomar Conf. Signals, Syst., Comput.*, 2003, pp. 672–676.
[17] H. Vikalo and B. Hassibi, "On joint ML detection and decoding," in *Proc. IEEE Int. Symp. Inf. Theory*, 2003, p. 275.
[18] J. Wang, "Average-case computational complexity theory," *Complexity Theory Retrospective II*, pp. 295–328, 1997.
[19] A. Edelman, "Eigenvalues and condition numbers of random matrices," Ph.D. dissertation, Dept. of Math., Mass. Inst. Technol., Cambridge, MA, 1989.

Haris Vikalo was born in Tuzla, Bosnia and Herzegovina. He received the B.S. degree from the University of Zagreb, Zagreb, Croatia, in 1995, the M.S. degree from Lehigh University, Bethlehem, PA, in 1997, and the Ph.D. degree from Stanford University, Stanford, CA, in 2003, all in electrical engineering.

He held a short-term appointment at Bell Laboratories, Murray Hill, NJ, in the summer of 1999. From January 2003 to July 2003, he was a Postdoctoral Researcher, and since July 2003, he has been an Associate Scientist at the California Institute of Technology, Pasadena. His research interests include wireless communications, signal processing, estimation. and genomic signal and information processing.

Babak Hassibi was born in Tehran, Iran, in 1967. He received the B.S. degree from the University of Tehran in 1989 and the M.S. and Ph.D. degrees from Stanford University, Stanford, CA, in 1993 and 1996, respectively, all in electrical engineering.

From October 1996 to October 1998, he was a Research Associate with the Information Systems Laboratory, Stanford University, and from November 1998 to December 2000, he was a Member of the Technical Staff in the Mathematical Sciences Research Center, Bell Laboratories, Murray Hill, NJ. Since January 2001, he has been with the Department of Electrical Engineering, California Institute of Technology, Pasadena, where he is currently an Associate Professor. He has also held short-term appointments at Ricoh California Research Center, Menlo Park, CA, the Indian Institute of Science, Bangalore, India, and Linköping University, Linköping, Sweden. His research interests include wireless communications, robust estimation and control, adaptive signal processing, and linear algebra. He is the coauthor of the books *Indefinite Quadratic Estimation and Control: A Unified Approach to H^2 and H^∞ Theories* (Philadelphia, PA: SIAM, 1999) and *Linear Estimation* (Englewood Cliffs, NJ: Prentice Hall, 2000).

Dr. Hassibi is a recipient of an Alborz Foundation Fellowship, the 1999 O. Hugo Schuck Best Paper Award of the American Automatic Control Council, the 2002 National Science Foundation Career Award, the 2002 Okawa Foundation Research Grant for Information and Telecommunications, the 2003 David and Lucille Packard Fellowship for Science and Engineering, and the 2003 Presidential Early Career Award for Scientists and Engineers (PECASE). He has been a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY special issue on space-time transmission, reception, coding, and signal processing and is currently an Associate Editor for Communications of the IEEE TRANSACTIONS ON INFORMATION THEORY.