Sphere decoding complexity exponent for full rate codes over the quasi-static MIMO channel

Joakim Jaldén and Petros Elia

Abstract—In the setting of quasi-static multiple-input multiple-output (MIMO) channels, we consider the high signal-to-noise (SNR) asymptotic complexity required by the sphere decoding (SD) algorithm for decoding a large class of full rate linear space-time codes. With SD complexity being a function of the code and having random fluctuations with varying channel, noise and codewords, the introduced *SD complexity exponent* manages to concisely describe the computational reserves required by the SD algorithm to achieve arbitrarily close to optimal performance in decoding the such codes. It is worth noting that, to date, this asymptotically describes the minimum known complexity required for a decoder and time-out policy to provably allow a gap to maximum likelihood performance that vanishes for increasing SNR. Bounds and exact expressions for the SD complexity exponent are then obtained for a large set of existing code designs of varying performance characteristics. For all currently known unified explicit code designs that are uniformly optimal with respect to the diversity multiplexing tradeoff (DMT), the SD complexity exponent is shown to take a particularly concise form as a function of the multiplexing gain.

Index Terms—Diversity-Multiplexing Tradeoff, Sphere Decoding, Complexity, Space-Time Block-Codes, Large Deviations.

I. INTRODUCTION

The past decade has seen the abundant use of the sphere decoding (SD) algorithm as a tool for facilitating maximum likelihood (ML) decoding over the coherent delay-limited (or quasi-static) multiple-input multiple-output (MIMO) channel. The SD algorithm allows for efficient optimal or near optimal detection of a large number of high rate space-time codes that map constituent constellation symbols linearly in space and time [1]–[4]. With the algorithm's computational cost naturally fluctuating as a function of the channel, it is generally known that in implementing a SD, one can tradeoff computational complexity for error performance by selectively choosing when to decode and when not to. Equivalently, in the presence of constraints on the computational reserves, the algorithm is faced with the prospect of encountering channel realizations that force it to violate these run-time constraints, thus having to declare decoding outages, and inevitably introducing a performance gap away from the optimal ML performance.

This naturally raises the intriguing open question of how to optimally traverse the reliability-complexity limits of sphere decoding.

While this question is hard to answer in general, or even ask in a rigorously meaningful way, we show herein that by following [5] and considering the decoding of families of codes in the high signal-to-noise ratio (SNR) limit, not only can the question be made rigorous: It also admits surprisingly simple explicit answers for several settings. Drawing from the DMT setting which has already been successfully applied to concisely describe the high SNR diversity exponent in reliability analysis [6]–[8] of decoders, we here introduce the notion of an *SD complexity exponent* as a measure of complexity of the SD algorithm when applied to the problem of decoding different codes. To this end we characterize the decoding complexity in the high SNR limit under the assumption that the code-rate scales with SNR in order to provide a given multiplexing gain. This approach naturally takes into account the dependency of the SD complexity on the codeword density and the codebook size, as well as the SNR and the fading characteristics of the wireless channel. Similar to previous work on the DMT relating the code rate and probability of decoding error, it is seen that also the complexity, although hard to characterize at any finite SNR, has mathematically tractable characterizations in the high SNR asymptote. These characterizations in turn yield valuable insights into the behavior of the algorithm. Very importantly, this exponent accepts a special role because, to date, it represents the minimum known complexity reserves required to maintain an arbitrarily small SNR gap to the ML decoder.

The SD algorithm is usually described as a branch-and-bound type search [4] over a regular tree and in line with most other works on SD complexity (cf. [2], [4], [9]–[11]) we equivocate the complexity with the number of nodes N visited in the traversal of the search tree. In the context of the DMT it is useful to note that in order to achieve a multiplexing gain of r the code must in the high SNR limit have rate of[1] $R = r \log \rho + o(\log \rho)$ bits per channel use where ρ denotes the SNR. Consequently, the cardinality of the codebook is $|\mathcal{X}| \doteq \rho^{rT}$ where T is the codeword length and where $\doteq$ denotes equality in the SNR exponent (cf. [5] and Section I-B). It is rather straightforward to show that in the worst case the sphere decoder is in essence forced to perform a complete search over the entire codebook, and its complexity is in this case (up to the high SNR exponent) equal to ρ^{rT}. However,

---

[1]Herein, log denotes the base-2 logarithm and $o(\cdot)$ is the standard Landau notation where $f(\rho) = o(\phi(\rho))$ implies $\lim_{\rho \to \infty} f(\rho)/\phi(\rho) = 0$. Similarly, $f(\rho) = O(\phi(\rho))$ implies that $\limsup_{\rho \to \infty} |f(\rho)|/\phi(\rho) < \infty$ for $\phi(\rho) > 0$.

although feasible, this event is also highly improbable. Thus, in order to quantify the probability of the event that the sphere decoder visits an (atypically) large number of nodes, we introduce a (complexity) rate-function $\Psi(x)$ over $0 \leq x \leq rT$ given implicitly by $P(N \geq \rho^x) \doteq \rho^{-\Psi(x)}$ where N is the complexity of the SD algorithm. In short, $\Psi(x)$ captures the decay-rate of the probability that the complexity exceeds a given SNR dependent threshold ρ^x. This decay-rate should be contrasted with the minimum probability of decoding error, which vanishes in the high SNR limit as $\rho^{-d(r)}$ where $d(r)$ is the diversity gain of the code under maximum likelihood (ML) decoding. We can thus judiciously argue that for any x such that $\Psi(x) > d(r)$, the probability that the complexity exceeds ρ^x is at high SNR insignificant in comparison to the overall probability of error of the decoder. In other words: Imposing a run-time limit of ρ^x on the complexity of the algorithm, and declaring a decoding outage or an error whenever this limit is not met, would cause a vanishing degradation in terms of the overall error probability at high SNR. This motivates us to introduce a quantity $c(r)$ defined as the infimum of all x for which $\Psi(x) > d(r)$, and refer to this quantity as the *complexity exponent*. Loosely speaking, $\rho^{c(r)}$ is the tightest runtime-constraint that can be imposed upon the algorithm without sacrificing performance. It also represents the minimum computational reserves required for achieving DMT optimal performance using the SD algorithm. Precise definitions of the above asymptotic measures, and a rigorous treatment of the notion of a vanishing probability of error is given in Section III-D, and by Theorem 1. The main topic of this work will then be to give closed form expressions, and bounds, for the complexity exponent of a class of full rate linear codes, to be described later, including the space-time codes proposed in [12]–[17].

Most other works on sphere decoding complexity consider uncoded (spatially multiplexed) systems and asymptotic results in terms of the signal space dimension, cf. [9], [10], [18], [19]. Our work is instead more related to the analysis in [11], which considers the complexity tail distribution for a fixed signal space dimension. However, unlike [11] we also incorporate the space-time codes into the analysis, as well as the SNR scalings of these codes mandated by the DMT characteristics.

In parallel with our work the work in [20] provides an analysis of the complexity tail distribution for unconstrained lattice sequential decoders, in the presence of DMT optimal random lattice codes. A fundamental difference with our work and [20] is that [20] considers unconstrained lattice decoding, whereas we explicitly take into account the constellation boundary in the decoder. Another difference is that the lattice codes considered in our work can be explicitly constructed and can have arbitrary DMT performance, unlike the random codes in [20] which are non-explicit and which are restricted to being DMT optimal. We also take our analysis one step further by coupling the complexity tail distribution to the DMT performance of the code in order to obtain the complexity exponent. Regarding the ultimate complexity limits on DMT optimal decoding, we have previously established that lattice reduction (LR)-aided linear decoders are sufficient for achieving the entire DMT tradeoff at a worst case complexity of $O(\log(\rho))$,

i.e., corresponding to a complexity exponent of $c(r) = 0$ [8]. This is lower than the SD complexity exponent that we will present in what follows. However, as the sphere decoder has become somewhat of the de-facto decoder for linear dispersive space-time codes, the analysis of its complexity is interesting in its own right. It should also be noted that the statements made herein are stronger in terms of error probability as they not only imply full diversity but also a vanishing SNR gap to the ML decoder (cf. Theorem 1 for details). Such a results was not established for the decoders in [8], [20].

A. Outline and contributions

The general definition of the complexity exponent is given in Definition 1. Theorem 1 describes how sphere decoding and the time-out policies to be employed, can guarantee a gap to ML that vanishes for increasing SNR. Theorem 2 then gives a general expression for an upper bound $\bar{c}(r)$ on the SD complexity exponent $c(r)$ of any full rate code with multiplexing gain r and diversity $d(r)$. An explicit closed form expression for $\bar{c}(r)$ is then given in Theorem 3 for all DMT optimal full rate codes. The bound $\bar{c}(r)$ is already useful in itself in that it establishes that the SD complexity exponent is much lower than the worst case SNR exponent rT associated with a full search of the codebook. However, in the interest of also establishing the tightness of this bound, Lemma 2 provides easy-to-check sufficient conditions on the generator matrix of the code lattice, that guarantee the tightness of $\bar{c}(r)$. Building on this, Theorem 4 establishes that, given any full rate design of arbitrary DMT performance, there is always at least one non-random SD detection ordering for which $c(r) = \bar{c}(r)$, i.e., for which the exact $c(r)$ can be explicitly calculated from the result of Theorem 2. Theorem 5 goes one step further and establishes the exact SD complexity exponent, given any *threaded* code design and the natural detection ordering, to be $c(r) = \bar{c}(r)$ while Theorem 6 provides an explicit expression for $c(r)$ for any DMT optimal threaded code design. Surprisingly this simple expression (see Fig. 1) serves as an upper bound on $c(r)$ for any full-rate code, irrespective of the fading statistics. Finally, and going on a different path, Theorem 7 establishes $c(r)$ for any 2×2 code that achieves DMT optimality for all fading statistics, irrespective of the specific structure of such code thus enabling this same $c(r)$ to hold for even possibly undiscovered code designs. Some general discussions of these results are then provided in Section V.

Note here that the class of threaded codes, for which $c(r)$ is fully established in Theorem 5, includes all code designs that are currently known to achieve the optimal DMT over all $r \leq n_T$. The SD complexity exponent for the class of full rate DMT-optimal threaded codes with minimum delay, i.e., for which $n_T = T = n$ where n_T denotes the number of transmit antennas, is shown[2] in Fig. 1 for $n = 2, \ldots, 6$. The results shown in the figure apply to codes such as those presented in [12]–[17]. Before proving the aforementioned results, it is worth commenting on the somewhat counterintuitive

---

[2] A closed form expression for the complexity exponent $c(r)$ shown in the Fig. 1 is given by (50) in Theorem 6.
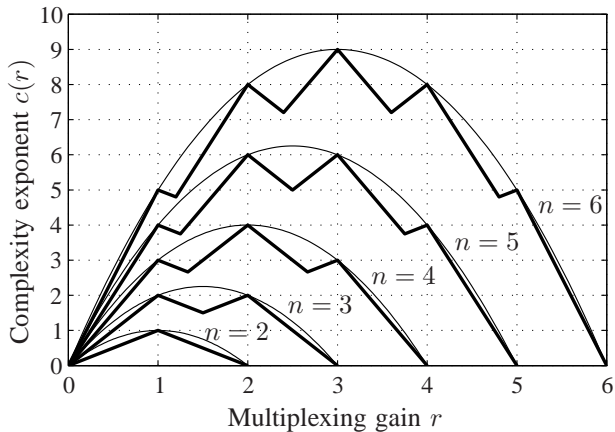
Fig. 1. The SD complexity exponent $c(r)$ corresponding to threaded minimum delay DMT optimal codes with $n_T = T = n$ for $n = 2, \dots, 6$. The complexity exponent is illustrated by the bold lines. The thin lines show the quadratic function given by $r(n-r)$ which provides the exact complexity exponent at integer multiplexing gains. The same exponent also serves as an upper bound to the SD complexity exponent for any minimum delay DMT optimal full rate linear dispersive code.

result suggested by the SD complexity exponent in Fig. 1. Namely, that while $c(r)$ initially increases as a function of the multiplexing gain r, it then decreases as r approaches its maximal value n_T. The initial increase can easily be explained by the fact that the cardinality (density) of the codebook $\mathcal{X}$ increases as a function of r. However, the decrease at high multiplexing gains can be understood in light of the coupling of the complexity and the overall probability of error: in short, at high multiplexing gains the error probability is also higher and this implies that the decoder may time out for a larger set of problem instances without affecting the overall performance, leading to an overall reduction in decoding complexity. Pushing the code-decoder pair towards the maximal data rate does therefore not imply that the decoding complexity is maximized. This effect is discussed further in Section V-A.

B. Notation

We let $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, denote the set of integer, real and complex numbers respectively and $\mathbb{F}^n$ and $\mathbb{F}^{m \times n}$ the set of n-vectors and $m \times n$-matrices over $\mathbb{F} \in \{\mathbb{Z}, \mathbb{R}, \mathbb{C}\}$. Vectors are denoted by lower-case bold letters $\boldsymbol{a}$, matrices are denoted by upper-case bold letters $\boldsymbol{A}$. We use $(\cdot)^T$ and $(\cdot)^H$ to denote the transpose and Hermitian (conjugate) transpose of vectors and matrices, and $\text{vec}(\cdot) : \mathbb{C}^{m \times n} \mapsto \mathbb{C}^{mn}$ the matrix to vector operation whereby the columns of the argument are stacked on top of each other. We use $\boldsymbol{I}_n \in \mathbb{C}^n$ to denote the $n \times n$ identity matrix, and use $\boldsymbol{0}$ to denote the zero vector or matrix where the dimensions are given by the context in which $\boldsymbol{0}$ is used. Deviating slightly from standard usage, we refer to a tall matrix $\boldsymbol{U} \in \mathbb{C}^{m \times n}$ where $m \geq n$ as unitary if $\boldsymbol{U}^H \boldsymbol{U} = \boldsymbol{I}$. For $a \in \mathbb{C}$ we use $\Re(a), \Im(a)$ to respectively denote the real and imaginary parts of a. For $a \in \mathbb{R}$ we use $\lfloor a \rfloor$ to denote the floor operation defined as the largest integer smaller than or equal to a, $\lceil a \rceil$ to denote the ceil operation defined as the smallest integer larger than or equal to a, and we let $(a)^+ \triangleq \max(a, 0)$.

We let $\sigma_1(\boldsymbol{A}) \leq \dots \leq \sigma_n(\boldsymbol{A})$ denote the ordered (structurally) non-zero singular values [21] of a matrix $\boldsymbol{A} \in \mathbb{C}^{m \times n}$ where $m \geq n$. We will on occasion use $\sigma_{\max}(\boldsymbol{A})$ to denote the largest singular value when the dimension of $\boldsymbol{A}$ is not explicit. We will also use $\lambda_i(\boldsymbol{A}) \leq \dots \leq \lambda_n(\boldsymbol{A})$ to denote the ordered (real) eigenvalues of a Hermitian matrix $\boldsymbol{A} = \boldsymbol{A}^H \in \mathbb{C}^{n \times n}$ and note that $\sigma_i^2(\boldsymbol{A}) = \lambda_i(\boldsymbol{A}^H \boldsymbol{A})$ for any $\boldsymbol{A} \in \mathbb{C}^{m \times n}$ where $m \geq n$. We make no notational difference between random variables and their realizations. We will use the notation $\Omega \triangleq \{\cdots\}$ to label the stochastic event within the brackets.

Finally, in order to simplify notation we will make use of the $\dot{=}$ (and $\dot{\leq}, \dot{\geq}, \dot{<}, \dot{>}$) notation for equalities (and inequalities) in the SNR exponent, cf. [5]. Specifically, we write $f(\rho) \dot{\leq} \rho^a$ and $g(\rho) \dot{\geq} \rho^b$ to denote

$$\limsup_{\rho \to \infty} \frac{\log f(\rho)}{\log \rho} \leq a \quad \text{and} \quad \liminf_{\rho \to \infty} \frac{\log g(\rho)}{\log \rho} \geq b$$

and $f(\rho) \dot{=} \rho^x$ when $f(\rho) \dot{\leq} \rho^x$ and $f(\rho) \dot{\geq} \rho^x$. The definition of $\dot{<}$ and $\dot{>}$ follows after replacing $\leq$ by $<$ and $\geq$ by $>$.

II. CHANNEL MODEL AND SPACE-TIME CODES

We consider the standard block Rayleigh fading $n_T \times n_R$ quasi-static point-to-point MIMO channel model with coherence-time T given by

$$\boldsymbol{Y} = \boldsymbol{H}\boldsymbol{X} + \boldsymbol{W} \tag{1}$$

where $\boldsymbol{X} \in \mathbb{C}^{n_T \times T}$, $\boldsymbol{Y} \in \mathbb{C}^{n_R \times T}$ and $\boldsymbol{W} \in \mathbb{C}^{n_R \times T}$ denote the transmitted space-time block codeword, the block of received signals, and additive spatially and temporally white Gaussian noise. The channel gains $\boldsymbol{H} \in \mathbb{C}^{n_R \times n_T}$ are assumed to be i.i.d. circularly symmetric complex Gaussian (i.e., Rayleigh fading) and constant over the duration of the transmission. We shall assume throughout that $n_R \geq n_T$. The transmitted codewords $\boldsymbol{X}$ are assumed to be drawn uniformly from a codebook $\mathcal{X}$ and we assume that

$$\mathrm{E}\{\|\boldsymbol{X}\|_F^2\} = \frac{1}{|\mathcal{X}|} \sum_{\boldsymbol{X} \in \mathcal{X}} \|\boldsymbol{X}\|_F^2 = \rho T, \tag{2}$$

so that the parameter ρ takes on the interpretation of an average SNR. Note also here that one use of (1) is viewed as T uses of the wireless channel in the definition of the data-rate.

We shall herein restrict our attention to full rate (complex) linear dispersion codes [22], [23] of the form

$$\boldsymbol{X} = \theta \sum_{i=1}^{\kappa} s_i \boldsymbol{D}_i \tag{3}$$

where $s_i \in \mathbb{S} \subset \mathbb{C}$ are information symbols drawn from a finite alphabet $\mathbb{S}$, $\{\boldsymbol{D}_i\}_{i=1}^{\kappa}$ is a set of linearly independent *dispersion matrices*, and θ is a parameter regulating the transmit power. The notion of full rate implies that each codeword $\boldsymbol{X} \in \mathbb{C}^{n_T \times T}$ can be viewed as carrying $\kappa = n_T T$ constellation symbols. We will further make the additional restriction that $\mathbb{S}$ belongs in the class of QAM-like alphabets of the form

$$\mathbb{S} = \mathbb{S}_\eta \triangleq \{s \,|\, \Re(s), \Im(s) \in \mathbb{Z} \cap [-\eta, \eta]\} \tag{4}$$

where $\eta > 0$ is a parameter regulating the size of the constellation[3]. We will use $\mathbb{S}_\infty$ to denote the extended (infinite) constellation obtained by letting $\eta = \infty$ in (4), and note that $\mathbb{S}_\infty$ is nothing but the set of Gaussian integers. QAM constellations will in general also include a translation and scaling of the underlying lattice $\mathbb{S}_\infty$. However, as including such a translation would not affect the results obtained herein, and as the scaling can easily be included in the dispersion matrices $\boldsymbol{D}_i$ or θ, we omit these variations and concentrate on (4) in the interest of notational simplicity.

The channel model in (1) may also be equivalently expressed in a vectorized form according to (cf. [24])

$$ \boldsymbol{y} = (\boldsymbol{I}_T \otimes \boldsymbol{H})\boldsymbol{x} + \boldsymbol{w} \tag{5} $$

where $\boldsymbol{y} = \mathrm{vec}(\boldsymbol{Y})$, $\boldsymbol{x} = \mathrm{vec}(\boldsymbol{X})$, and $\boldsymbol{w} = \mathrm{vec}(\boldsymbol{W})$, and where $\otimes$ denotes the Kronecker product [25]. We shall mainly work with (5) rather than (1) directly. In the vectorized form the codewords $\boldsymbol{x}$ are given by

$$ \boldsymbol{x} = \theta \boldsymbol{G} \boldsymbol{s} $$

for $\boldsymbol{s} \in \mathbb{S}_\eta^\kappa$, and where the full rank matrix

$$ \boldsymbol{G} = \begin{bmatrix} \mathrm{vec}(\boldsymbol{D}_1) & \cdots & \mathrm{vec}(\boldsymbol{D}_\kappa) \end{bmatrix} \tag{6} $$

is referred to as the *generator matrix* of the code. The linear dispersive codes form a subset of the lattice codes [23] as the codewords constitute a subset of the (complex) lattice $\theta \boldsymbol{G} \mathbb{S}_\infty$.

The parameters θ and η are, as noted, chosen in order to satisfy given transmit power and rate constraints. In particular, in order to ensure a multiplexing gain of

$$ r \triangleq \lim_{\rho \to \infty} \frac{1}{T} \frac{\log |\mathcal{X}|}{\log \rho}, \tag{7} $$

or equivalently a rate of $R = r \log \rho + o(\log \rho)$, it must hold that $\eta \doteq \rho^{\frac{rT}{2\kappa}}$ which by (2) and (4) implies that $\theta^2 \doteq \rho^{1 - \frac{rT}{\kappa}}$. The code structure described above includes the codes proposed in [12]–[15], [17], as well as the QAM-based codes of [16], as special cases. Finally, we will hereafter with slight abuse of terminology but still in line with [12]–[17] also use the term *full rate linear dispersive code* when referring to the whole *family* of codes that is generated by a single generator matrix $\boldsymbol{G}$ for different multiplexing gains and SNRs, and trust that no confusion should follow by this usage.

III. DECODING

The coherent ML decoder for (1) is well known to be

$$ \hat{\boldsymbol{X}}_{\mathrm{ML}} = \arg \min_{\hat{\boldsymbol{X}} \in \mathcal{X}} \| \boldsymbol{Y} - \boldsymbol{H} \hat{\boldsymbol{X}} \|_{\mathrm{F}}^2. \tag{8} $$

The resulting diversity gain of the code, under ML decoding, is correspondingly given by (cf. [5])

$$ d(r) \triangleq - \lim_{\rho \to \infty} \frac{\log \mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}{\log \rho}, \tag{9} $$

[3]The assumption of a square constellation is made here for simplicity of exposition and in line with practical encoding schemes. This assumption though can readily be relaxed without affecting the presented results, as long as the constellation is the same for all s_i, $i = 1, \cdots, \kappa$. A detailed exposition of the mathematical machinery that allows for this relaxation can be found in [8, Section III]

where the notation $d(r)$ accentuates the dependence of the diversity on the multiplexing gain r.

One of the main features of the linear dispersive codes, as was noted in the introduction, is that their lattice structure allows for efficient – optimal and near optimal – solutions to (8) using the sphere decoding algorithm, cf. [24]. Using the linearity of the map from $\boldsymbol{s}$ to $\boldsymbol{x} = \mathrm{vec}(\boldsymbol{X})$ we obtain (cf. (5))

$$ \boldsymbol{y} = \boldsymbol{M} \boldsymbol{s} + \boldsymbol{w} \tag{10} $$

where the code channel generator matrix $\boldsymbol{M}$ is given by

$$ \boldsymbol{M} \triangleq \theta(\boldsymbol{I}_T \otimes \boldsymbol{H})\boldsymbol{G} \in \mathbb{C}^{n_\mathrm{R} T \times \kappa}. \tag{11} $$

We can thus instead of solving (8) directly equivalently obtain an estimate of $\boldsymbol{s}$ through

$$ \hat{\boldsymbol{s}}_{\mathrm{ML}} = \arg \min_{\hat{\boldsymbol{s}} \in \mathbb{S}_\eta^\kappa} \| \boldsymbol{y} - \boldsymbol{M} \hat{\boldsymbol{s}} \|^2, \tag{12} $$

where (12) is an optimization problem suitable for the sphere decoder, and then easily recover $\hat{\boldsymbol{X}}_{\mathrm{ML}}$ from $\hat{\boldsymbol{s}}_{\mathrm{ML}}$.

A. The Sphere Decoder

The sphere decoding algorithm solves (12) by a branch-and-bound like traversal of a regular tree. Detailed descriptions of the algorithm are found in [1] and the semi-tutorial papers [2]–[4], and most implementation issues will not be repeated herein. However, in order to make our results precise and to introduce notation we need to review some or the key ideas as they apply to (12).

To this end, note that by the rotational invariance of the Euclidean norm it follows that (12) is equivalent to

$$ \hat{\boldsymbol{s}}_{\mathrm{ML}} = \arg \min_{\hat{\boldsymbol{s}} \in \mathbb{S}_\eta^\kappa} \| \boldsymbol{r} - \boldsymbol{R} \hat{\boldsymbol{s}} \|^2 \tag{13} $$

where $\boldsymbol{Q} \boldsymbol{R} = \boldsymbol{M}$ is the thin QR-decomposition of $\boldsymbol{M}$ (i.e. $\boldsymbol{Q} \in \mathbb{C}^{n_\mathrm{R} T \times \kappa}$ is unitary and $\boldsymbol{R} \in \mathbb{C}^{\kappa \times \kappa}$ is upper triangular) and where $\boldsymbol{r} = \boldsymbol{Q}^\mathrm{H} \boldsymbol{y}$. The sphere decoder solves (13) by enumerating symbol vectors $\hat{\boldsymbol{s}} \in \mathbb{S}_\eta^\kappa$ within a given sphere of radius $\xi > 0$, i.e., $\hat{\boldsymbol{s}}$ that satisfy

$$ \| \boldsymbol{r} - \boldsymbol{R} \hat{\boldsymbol{s}} \|^2 \leq \xi^2. \tag{14} $$

If (14) is satisfied for at least one $\hat{\boldsymbol{s}} \in \mathbb{S}_\eta^\kappa$, then also the ML solution must satisfy (14) as the ML solution yields the minimum metric in (12). The set of vectors that satisfy (14) is found by recursively considering partial symbol vectors $\hat{\boldsymbol{s}}_k \in \mathbb{S}_\eta^k$ for $k = 1, \ldots, \kappa$. Specifically, if $\hat{\boldsymbol{s}}_k$ is the vector containing the last k components of $\hat{\boldsymbol{s}}$, a necessary condition for (14) to be satisfied is given by

$$ \| \boldsymbol{r}_k - \boldsymbol{R}_k \hat{\boldsymbol{s}}_k \|^2 \leq \xi^2, \tag{15} $$

where $\boldsymbol{r}_k \in \mathbb{C}^k$ denotes the last k components of $\boldsymbol{r}$, and where $\boldsymbol{R}_k \in \mathbb{C}^{k \times k}$ denotes the $k \times k$ lower right corner of $\boldsymbol{R}$. Thus, any set of vectors $\boldsymbol{s} \in \mathbb{S}_\eta^\kappa$ with common last k components that fail to satisfy (15) may be excluded from the set of ML candidate vectors. Enumerating all partial symbol vectors that satisfy (15), beginning with $k = 1$, extending these to $k = 2$ and so on, yields a recursive procedure for enumerating all $\boldsymbol{s} \in \mathbb{S}_\eta^\kappa$ that satisfy (14).

The enumeration of partial symbol vectors s_k is equivalent to the traversal of a regular tree with κ layers – one per symbol s_k where s_k is the kth component of s – and $|\mathbb{S}_\eta|$ children per node [4]. There is a one to one correspondence between the nodes at layer k (the layers are enumerated with the root node corresponding to $k = 0$) and the partial vectors s_k. We say that a node is visited by the sphere decoder if and only if the corresponding partial vector s_k satisfies (15), i.e., there is a bijection between the visited nodes at layer k and the set

$$\mathcal{N}_k \triangleq \{ \, \hat{s}_k \in \mathbb{S}_\eta^k \mid \|r_k - R_k \hat{s}_k\|^2 \leq \xi^2 \, \} . \tag{16}$$

Due to this relation we will in what follows not make the distinction between nodes and partial symbol vectors and simply refer to s_k as nodes at layer k when discussing the search. The total number of visited nodes (in all layers of the tree) is given by

$$N = \sum_{k=1}^{\kappa} N_k . \tag{17}$$

where $N_k \triangleq |\mathcal{N}_k|$ is the number of visited nodes at layer k of the search tree. The total number of visited nodes is commonly taken as a measure of the sphere decoder complexity [9], [11] and this will also be done in what follows. Note however that as the total number of floating point operations (flops) required for evaluating the bound in (15) may be upper and lower bounded by constants that are independent of ρ our results relating to the SD complexity exponent would not change if we instead considered N to be the number of flops spent by the decoder.

B. The search radius

The description of the sphere decoder is not complete without specifying how the search radius is selected. In the interest of obtaining the complexity exponent, we may argue that any reasonable choice of a fixed (non-random) search radius should satisfy

$$\xi \doteq \rho^0 . \tag{18}$$

To see this, it is sufficient to note that the metric in (13) satisfies

$$\|r - Rs\|^2 = \|Q^H w\|^2$$

for the transmitted vector s. Thus, if $\|Q^H w\|^2 > \xi^2$ the transmitted symbol vector is excluded from the search, resulting in a decoding error. By considering a radius that grows slowly with SNR, say $\xi^2 = z \log \rho \doteq \rho^0$, it can be shown that

$$P(\|Q^H w\|^2 \geq \xi^2) \dot{<} \rho^{-d} , \tag{19}$$

provided $z > 0$ is sufficiently large, i.e., the probability of excluding the transmitted vector will vanish faster than the probability of error and cause vanishing degradation to the overall probability of error. At the same time, if the radius does not tend to infinity with increasing ρ, it will follow that $P(\|Q^H w\|^2 > \xi^2)$ is bounded away from zero. This implies a non-vanishing probability of error and a resulting diversity gain of zero, which is clearly undesirable. Thus, as the complexity exponent is not affected by the particular choice of z, we shall unless otherwise stated in the following

for simplicity assume that ξ is non-random and that (18) holds, with z chosen in order to ensure vanishing degradation to the overall probability of error. This said, the SD complexity exponent would be the same if we considered adaptive radius updates as used in the Schnorr-Euchner (SE) implementation [2], [3]. This may be shown by following the argument in [10], and we sketch a proof of this statement in the present setting in Appendix B-D.

C. Decoding Complexity

The sphere decoder complexity, or equivalently the number of visited nodes N, is as stated a random variable with a distribution that depends on a number of parameters, e.g., the system dimensions n_R, n_T and T, the SNR ρ, the multiplexing gain r, the generator matrix G, and the search radius ξ. This is well known and follows by the randomness of the bound in (15). Naturally this randomness must be considered in properly analyzing the sphere decoder complexity.

In order to illustrate one of the problems with studying the worst case complexity consider the event that $H = 0$ and $\|w\|^2 < \xi^2$, where it is easily seen that (14) and (15) are always satisfied. As a consequence, the complexity of the sphere decoder would be equal to

$$N = \sum_{k=1}^{\kappa} |\mathbb{S}_\eta|^k \doteq \sum_{k=1}^{\kappa} \rho^{\frac{rT}{\kappa}} \doteq \rho^{rT} ,$$

where we have used that $\eta \doteq \rho^{\frac{rT}{2\kappa}}$ to obtain the size of $\mathbb{S}_\eta$ in (4). The worst case complexity would thus end up being comparable to that of a full search over $\mathcal{X}$ as $|\mathcal{X}| \doteq \rho^{rT}$. However, there is also no point in decoding when $H = 0$ as all codewords would yield the same ML metric which in turn implies a high probability of error. Essentially the same argument, for opting out of decoding, can be made whenever the MIMO channel is in information theoretic outage [5]. In this case it follows by Fano's inequality that the probability of detection error will be bounded away from zero. In fact, for a code with a diversity gain of $d(r)$ any set of channel matrices $\mathcal{H}$ for which $P(H \in \mathcal{H}) \dot{<} \rho^{-d(r)}$, may be neglected by the decoder with vanishing degradation of the overall probability of error. However, rather than identifying and excluding a set of bad channel matrices directly, a more pragmatic approach is to impose a run-time constraint on the decoder and ensure that this constraint is such that the probability of it being violated is insignificant in relation to the probability of error. This leads to the following measure of the decoding complexity, which we will use throughout.

Definition 1: Let

$$\Psi(x) \triangleq - \lim_{\rho \to \infty} \frac{\log P(N \geq \rho^x)}{\log \rho} \tag{20}$$

where N is the number of nodes visited by the sphere decoder (cf. (17)). The *SD complexity exponent* is then given by

$$c(r) \triangleq \inf\{x \mid \Psi(x) > d(r)\} \tag{21}$$

where $d(r)$ (cf. (9)) is the diversity gain of the code at multiplexing gain r.

D. Vanishing SNR gap to the ML performance

We recall that in addition to the instances where the ML decoder makes an incorrect decision, a time-limited sphere decoder can additionally make decoding errors when the search radius is selected too small, i.e., when $\mathcal{N}_\kappa = \emptyset$ (cf.(16)), or when the run-time limit of ρ^x becomes active, i.e., when $N \geq \rho^x$. These extra errors cause a gap to ML performance which can be quantified as

$$g(x) \triangleq \frac{\mathrm{P}(\{\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X}\} \cup \{\mathcal{N}_\kappa = \emptyset\} \cup \{N \geq \rho^x\})}{\mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}$$

describing the ratio between the probability of error of the time-limited sphere decoder and the ML decoder. With respect to $c(r)$ we then have the following.

Theorem 1: The SD complexity exponent $c(r)$ is the tightest lower bound on the SNR exponents of all run-time constrains ρ^x for which a sphere decoder can allow for a vanishing gap to ML performance, i.e., where

$$\lim_{\rho \to \infty} g(x) = 1, \quad \text{for any } x > c(r). \tag{22}$$

The above simply states that for any $x > c(r)$ it is possible to design a decoder based on the SD algorithm that achieves a vanishing SNR gap to the ML decoder, at a worst case complexity of ρ^x. To see this apply the union bound to get

$$g(x) \leq \underbrace{\frac{\mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}{\mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}}_{=1} + \underbrace{\frac{\mathrm{P}(\xi_{\mathrm{ML}} > \xi)}{\mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}}_{\to 0} + \underbrace{\frac{\mathrm{P}(N \geq \rho^x)}{\mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}}_{\to 0}$$

where the second and third term tend to zero with increasing ρ as the numerator tends to zero at a faster rate than the denominator cf. (19),(21). This immediately translates to a vanishing SNR gap to the ML decoder at high SNR. In short, the probabilities of the events that the search space is empty or that the complexity of the run-time-unconstrained sphere decoder exceeds ρ^x are insignificant in comparison to the probability of ML decoding errors.

Furthermore it is the case that one cannot time-limit the sphere decoder to ρ^x for some $x < c(r)$ and expect an arbitrary small gap to ML performance. Specifically, one can show (cf. (67)) that $\mathrm{P}(N \geq \rho^x) \dot{>} \rho^{-d(r)}$ for any $x < c(r)$, and as a result, for all codes where we are able to determine $c(r)$ exactly, it follows that for $x < c(r)$ then

$$g(x) \geq \underbrace{\frac{\mathrm{P}(N \geq \rho^x)}{\mathrm{P}(\hat{\boldsymbol{X}}_{\mathrm{ML}} \neq \boldsymbol{X})}}_{\to \infty}$$

implying that any attempt to significantly reduce the complexity beyond $\rho^{c(r)}$ will be at the expense of the vanishing SNR gap to ML decoding.

IV. THE SPHERE DECODER COMPLEXITY EXPONENT

We proceed to establish upper and lower bounds on the SD complexity exponent, in essence through the application of a principle (dating back to Gauss) which states that the number of integer lattice points within a (large) set is well approximated by the volume of the set [26], [27]. Thus, in order to approximate the number of nodes at layer k of the search tree, i.e., the size of $\mathcal{N}_k$ defined in (16), we are primarily concerned with the volume of $([-\eta, \eta] + \sqrt{-1}[-\eta, \eta])^k \cap \mathcal{E}_k$ where $\mathcal{E}_k$ is the elliptical set given by (cf. (16))

$$\mathcal{E}_k = \{\tilde{\boldsymbol{s}}_k \in \mathbb{C}^k \mid \|\boldsymbol{r}_k - \boldsymbol{R}_k \tilde{\boldsymbol{s}}_k\|^2 \leq \xi^2\}. \tag{23}$$

The use of the volume principle for assessing the sphere decoder complexity was previously used in [2], [11], [28] although its prior use in the communications literature is limited to the case of lattice decoding (i.e., where the constellation boundary constraint imposed by $[-\eta, \eta]$ is ignored by the decoder). Herein, we have to take the constellation boundary into account to obtain tight bounds on the SD complexity exponent.

The upper and lower bounds presented in this section are essentially obtained in three main steps: 1) The volume principle is used to obtain an expression for the number N_k of visited nodes at layer k in terms of the singular values of $\boldsymbol{R}_k$; 2) the singular values of $\boldsymbol{R}_k$ for $k = 1, \ldots, \kappa$ are related to the singular values of the channel matrix $\boldsymbol{H}$; and 3) the theory of large deviations is used similarly to [5] to identify random events likely to cause an atypically large decoding complexity. Establishing the upper bound on $c(r)$ turns out to be easier mathematically. The reason for this is primarily in the second step where the interlacing property of singular values of sub-matrices [21] can be used to lower bound the singular values of $\boldsymbol{R}_k$ by the singular values of $\boldsymbol{H}$, to yield results that are universally applicable for any full rank generator matrix $\boldsymbol{G}$, cf. Theorem 2. Although the interlacing property gives both upper and lower bounds on the singular values of $\boldsymbol{R}_k$, the upper bounds are unfortunately not sufficient for establishing tight lower bounds on $c(r)$. We are therefore forced to develop tighter bounds that depend on some technical assumptions on $\boldsymbol{G}$, cf. Lemma 2. While these conditions are, at least in principle, easily verified for any given code design, they are generally hard to verify for arbitrary classes of codes. Nevertheless, for some important classes discussed in Section IV-D we are able to conclude that the upper bound on $c(r)$ is tight, thereby establishing $c(r)$ exactly.

The derivation of the upper bound on $c(r)$ is given in the following sub-sections, while the derivation of the lower bound, which is similar in spirit to the upper bound but complicated by some technical details, is primarily given in Appendix B, and discussed in Section IV-D.

A. The volume principle

As noted, we begin by establishing bounds on $N_k = |\mathcal{N}_k|$ in terms of the eigenvalues of the matrix $\boldsymbol{R}_k$ in (15), the sphere radius ξ and the constellation size η. To this end, consider the following lemma, which corresponds to rigorous applications of the volume principle discussed above.

Lemma 1: Let $\mathcal{E} \subset \mathbb{R}^n$ be the ellipsoidal set given by

$$\mathcal{E} \triangleq \{\boldsymbol{d} \in \mathbb{R}^n \mid \|\boldsymbol{c} - \boldsymbol{D}\boldsymbol{d}\|^2 \leq \xi^2\} \tag{24}$$

where $\boldsymbol{D} \in \mathbb{R}^{n \times n}$ and $\boldsymbol{c} \in \mathbb{R}^n$. Let $\mathcal{B} \subset \mathbb{R}^n$ be the hypercube given by

$$\mathcal{B} \triangleq \{\boldsymbol{d} \in \mathbb{R}^n \mid |d_i| \leq \eta, \, i = 1, \ldots, n\}. \tag{25}$$

Then, the number of integer points contained in the intersection of $\mathcal{E}$ and $\mathcal{B}$ is upper bounded as

$$|\mathcal{E} \cap \mathcal{B} \cap \mathbb{Z}^n| \leq \prod_{i=1}^{n} \left[\sqrt{n} + \min\left(\frac{2\xi}{\sigma_i(D)}, 2\sqrt{n}\eta \right) \right], \quad (26)$$

and the number of integer points contained in $\mathcal{E}$ is lower bounded by

$$|\mathcal{E} \cap \mathbb{Z}^n| \geq \prod_{i=1}^{n} \left(\frac{2\xi}{\sqrt{n}\sigma_i(D)} - \sqrt{n} \right)^{+}. \quad (27)$$

where $\sigma_i(D)$, $i = 1, \ldots, n$ denote the singular values of D.

Proof: Given in Appendix A.

Although Lemma 1 is phrased in terms of real valued quantities, it is easily applied to complex valued sets by considering each complex dimension as two real valued dimensions. In particular, the expression in (14) is equivalent to

$$\|\underline{r}_k - \underline{R}_k \underline{s}_k\|^2 \leq \xi^2$$

where

$$\underline{r}_k = \begin{bmatrix} \Re(r_k) \\ \Im(r_k) \end{bmatrix}, \quad \underline{R}_k = \begin{bmatrix} \Re(R_k) & -\Im(R_k) \\ \Im(R_k) & \Re(R_k) \end{bmatrix},$$

and

$$\underline{s}_k = \begin{bmatrix} \Re(s_k) \\ \Im(s_k) \end{bmatrix}.$$

By noting that if $R_k = U\Sigma V^{\mathrm{H}}$ is the singular value decomposition (SVD) [21] of R_k, then

$$\underline{R}_k = \begin{bmatrix} \Re(U) & -\Im(U) \\ \Im(U) & \Re(U) \end{bmatrix} \begin{bmatrix} \Sigma & 0 \\ 0 & \Sigma \end{bmatrix} \begin{bmatrix} \Re(V^{\mathrm{H}}) & -\Im(V^{\mathrm{H}}) \\ \Im(V^{\mathrm{H}}) & \Re(V^{\mathrm{H}}) \end{bmatrix}$$

is the SVD of $\underline{R}_k$, it follows that the singular values of $\underline{R}_k$ are the same as those of R_k albeit with a multiplicity of 2. Thus, applying (26) in Lemma 1 to $\mathcal{N}_k$ (cf. (16)) yields an upper bound on the number of nodes visited at layer k according to

$$N_k = |\mathcal{N}_k| \leq \prod_{i=1}^{k} \left[\sqrt{2k} + \min\left(\frac{2\xi}{\sigma_i(R_k)}, 2\sqrt{2k}\eta \right) \right]^2 \quad (28)$$

where $\sigma_i(R_k)$, $i = 1, \ldots, k$ denote the singular values of R_k. Here, in essence, the additive $\sqrt{2k}$ term accounts for edge effects in the volume approximation, the first term in the minimum accounts for the size of the search sphere, and the second term in the minimum accounts for the finiteness of the constellation.

The lower bound in (27) will be used later in order to assess the tightness of the upper bound on $c(r)$ developed next. The reason for providing a lower bound on $|\mathcal{E} \cap \mathbb{Z}^n|$ and not $|\mathcal{E} \cap \mathcal{B} \cap \mathbb{Z}^n|$ is that we cannot a-priori rule out that c in (24) is such that $\mathcal{E} \cap \mathcal{B} = \emptyset$, a case which if not ruled out would lead to the trivial lower bound $|\mathcal{E} \cap \mathcal{B} \cap \mathbb{Z}^n| \geq 0$.

B. Singular value bounds

The interlacing theorem of singular values of sub-matrices (cf. [21, Th. 7.3.9] and [25, Corollary 3.1.3]) states that the singular values of R_k are bounded by the singular values of R according

$$\sigma_{i+\kappa-k}(R) \geq \sigma_i(R_k) \geq \sigma_i(R), \quad i = 1, \ldots, k, \quad (29)$$

where $\sigma_i(R_k)$ and $\sigma_i(R)$ denotes the ith singular values of R_k and R respectively. As $R = Q^{\mathrm{H}}M$ where Q has a set of orthogonal columns that span the range of M it follows that $\sigma_i(R) = \sigma_i(M)$. Further, by the definition of M in (11) we have that $\sigma_i(M) \geq \theta\gamma\sigma_i(I_T \otimes H)$ where $\gamma \triangleq \sigma_1(G) > 0$ due to the assumption that G is full rank. The singular values of $I_T \otimes H$ are the same as those of the channel matrix H in (1), albeit with a multiplicity of T, i.e.,

$$\sigma_i(I_T \otimes H) = \sigma_{\iota_T(i)}(H), \quad i = 1, \ldots, n_{\mathrm{T}},$$

where

$$\iota_T(i) \triangleq \left\lceil \frac{i}{T} \right\rceil. \quad (30)$$

This can be seen by noting that if $H = U\Sigma V^{\mathrm{H}}$ is the SVD of H, then

$$(I_T \otimes U)(I_T \otimes \Sigma)(I_T \otimes V^{\mathrm{H}})$$

is an SVD of $I_T \otimes H$ (albeit with a non-standard ordering of the singular values). Alternatively, on can apply [25, Theorem 4.2.12] to the eigenvalues of $I_T \otimes H^{\mathrm{H}}H$.

Combining the above yields a lower bound on the singular values of R_k in terms of the singular values of the channel matrix H according to

$$\sigma_i(R_k) \geq \theta\gamma\sigma_{\iota_T(i)}(H), \quad i = 1, \ldots, k,$$

and an upper bound on the number of nodes visited by the sphere decoder at layer k according to

$$N_k \leq \prod_{i=1}^{k} \left[\sqrt{2k} + \min\left(\frac{2\xi}{\theta\gamma\sigma_{\iota_T(i)}(H)}, 2\sqrt{2k}\eta \right) \right]^2. \quad (31)$$

In order to bound the probability that the right hand side of (31) is atypically large in the high SNR regime it is useful to introduce the SNR dependent parameterization of the singular values (or eigenvalues) of $H^{\mathrm{H}}H$ introduced in [5], i.e., SNR dependent random variables α_i, for $i = 1, \ldots, n_{\mathrm{T}}$, defined by

$$\alpha_i \triangleq -\frac{\log \lambda_i(H^{\mathrm{H}}H)}{\log \rho} \quad \Leftrightarrow \quad \lambda_i(H^{\mathrm{H}}H) = \rho^{-\alpha_i}. \quad (32)$$

Note that by this definition $\sigma_i(H) = \rho^{-\frac{1}{2}\alpha_i}$. The variables, α_i for $i = 1, \ldots, n_{\mathrm{T}}$ are refereed to as the *singularity levels* of H as they give an indication of how close to singular the channel H is in relation to the inverse SNR ρ^{-1}. As $\xi \doteq \rho^0$, $\theta \doteq \rho^{\frac{1}{2} - \frac{rT}{2\kappa}}$ and $\eta = \rho^{\frac{rT}{2\kappa}}$ it holds that

$$\left[\sqrt{k} + \min\left(\frac{2\xi}{\theta\gamma\sigma_{\iota_{2T}(i)}(H)}, 2\sqrt{k}\eta \right) \right]^2 \dot{\leq} \rho^{\nu_i}$$

where

$$\nu_i \triangleq \min\left(\frac{rT}{\kappa} - 1 + \alpha_{\iota_T(i)}, \frac{rT}{\kappa} \right)^{+}. \quad (33)$$

By (31) it follows that

$$N_k \dot{\leq} \prod_{i=1}^{k} \rho^{\nu_i} = \rho^{\sum_{i=1}^{k} \nu_i}. \quad (34)$$

However, as the SNR exponent on the right hand side of (34) is non decreasing in k it must for the total number of visited

nodes N hold that $N = \sum_{k=1}^{\kappa} N_k \overset{.}{\leq} \rho^{\sum_{i=1}^{\kappa} \nu_i}$ or for any given $\delta > 0$ hold that

$$N \leq \rho^{\sum_{i=1}^{\kappa} \nu_i + \delta} \tag{35}$$

provided ρ is sufficiently large.

Consider now the set (cf. (33) and (35))

$$\mathcal{T}(x) \triangleq \left\{ \boldsymbol{\alpha} \mid \sum_{i=1}^{\kappa} \min\left(\frac{rT}{\kappa} - 1 + \alpha_{\iota_{2T}(i)}, \frac{rT}{\kappa} \right)^+ \geq x \right\}, \tag{36}$$

where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{n_{\mathrm{T}}})$. As (35) holds (asymptotically) for any $\delta > 0$, and since $\boldsymbol{\alpha} \notin \mathcal{T}(y)$ implies that $N < \rho^x$ for any $y < x$ by (35) and (33), it follows that

$$\lim_{\rho \to \infty} \frac{\log \mathrm{P}\,(N \geq \rho^x)}{\log \rho} \leq \lim_{\rho \to \infty} \frac{\log \mathrm{P}\,(\boldsymbol{\alpha} \in \mathcal{T}(y))}{\log \rho}.$$

Equivalently (cf. (20))

$$\Psi(x) \geq - \lim_{\rho \to \infty} \frac{\log \mathrm{P}\,(\boldsymbol{\alpha} \in \mathcal{T}(y))}{\log \rho} \tag{37}$$

for $y < x$. The value of the bound in (37) is that the right hand side is readily computed using large deviation theory [29].

C. Large deviations

A sequence of random vectors $\boldsymbol{\beta}_\rho \in \mathbb{R}^n$ parameterized by ρ is said to satisfy the *large deviation principle* [29] with *rate function* I,

$$I : \mathbb{R}^n \mapsto \{\mathbb{R}_+, \infty\},$$

if for every open set $\mathcal{G} \subseteq \mathbb{R}^n$ it holds that

$$\liminf_{\rho \to \infty} \frac{\log \mathrm{P}\,(\boldsymbol{\beta}_\rho \in \mathcal{G})}{\log \rho} \geq - \inf_{\boldsymbol{\beta} \in \mathcal{G}} I(\boldsymbol{\beta}) \tag{38}$$

and if for every closed set $\mathcal{F} \subseteq \mathbb{R}^n$ it holds that

$$\liminf_{\rho \to \infty} \frac{\log \mathrm{P}\,(\boldsymbol{\beta}_\rho \in \mathcal{F})}{\log \rho} \leq - \inf_{\boldsymbol{\beta} \in \mathcal{F}} I(\boldsymbol{\beta}). \tag{39}$$

Although not stated formally, one of the central results of [5] is that the sequence of random variables given by $\boldsymbol{\alpha}_\rho = \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{n_{\mathrm{T}}})$ (cf. (32)) satisfies the large deviation principle with rate function (cf. (38), and proof of Theorem 4 in [5])

$$I(\boldsymbol{\alpha}) = \sum_{i=1}^{n_{\mathrm{T}}} (n_{\mathrm{R}} - n_{\mathrm{T}} + 2i - 1)\alpha_i \tag{40}$$

if $\alpha_1 \geq \ldots \geq \alpha_{n_{\mathrm{T}}} \geq 0$ and $I(\boldsymbol{\alpha}) = \infty$ otherwise. This observation was key in establishing the DMT in [5].

By combining (37) with (39), and noting that $\mathcal{T}(y)$ is a closed set, it follows that

$$\Psi(x) \geq f(y) \triangleq \inf_{\boldsymbol{\alpha} \in \mathcal{T}(y)} I(\boldsymbol{\alpha}) \tag{41}$$

for any $y < x$. As $\mathcal{T}(x) \subseteq \mathcal{T}(y)$ for all $y \leq x$ it follows that $f(y)$ is non-decreasing and it can additionally be verified that $f(y)$ is left-continuous, i.e.,

$$\sup_{y < x} f(y) = f(x),$$

which implies that

$$\Psi(x) \geq f(x) = \inf_{\boldsymbol{\alpha} \in \mathcal{T}(x)} I(\boldsymbol{\alpha}). \tag{42}$$

From (42) it follows that the complexity exponent $c(r)$ is upper bounded by $\bar{c}(r)$ where

$$\bar{c}(r) \triangleq \inf\{x \mid f(x) > d(r)\} = \sup\{x \mid f(x) \leq d(r)\} \tag{43}$$

and where the last equality follows as $f(x)$ is non-decreasing. Further, by the left-continuity of $f(x)$ it follows that the supremum on the right is attained, i.e., the supremum can be replaced by a maximum.

Note however that the condition that $f(x) \leq d(r)$ is satisfied if and only if there exist an $\boldsymbol{\alpha} \in \mathcal{T}(x)$ such that $I(\boldsymbol{\alpha}) \leq d(r)$. Thus, $\bar{c}(r)$ in (43) could alternatively be obtained as the solution to a constrained maximization problem according to

$$\max_{\boldsymbol{\alpha}, x} \quad x \tag{44a}$$

$$\text{s.t.} \quad \sum_{i=1}^{\kappa} \min\left(\frac{rT}{\kappa} - 1 + \alpha_{\iota_T(i)}, \frac{rT}{\kappa} \right)^+ \geq x \tag{44b}$$

$$\sum_{i=1}^{n_{\mathrm{T}}} (n_{\mathrm{R}} - n_{\mathrm{T}} + 2i - 1)\alpha_i \leq d \tag{44c}$$

$$\alpha_1 \geq \ldots \geq \alpha_{n_{\mathrm{T}}} \geq 0, \tag{44d}$$

where (44b) follows from the constraint $\boldsymbol{\alpha} \in \mathcal{T}(x)$, and where (44c) and (44d) follows from $I(\boldsymbol{\alpha}) \leq d(r)$. It is straightforward to show that the optimal x in (44) must be such that (44b) is satisfied with equality. By further noting that the sum in (44b) contains only n_{T} distinct terms, each with multiplicity T, it can be seen that

$$\sum_{i=1}^{\kappa} \min\left(\frac{rT}{\kappa} - 1 + \alpha_{\iota_T(i)}, \frac{rT}{\kappa} \right)^+$$

$$= \sum_{i=1}^{n_{\mathrm{T}}} T \min\left(\frac{r}{n_{\mathrm{T}}} - 1 + \alpha_i, \frac{r}{n_{\mathrm{T}}} \right)^+,$$

where we have also used the full rate assumption that $\kappa = n_{\mathrm{T}} T$. We summarize the above in the following theorem.

Theorem 2: The complexity exponent $c(r)$ of any full rate linear dispersive code with multiplexing gain r and diversity $d(r)$ is upper bounded as $c(r) \leq \bar{c}(r)$ where

$$\bar{c}(r) \triangleq \max_{\boldsymbol{\alpha}} \sum_{i=1}^{n_{\mathrm{T}}} T \min\left(\frac{r}{n_{\mathrm{T}}} - 1 + \alpha_i, \frac{r}{n_{\mathrm{T}}} \right)^+ \tag{45a}$$

$$\text{s.t.} \sum_{i=1}^{n_{\mathrm{T}}} (n_{\mathrm{R}} - n_{\mathrm{T}} + 2i - 1)\alpha_i \leq d(r) \tag{45b}$$

$$\alpha_1 \geq \ldots \geq \alpha_{n_{\mathrm{T}}} \geq 0. \tag{45c}$$

The upper bound given by Theorem 2 can naturally be computed given explicit values for the multiplexing gain r and diversity gain[4] $d(r)$. However, it is also possible in some cases to give general solutions as a function of r when the DMT curve $d(r)$ of the code is known explicitly. In particular, DMT optimal codes such as those presented in [12]–[17] have a diversity gain of $d(k) = (n_{\mathrm{T}} - k)(n_{\mathrm{R}} - k)$ at any integer

---

[4]Note that Theorem 2 does not assume a diversity optimal code.

multiplexing gain $r = k$ [5]. In this case it is straightforward to verify that an[5] optimal $\boldsymbol{\alpha}$ in (45) is given by

$$\alpha_i^\star = 1, \quad \text{for } i = 1, \dots, n_\text{T} - k$$

and

$$\alpha_i^\star = 0, \quad \text{for } i = n_\text{T} - k + 1, \dots, n_\text{T}.$$

To see this, note that the objective function in (45a) is symmetric with respect to permutations of the set of α_i for $i = 1, \dots, n_\text{T}$. As the sum in the diversity constraint (45b) places more weigh on α_j than on α_i, for $j > i$, it is optimal to increase α_1 until the term in (45a) containing α_1 saturates (i.e., when $\alpha_1 = 1$), then to increase α_2 etcetera, until the constraint is satisfied with equality. This yields the aforementioned solution. Note also that $\alpha_1^\star, \dots, \alpha_{n_\text{T}}^\star$ are the same singularity levels that give the typical outages in [5], (cf. Section V-A). Inserting the optimal solution into (45a) yields

$$\bar{c}(k) = \frac{Tk(n_\text{T} - k)}{n_\text{T}},$$

which is a remarkably simple (tight) upper bound on the complexity exponent of any DMT optimal code at integer multiplexing gain $r = k$.

For a DMT optimal code at a possibly non-integer value of r, let k be the integer such that $r \in [k, k+1)$, i.e., $k = \lfloor r \rfloor$. The optimal solution is in this case given by

$$\alpha_i^\star = 1, \quad \text{for } i = 1, \dots, n_\text{T} - k - 1,$$

$$\alpha_i^\star = 0, \quad \text{for } i = n_\text{T} - k + 1, \dots, n_\text{T},$$

and

$$\alpha_{n_\text{T} - k}^\star = k + 1 - r.$$

Substituting the above solution back into (45a) yields

$$\bar{c}(r) = \frac{T}{n_\text{T}} \left(r(n_\text{T} - k - 1) + \left(n_\text{T} k - r(n_\text{T} - 1) \right)^+ \right).$$

We summarize the above in the following theorem.

Theorem 3: The complexity exponent $c(r)$ of any DMT optimal full rate linear dispersive code with integer multiplexing gain $r = k$ is upper bounded as

$$c(k) \le \bar{c}(k) = \frac{Tk(n_\text{T} - k)}{n_\text{T}}. \tag{46}$$

For general r where $0 \le r \le n_\text{T}$ the complexity exponent $c(r)$ is upper bounded as $c(r) \le \bar{c}(r)$ where

$$\bar{c}(r) = \frac{T}{n_\text{T}} \left(r(n_\text{T} - \lfloor r \rfloor - 1) + \left(n_\text{T} \lfloor r \rfloor - r(n_\text{T} - 1) \right)^+ \right). \tag{47}$$

The function $\bar{c}(r)$ in (47) is a piecewise linear function in r, although unlike the optimal DMT $d(r)$ it is not as simple as the set of straight lines connecting its values at integer multiplexing gains. For $n_\text{T} = T = n$ the function in (47) coincides with the curve for $c(r)$ shown in Fig. 1.

[5]In general, (45) does not have a unique optimal point as $\min(a, b)^+$ is constant in a for $a \le 0$ and $a \ge b$.

D. Establishing the exact complexity exponent

We now turn to specific cases where we can exactly establish the complexity exponent $c(r)$ by establishing that the upper bound $c(r) \le \bar{c}(r)$ is in fact tight. To this end, we begin with the following lemma, which provides a sufficient condition for $c(r) = \bar{c}(r)$, i.e., for the tightness of the upper bound.

Lemma 2: Let $\boldsymbol{G}_{|p} \in \mathbb{C}^{\kappa \times Tp}$ be the matrix consisting of the first Tp columns of the generator matrix $\boldsymbol{G} \in \mathbb{C}^{\kappa \times \kappa}$ of some given full rate linear dispersive code. If there for $p = 1, \dots, n_\text{T}$ exists unitary matrices $\boldsymbol{U}_p \in \mathbb{C}^{n_\text{T} \times p}$ such that

$$\text{rank} \left((\boldsymbol{I}_T \otimes \boldsymbol{U}_p^\text{H}) \boldsymbol{G}_{|p} \right) = pT, \tag{48}$$

then $c(r) = \bar{c}(r)$ for all $r \in [0, n_\text{T}]$, where $\bar{c}(r)$ is given by (45) in Theorem 2.

The proof of Lemma 2 is similar in spirit to the proof of Theorem 2, although riddled with technical details, and therefore relegated to Appendix B. In essence, the condition posed in (48) implies that there are certain orientations of the right singular vectors of the channel $\boldsymbol{H}$ (in relation to the code generated by $\boldsymbol{G}$) for which the lower bound in (29) is tight. Details are provided in Appendix B, and some additional interpretations of (48) and the general applicability of the lemma can be found in Section V. However, we first apply Lemma 2 to find $c(r)$ in some very important special cases.

To this end, it is useful to first note that permuting the columns of $\boldsymbol{G}$, i.e., replacing $\boldsymbol{G}$ with $\boldsymbol{G}\boldsymbol{\Pi}$ where $\boldsymbol{\Pi} \in \mathbb{R}^{\kappa \times \kappa}$ is a permutation matrix, does not change the code $\mathcal{X}$. Instead, the effect such a permutation would have is that it would change the order in which the symbols in $\boldsymbol{s}$ are enumerated by the sphere decoder described in Section III-A (cf. [3, Section IV]). In the present context, the first pT columns of $\boldsymbol{G}\boldsymbol{\Pi}$, i.e., $[\boldsymbol{G}\boldsymbol{\Pi}]_{|p}$, may differ from those of $\boldsymbol{G}$. Thus, we see that (48) depends not only on the code itself, but also on the order in which the constituent symbols s_i are enumerated by the sphere decoder (cf. [3], [4] where the topic of detection or column ordering is discussed in detail).

In the context of Lemma 2, it can be seen that as $(\boldsymbol{I}_T \otimes \boldsymbol{U}_p^\text{H}) \boldsymbol{G} \in \mathbb{C}^{nT \times \kappa}$ have rank pT for any unitary $\boldsymbol{U}_p$ due to the full rank assumption on $\boldsymbol{G}$, one can always select pT linearly independent columns, or equivalently, find a permutation matrix $\boldsymbol{\Pi}$ such that $(\boldsymbol{I}_T \otimes \boldsymbol{U}_p^\text{H}) [\boldsymbol{G}\boldsymbol{\Pi}]_{|p}$ has full rank. Using a similar argument, we can recursively construct a (single) $\boldsymbol{\Pi}$ for which there are $\boldsymbol{U}_p$ for $p = 1, \dots, n_\text{T}$ satisfying

$$\text{rank} \left((\boldsymbol{I}_T \otimes \boldsymbol{U}_p^\text{H}) [\boldsymbol{G}\boldsymbol{\Pi}]_{|p} \right) = pT$$

by constructing $\boldsymbol{U}_{p-1}$ from $\boldsymbol{U}_p$ by removing a column, selecting the appropriate columns from $\boldsymbol{G}$, and starting the recursion with an arbitrary $\boldsymbol{U}_{n_\text{T}}$. Interpreting the above in light of Theorem 2 and Lemma 2 we can thus establish that for any full rate linear dispersive code design, $\bar{c}(r)$ as defined in Theorem 2 and given in Theorem 3 for DMT optimal codes, is the tightest upper bound on the complexity exponent that can possibly hold under arbitrary detection orderings. This is formalized in the following.

Theorem 4: Given any full rate linear dispersion code achieving diversity $d(r)$, there is always at least one detection ordering for which $c(r) = \bar{c}(r)$.

However, while Theorem 4 is useful in the sense that it tells us that one could not improve upon the tightness of $\bar{c}(r)$ without introducing further assumptions regarding the particular code design considered, it is obviously not of practical interest to use the worst possible detection ordering. Therefore, we turn our attention to the important class of threaded codes [30] for which we will show that the *natural* detection ordering $\mathbf{\Pi} = \boldsymbol{I}_\kappa$ implies $c(r) = \bar{c}(r)$.

1) Threaded codes: The class of threaded code designs is of particular interest, as it includes full rate codes that perform very well in a variety of settings. The threaded algebraic space-time (TAST) codes [30], codes constructed from CDAs [31], [32], and specifically modified CDA codes [14]–[17] that were shown (cf. [15]) to achieve the DMT tradeoff, are prime examples. The CDA based threaded designs are also the only currently known explicit constructions capable of achieving the DMT for all values of n_T and simultaneously over all $r \in [0, n_\mathrm{T}]$. All these codes have a common threaded structure. Specifically an $n \times n$ threaded code is built from n component codes mapped cyclically in threads (or layers) to the codewords $\boldsymbol{X}$. For example, in the special case of $n = n_\mathrm{T} = T = 4$, the thread structure is given by

$$\begin{bmatrix} 1 & 4 & 3 & 2 \\ 2 & 1 & 4 & 3 \\ 3 & 2 & 1 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

where the numbers $1, 2, 3, 4$ indicate the thread to which a particular entry of $\boldsymbol{X}$ belongs. In general, symbol j in thread l is mapped to $\boldsymbol{X}_{j,k}$ where $k = \mod(j-l, n)+1$ and where $\mod(\cdot, n)$ denotes the modulo n operation. For example, in the case of perfect codes [16], [17] which also employ a threaded structure, the code follows from

$$\mathrm{lay}(\boldsymbol{X}) = \underbrace{\begin{bmatrix} \boldsymbol{B}_0\boldsymbol{C} & & \\ & \ddots & \\ & & \boldsymbol{B}_{n-1}\boldsymbol{C} \end{bmatrix}}_{\boldsymbol{\Upsilon}} \begin{bmatrix} \boldsymbol{s}_1 \\ \vdots \\ \boldsymbol{s}_n \end{bmatrix} \quad (49)$$

where

$$\boldsymbol{B}_i \triangleq \mathrm{Diag}(\underbrace{1, 1, \ldots, 1}_{n-i \text{ entries}}, \underbrace{\gamma, \gamma, \ldots, \gamma}_{i \text{ entries}}), \quad i = 0, \cdots, n-1$$

are full rank diagonal matrices incorporating a properly chosen thread-separating scalar γ, where $\boldsymbol{C} \in \mathbb{C}^{n \times n}$ is a (unitary) full rank generator matrix for the component code of each thread, $\boldsymbol{s}_l \in \mathbb{S}_\eta^n$ are the constellation symbols of thread l, and where $\mathrm{lay}(\boldsymbol{X})$ denotes the matrix to vector operation obtained by stacking the elements of $\boldsymbol{X}$ according to their thread (cf. the column based stacking of the $\mathrm{vec}(\cdot)$ operation).

Regarding the decoding complexity introduced by such codes, we note that the corresponding generator matrix $\boldsymbol{G} \in \mathbb{C}^{n^2 \times n^2}$ is related to $\boldsymbol{\Upsilon}$ through a permutation of the rows in such a way that the (i, j)th block $\boldsymbol{G}_{ij} \in \mathbb{C}^{n \times n}$ of $\boldsymbol{G}$ contains exactly one non zero row which it self is one of the rows

of $\boldsymbol{B}_{j-1}\boldsymbol{C}$. Consequently, $\boldsymbol{G}_{|ip} \triangleq \begin{bmatrix} \boldsymbol{G}_{i1} & \cdots & \boldsymbol{G}_{ip} \end{bmatrix} \in \mathbb{C}^{n \times np}$ has rank p and contains exactly p non-zero rows. This holds for any n and $p \leq n$. Now, let $\boldsymbol{U}_p \in \mathbb{C}^{n \times p}$ be a unitary matrix with the property that any p rows of $\boldsymbol{U}_p$ are linearly independent. Such matrices can clearly be constructed, and an example is the matrix that contains the first p discrete Fourier transform (DFT) vectors of length n. Let $\tilde{\boldsymbol{G}}_{|ip} \in \mathbb{C}^{p \times np}$ be the matrix containing only the non-zero rows of $\boldsymbol{G}_{|ip} \in \mathbb{C}^{p \times np}$, and let $\tilde{\boldsymbol{U}}_{ip} \in \mathbb{C}^{p \times p}$ be the full rank matrix consisting of the rows of $\boldsymbol{U}_p$ matching the non-zero rows of $\boldsymbol{G}_{|ip}$. It follows that

$$(\boldsymbol{I}_n \otimes \boldsymbol{U}_p^\mathrm{H})\boldsymbol{G}_{|p} = \underbrace{\begin{bmatrix} \tilde{\boldsymbol{U}}_{1p}^\mathrm{H} & & \\ & \ddots & \\ & & \tilde{\boldsymbol{U}}_{np}^\mathrm{H} \end{bmatrix}}_{\tilde{\boldsymbol{U}}_p} \underbrace{\begin{bmatrix} \tilde{\boldsymbol{G}}_{|1p} \\ \vdots \\ \tilde{\boldsymbol{G}}_{|np} \end{bmatrix}}_{\tilde{\boldsymbol{G}}_{|p}} \in \mathbb{C}^{np \times np}$$

is full rank as both $\tilde{\boldsymbol{U}}_p \in \mathbb{C}^{np \times np}$ and $\tilde{\boldsymbol{G}}_{|p} \in \mathbb{C}^{np \times np}$ are full rank and square matrices. Note also that the same argument can be made regardless of the ordering of the threads, and for any other code with a threaded structure, provided the symbols in $\boldsymbol{s}$ are grouped into layers as in (49). This is stated in the following.

Theorem 5: The SD complexity exponent, given any threaded code with $n = n_\mathrm{T} = T$ that is decoded with the natural detection ordering or under any other threat-wise grouping, is $c(r) = \bar{c}(r)$ where $\bar{c}(r)$ is given in Theorem 2.

Consequently directly from Theorems 3 and 5, we have the following result for the $n_\mathrm{T} \times n_\mathrm{R}$ quasi-static Rayleigh fading MIMO channel.

Theorem 6: Sphere decoding with thread-wise grouping of any DMT optimal threaded code with $n = n_\mathrm{T} = T$, achieves DMT optimality with a complexity exponent of

$$c(r) = r(n - \lfloor r \rfloor - 1) + (n\lfloor r \rfloor - r(n-1))^+ \quad (50)$$

which, for integer values of $r = k$, simplifies to

$$c(k) = k(n-k). \quad (51)$$

We briefly note that as expected the complexity increases with increasing n_T for any fixed r which is quite natural as the size of the codebook $\mathcal{X}$ and the signal space dimension increase. One can however note that $c(r)$ is independent of the number of receive antennas n_R (provided $n_\mathrm{R} \geq n_\mathrm{T}$). This is specific to the DMT optimal behavior and threaded structure of the codes, and may be explained by the fact that even though the channel quality generally improves by adding receive antennas - thus generally reducing complexity - the same improvement also occurs in the error probability performance of the code, and these two effects cancel each other in the complexity exponent.

2) 2×2 approximately universal codes: We here go one step further and identify classes of codes for which we can state, without limitations on the actual coding structure, that $c(r) = \bar{c}(r)$ for any detection ordering. This is done herein for the class of all 2×2 approximately universal codes, i.e., all

minimum delay codes that can achieve DMT optimality over the $2 \times n_R$ channel irrespective of fading statistics [33].

We are able to show, albeit only for the specific case of $n_T \times T = 2 \times 2$, that (48) follows from the so called non-vanishing determinant (NVD) condition [32] which is well known to be a necessary and sufficient condition for approximate universality. We consequently have the following.

Theorem 7: Any 2×2 full rate approximately universal linear dispersive code, irrespective of its structure, introduces a SD complexity exponent of

$$c(r) = \max(r, 2 - r).$$

As the NVD property is not dependent on the ordering of the columns of G, it also follows that the conclusion of Theorem 7 holds irrespective of the detection ordering.

V. Implications and Discussions

A. Decoding complexity and information theoretic outages

The claim of Theorem 2 may be expressed in terms of the function (cf. (45a))

$$\bar{c}(r : \boldsymbol{\alpha}) \triangleq \sum_{i=1}^{n_T} T \min \left(\frac{r}{n_T} - 1 + \alpha_i , \; \frac{r}{n_T} \right)^+ ,$$

which provides a conditional, asymptotic, upper bound on the sphere decoding complexity according to $N \leq \rho^{\bar{c}(r:\boldsymbol{\alpha})}$ in terms of the singularity level $\boldsymbol{\alpha}$. The final upper bound $\bar{c}(r)$ is then given as the worst case $\bar{c}(r : \boldsymbol{\alpha})$ over all singularity levels that occur with a probability that is larger than or equal to the probability of error, given asymptotically by the diversity gain $d(r)$ of the code.

This interpretation is similar to the notion of typical error events in [5]. In particular, the characterization of the DMT in [5] relies on the asymptotic probability of outages at high SNR, i.e., the probability that the i.i.d. Rayleigh fading AWGN channel given by

$$\boldsymbol{y}_t = \boldsymbol{H}\boldsymbol{x}_t + \boldsymbol{w}_t$$

with a power constraint $\mathrm{E}\left\{ \|\boldsymbol{x}_t\|^2 \right\} \leq \rho$ cannot support an asymptotic data-rate of $R = r \log \rho + o(\log \rho)$. As was shown in [5], this occurs when the singularity levels belong to the outage set $\mathcal{A}(r) = \{ \boldsymbol{\alpha} \mid \sum_i (1 - \alpha_i)^+ < r \}$, and the diversity of the outage event is given by the most likely set of singularity levels that satisfy this condition, i.e., $d(r) = \inf_{\boldsymbol{\alpha} \in \mathcal{A}(r)} I(\boldsymbol{\alpha})$ (cf. 40).

If we restrict attention to the set of singularity levels whose probability of occurring does not vanish exponentially fast, i.e., for which $I(\boldsymbol{\alpha}) < \infty$ or equivalently $\alpha_{n_T} \geq \ldots \geq \alpha_1 \geq 0$, we can for DMT optimal codes[6], make an interesting connection between the decoding complexity and information theoretic outages. In particular, for $0 \leq r \leq n_T$ the infimum of $I(\boldsymbol{\alpha})$ is not attained over $\mathcal{A}$ which implies (cf. 40) that $\sum_i (n_R -$

---

[6]To be precise, we are assuming here that we are working with approximately universal codes for which it is known that errors are only likely when the channel is in outage [33]. All explicitly constructed full rate DMT-optimal codes known to date, are also approximately universal.

$n_T + 2i - 1)\alpha_i \leq d(r)$ if and only if $\sum_i (1 - \alpha_i)^+ \geq r$. We can thus obtain the bound $\bar{c}(r)$ by solving

$$\bar{c}(r) = \max_{\boldsymbol{\alpha}} \bar{c}(r : \boldsymbol{\alpha}) \tag{52a}$$

$$\text{s.t. } \sum_{i=1}^{n_T} (1 - \alpha_i)^+ \geq r \tag{52b}$$

$$\alpha_1 \geq \ldots \geq \alpha_{n_T} \geq 0 , \tag{52c}$$

which may be interpreted as the worst case complexity (bound) over all channels that are not in outage.

The concept is illustrated for $n_T = T = 2$ in Fig. 2 where $\bar{c}(r : \boldsymbol{\alpha})$ is plotted as a function of $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$ over $\alpha_1 \geq \alpha_2 \geq 0$. In this case, $\bar{c}(r) = \max(r, 2 - r)$. Note also here that we know by Theorem 7 that $c(r) = \bar{c}(r)$. Singularity levels that are in the outage region $\sum_i (1 - \alpha_i)^+ < r$ are shown in a darker shade. It can be seen that increasing the multiplexing gain r increases the codeword density and consequently broadens the set of singularity levels that can potentially lead to higher complexity. However, increasing the multiplexing gain also reduces the set of channels that support the data-rate, thus limiting the set of singularity levels for which the decoder needs to be applied, leading to an overall reduction in the complexity exponent as r approaches its maximum value.

However, in general, the observations made above are one-sided in the sense that we may omit to decode when the channel is in outage, but a channel not in outage does not necessarily imply low decoding complexity. There can be channels that incur high decoding complexity while not in outage. For the sphere decoder, such channels may be constructed by allowing one or several α_i to be negative, i.e., for one or several eigenvalues of $\boldsymbol{H}^H \boldsymbol{H}$ to be atypically large. However, as these channels occur with a probability that vanish exponentially fast with ρ, they can also be safely ignored when decoding without degrading the probability of error in the high SNR asymptote, as was argued in Section III-D. Essentially, any set of channels with probability mass less than the probability of outages may be safely ignored by the decoder. This is intrinsically captured in the complexity measure given by the complexity exponent as it is tied to the probability of error directly rather than the set of channels in outage. Finally, it is illustrative to note that the discussion above does not explicitly depend on the i.i.d. Rayleigh fading assumption. Therefore, (52) provides a universal upper bound on the SD complexity exponent given any fading distribution for which (52c) is violated with a probability that vanishes exponentially fast.

Towards gaining further intuition for the result of Theorem 6, and in particular (51), it is illustrative to consider a heuristic argument involving low rank channel matrices $\boldsymbol{H}$. As noted in [5], the typical outages at integer multiplexing gains $r = k$ are caused by channels that are close to the set of rank k matrices, i.e., that have $n - k$ small eigenvalues. If we for the purpose of the illustration assume that $\boldsymbol{H}$ has rank k, it follows that $\boldsymbol{I}_n \otimes \boldsymbol{H}$, and $\boldsymbol{M}$, have rank nk, and consequently a null-space of dimension $n(n - k)$. This implies that the
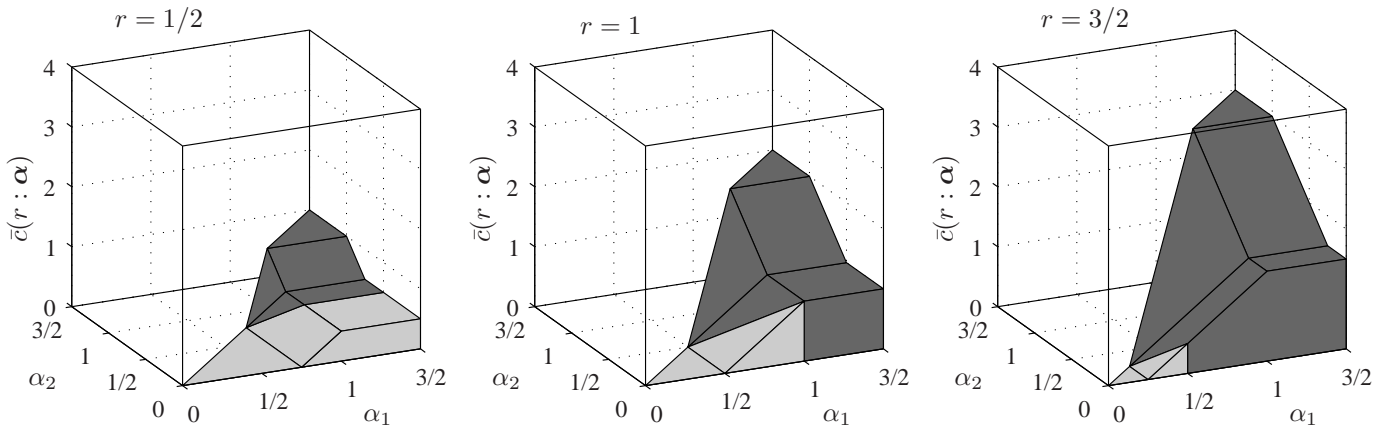
Fig. 2. Conditional complexity exponent bound $\bar{c}(\boldsymbol{\alpha})$ as a function of singularity level $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$. Singularity levels that corresponds to outage events at the target multiplexing gain r are shown in dark grey, while singularity levels capable of supporting the target multiplexing gain are shown in light grey.

$n(n-k) \times n(n-k)$ lower right block of $\boldsymbol{R}$ is[7] identically equal to zero, and the sphere decoder pruning ~~criteria become~~ totally ineffective up to and including layer $n(n-k)$. As the size of $\mathbb{S}_\eta$ is $|\mathbb{S}_\eta| \doteq \rho^{\frac{k}{n}}$ for $r = k$, we see that the number of nodes searched at layer $n(n-k)$ of the SD search tree is $|\mathbb{S}_\eta^{n(n-k)}| \doteq \rho^{k(n-k)}$ (cf. (51)). In order to ensure close to optimal performance, the sphere decoder must be able to decode for channels where $n - k$ singular values are close to zero. However, channels with even more singular values close to zero occur with a probability that is small in relation to the outage probability or the probability of ML decoder error, and can thus be safely ignored by the decoder.

B. Fast decodable codes

In [34]–[36] a family of DMT optimal $n_T \times T = 2 \times 2$ space-time codes called fast decodable codes [37] were constructed. The complexity exponent (and also its upper bound) provides an interesting approach for comparing regular codes with the fast decodable codes. Before doing so it should be noted that these fast decodable codes are not, strictly speaking, of the form in (3) as the real and imaginary part of each constituent symbol is dispersed separately. Nevertheless, the fast decodable codes may be decoded by an equivalent *real valued* sphere decoder that performs a search over a regular tree with 2κ layers and $|\mathbb{S}_\eta|^{\frac{1}{2}}$ branches per node, and we can compare the reported worst case complexity of this real valued sphere decoder to the complexity of the complex valued sphere decoder considered herein.

The fast decodable codes have the appealing property that the upper right 4×4 block of the real valued $\boldsymbol{R} \in \mathbb{R}^{8 \times 8}$ (cf. (13)) is always a diagonal matrix, regardless of the particular realization of $\boldsymbol{H}$. While the regular real valued sphere decoder for a 2×2 full rate code would perform a (bounded) search over the entire tree, it is sufficient for the fast decodable codes to (without loss of optimality) perform a search over only the 4 first layers, and extend each node at layer 4 to a valid codeword

---

[7]This also requires that the first nk columns of $\boldsymbol{R}$ are linearly independent. In fact, the rigorous treatment of the technical detail is largely responsible for much of the difficulty in establishing the lower bounds on $c(r)$ in [?].
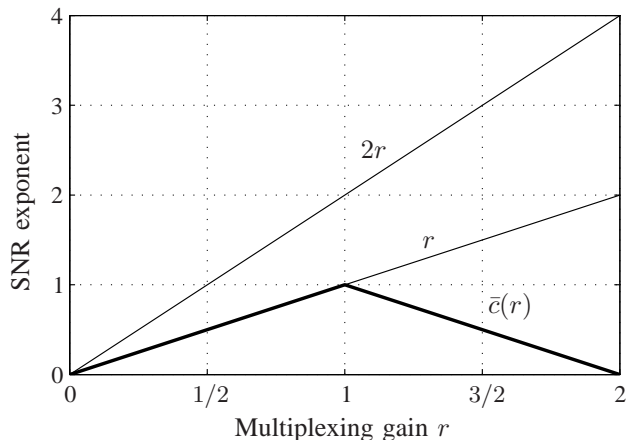

Fig. 3. Comparing the SD complexity exponent $c(r) = \min(r, 2-r)$, with the (worst-case) SNR exponent $(2r)$ of the regular sphere decoder, and with the maximal SNR exponent (r) of the simplified sphere decoder.

through a faster, linear, ML decoding. This simplified version of the real valued sphere decoder can be viewed as a search over a regular tree where each node has $|\mathbb{S}_\eta|^{\frac{1}{2}}$ children up to layer 4, but only one child per node for the 4 remaining layers. Consequently, the worst case number of nodes visited by the simplified sphere decoder is $5|\mathbb{S}_\eta|^{\frac{4}{2}} + \sum_{k=1}^{3} |\mathbb{S}_\eta|^{\frac{k}{2}} \doteq |\mathbb{S}_\eta|^2 \doteq \rho^r$ as opposed to $\sum_{k=1}^{8} |\mathbb{S}_\eta|^{\frac{k}{2}} \doteq \rho^{2r}$ for the regular real valued sphere decoder, cf. [37]. Thus, fast decodability implies a reduction by a factor of 2 in the worst case SNR exponent, which is significant at high SNR.

However, this worst case SNR exponent of the simplified SD should be viewed in light of the complexity exponent of any 2×2 approximately universal code as given by Theorem 7, i.e., $c(r) = \min(r, 2-r)$. The worst-case SNR exponent of the regular sphere decoder and of the simplified sphere decoder, and the SD complexity exponent $c(r)$ are shown in Fig. 3. For multiplexing gains lower than or equal to 1, the SD complexity exponent and the worst-case SNR exponent of the simplified sphere decoder actually coincide, while the SD complexity exponent is strictly lower for multiplexing gains higher than one. The interpretation is that a run-time constrained sphere

decoder will yield asymptotic ML performance for *any* 2×2 approximately universal code at a complexity that is comparable to the reported worst case complexity of the fast decodable codes at low multiplexing gains, and significantly better at high multiplexing gains. Thus, in a sense, all approximately universal codes are fast decodable at high SNR. However, we hasten to add that the fast decodable structure can naturally still be desirable in many cases of practical interest.

C. The applicability of Lemma 2

Finally, we discuss the application of Lemma 2 to codes not considered herein. To this end, note that for any given generator matrix G of some code not covered by Section IV-D, it should be clear that if (48) holds then Lemma 2 could be used to establish a tight lower bound on $c(r)$. This said, we also wish to caution the reader that (48) only represents a sufficient condition for $c(r) = \bar{c}(r)$. It does not necessarily follow that $c(r) < \bar{c}(r)$ if (48) is not true. In other words, the question of if there are code designs that improve upon the bound $\bar{c}(r)$ is not answered in the positive by finding code designs for which (48) does not hold.

As for testing (48) it should also be noted that one does not have to restrict the search for U_p to the set of unitary matrices. Any full rank matrix $A \in \mathbb{C}^{n_\mathrm{T} \times p}$ can be factored, e.g., by the QR decomposition, as $U_p T = A$ where $T \in \mathbb{C}^{p \times p}$ has rank p and where U_p is unitary. Hence, as $(I_T \otimes T^\mathrm{H})$ is full rank, it follows that

$$(I_T \otimes A^\mathrm{H})G_{|p} = (I_T \otimes T^\mathrm{H})(I_T \otimes U_p^\mathrm{H})G_{|p}$$

is rank deficient if and only if (48) fails to hold. Hence, the statement of Lemma 2 could be phrased in terms of the existence of any U_p, not necessarily unitary.

Further, let

$$p(A) \triangleq |(I_T \otimes A^\mathrm{H})G_{|p}| ,$$

where $| \cdot |$ denotes the determinant, and note that $p(A)$ is a polynomial in the elements of A. It can thus be seen that if $p(A) \neq 0$ for some $A \in \mathbb{C}^{n_\mathrm{T} \times p}$, i.e., $p(A)$ is not the zero polynomial, it follows that the set of A for which $p(A) = 0$ has zero Lebesgue measure. It is then a straightforward extension to show that (48) holds either never or almost always with respect to the set of unitary matrices U_p over the Stiefel manifold (i.e., the set of all unitary $n \times p$ matrices) endowed with the Haar (uniform) measure. This suggests a rather interesting conceptual method for verifying (48). Given a specific generator matrix one could at least in theory test the condition of Theorem 2 by selecting U_p (or A) uniformly at random, and the condition of Theorem 2 would be proven with probability one if true. However, finite precision computations will limit the practical applicability of such an approach, although symbolic computations could potentially be a way to test a specific code design.

VI. Conclusion

The work applies as an analytical tool in communication settings where rate, reliability and computational complexity are principal intertwined concerns. In this setting, the work
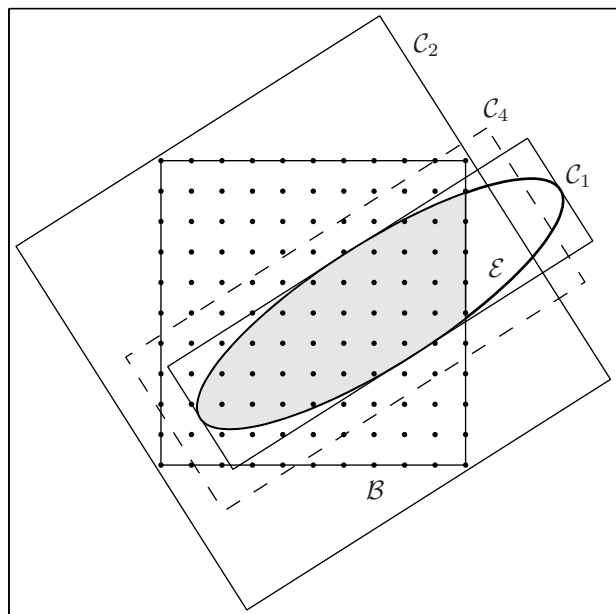

Fig. 4. Illustration of the proof of (26) in Lemma 1 in the case of $n = 2$. The lemma provides an upper bound on the number of integer points within the shaded area, corresponding to the intersection of the ellipsoid and the constellation boundary.

bounds the complexity required for achieving decoding with an ML gap that vanishes with increasing SNR.

The introduced SD complexity exponent was computed for a large family of lattice designs, and often assumed a simple closed form; especially when the DMT performance of the code designs is known. We hope that this simplicity will provide insight and guidance in designing robust encoders and decoders. In light of Lemma 2, the results may help in further unifying encoding and decoding methodologies, and may serve as construction criteria for faster-to-decode linear dispersive lattice codes. The provided limits and guarantees can be used for planning operational policies in networks: for example, in the presence of complexity limitations the results can assist in selecting preferable rate-SNR regions of operation, resulting in savings on power, hardware and processors.

TODO can say that we have set the stage for the race of reducing this exponent, given ML vanishing (shift of the fundamental task)

Appendix A
Proof of Lemma 1

In the following, we provide a proof of Lemma 1, starting with the upper bound in (26) and then establishing the lower bound in (27). To this end, note that the length of the ith semi-axis of $\mathcal{E}$, denoted e_i, is given by

$$e_i \triangleq \frac{2\xi}{\sigma_i(D)} .$$

Let $\mathcal{C}_1$ be the smallest orthotope (box), aligned with and containing $\mathcal{E}$, i.e., $\mathcal{C}_1$ is an orthotope with side lengths e_i (cf. Fig. 4). Let $\mathcal{C}_2$ be a hypercube with side-length $2\sqrt{n}\eta$, centered at the origin and aligned with $\mathcal{C}_1$ (cf. Fig. 4). As the

diagonal of $\mathcal{B}$ is $2\sqrt{n}\eta$ it follows that $\mathcal{B} \subset \mathcal{C}_2$, regardless of the orientation of $\mathcal{C}_2$. Let $\mathcal{C}_3$ be given by $\mathcal{C}_3 = \mathcal{C}_1 \cap \mathcal{C}_2$ and note that $\mathcal{E} \cap \mathcal{B} \subset \mathcal{C}_3$ as $\mathcal{E} \subset \mathcal{C}_1$ and $\mathcal{B} \subset \mathcal{C}_2$. As $\mathcal{C}_1$ and $\mathcal{C}_2$ are aligned, it follows that $\mathcal{C}_3$ is also an orthotope. Let $l_1, \ldots, l_n$ denote the side-lengths of $\mathcal{C}_3$ and note that $l_i \leq \min(e_i, 2\sqrt{n}\eta)$.

As noted in Section IV the number of integer lattice points in a set may be approximated by its volume. This notion can be made precise by noting that for any (bounded and measurable) set $\mathcal{C} \subset \mathbb{R}^n$ it follows that

$$\mathrm{Vol}(\mathcal{C}) = \int_{\mathcal{U}} |\mathbb{Z}^n \cap \mathcal{C} + \boldsymbol{u}| d\boldsymbol{u} \qquad (53)$$

where

$$\mathcal{U} \triangleq \left[-\tfrac{1}{2}, \tfrac{1}{2} \right]^n$$

denotes the unit cube in $\mathbb{R}^n$, i.e., the volume of the set equals the average number of integer points in the set when perturbed by a uniform random perturbation over the unit cube [27]. Let $\mathcal{C}_4$ be the orthotope, aligned with and centered around $\mathcal{C}_3$, with side lengths $l_i + \sqrt{n}$ (cf. Fig. 4). By construction, it follows that

$$\mathcal{C}_3 \subset \mathcal{C}_4 + \boldsymbol{u}$$

for any $\boldsymbol{u} \in \mathcal{U}$. It therefore follows by (53) that

$$|\mathcal{C}_3 \cap \mathbb{Z}^n| \leq \mathrm{Vol}(\mathcal{C}_4) = \prod_{i=1}^{n} \left[\sqrt{n} + l_i \right],$$

where

$$l_i \leq \min\left(\frac{2\xi}{\sigma_i(\boldsymbol{D})}, 2\sqrt{n}\eta \right).$$

As $\mathcal{E} \cap \mathcal{B} \subset \mathcal{C}_3$ the upper bound in (26) follows.

In order to establish the lower bound in (27) we may redefine $\mathcal{C}_1$ to be the orthotope, aligned with the semiaxes of $\mathcal{E}$ and with the same center, having side-lengths

$$b_i = \frac{2\xi}{\sqrt{n}\sigma_i(\boldsymbol{D})},$$

for $i = 1, \ldots, n$. Now, by construction $\mathcal{C}_1 \subset \mathcal{E}$ which implies that $|\mathcal{C}_1 \cap \mathbb{Z}^n| \leq |\mathcal{E} \cap \mathbb{Z}^n|$. Let $\mathcal{C}_2$ be another orthotope, aligned with $\mathcal{C}_1$ and with side-lengths $\max(b_i - \sqrt{n}, 0)$. It follows that $\mathcal{C}_2 + \boldsymbol{u} \subset \mathcal{C}_1$ for any $\boldsymbol{u} \in \mathcal{U}$, where $\mathcal{U} = [-\tfrac{1}{2}, \tfrac{1}{2}]^n$ denotes the unit cube. By reasoning similar to what is used in the proof of the upper bound (cf. (53)) it follows that

$$|\mathcal{E} \cap \mathbb{Z}^n| \geq \mathrm{vol}(\mathcal{C}_2) = \prod_{i=1}^{n} \max(b_i - \sqrt{n}, 0),$$

which establish the lower bound in (27).

APPENDIX B
PROOF OF LEMMA 2

Let $\boldsymbol{\alpha}^\star = (\alpha_1^\star, \ldots, \alpha_{n_\mathrm{T}}^\star)$ be an optimal point of (45) and let q be the largest integer for which (cf. (45a))

$$\frac{r}{n_\mathrm{T}} - 1 + \alpha_q^\star > 0. \qquad (54)$$

It follows that $\alpha_i^\star > 0$ for $i = 1, \ldots, q$ and we may without loss of generality assume that $\alpha_i^\star \leq 1$ for $i = 1, \ldots, n_\mathrm{T}$ as the objective in (45) does not increase in α_i beyond $\alpha_i = 1$. The goal will be to show that layer $k = qT$ of the sphere

decoder contains close to $\rho^{\bar{c}(r)}$ nodes with a probability that is large with respect to the probability of decoding error $\mathrm{P}\left(\boldsymbol{X}_\mathrm{ML} \neq \boldsymbol{X}\right) \doteq \rho^{-d(r)}$.

To this end, let $\boldsymbol{H}^\mathrm{H}\boldsymbol{H} = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^\mathrm{H}$ be the eigenvalue decomposition of $\boldsymbol{H}^\mathrm{H}\boldsymbol{H}$, where

$$\boldsymbol{\Lambda} \triangleq \mathrm{Diag}(\lambda_1(\boldsymbol{H}^\mathrm{H}\boldsymbol{H}), \ldots, \lambda_{n_\mathrm{T}}(\boldsymbol{H}^\mathrm{H}\boldsymbol{H}))$$

and $\boldsymbol{U}^\mathrm{H}\boldsymbol{U} = \boldsymbol{I}$. Let $\boldsymbol{U}_p$ denote the last $p \triangleq n_\mathrm{T} - q$ columns of $\boldsymbol{U}$ (corresponding to the p largest eigenvalues) and let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{n_\mathrm{T}})$ be the random vector of singularity levels given by (32). Now, consider the set of conditions (or events) given by

$$\Omega_1 \triangleq \{ \, \alpha_i^\star - 2\delta < \alpha_i < \alpha_i^\star - \delta, \; i = 1, \ldots, q, $$
$$0 < \alpha_i < \delta, \; i = q+1, \ldots, n_\mathrm{T} \}, \qquad (55a)$$

for some given (small) $\delta > 0$,

$$\Omega_2 \triangleq \{ \sigma_1((\boldsymbol{I}_T \otimes \boldsymbol{U}_p^\mathrm{H})\boldsymbol{G}_{|p}) \geq u \}, \qquad (55b)$$

for some given $u > 0$,

$$\Omega_3 \triangleq \{ \|\boldsymbol{Q}^\mathrm{H}\boldsymbol{w}\| \leq 1 \}, \qquad (55c)$$

and

$$\Omega_4 \triangleq \{ \|\boldsymbol{s}\| \leq \tfrac{1}{2}\eta \}. \qquad (55d)$$

Note also that by choosing δ sufficiently small, we may without loss of generality assume that Ω_1 implies that $\alpha_i > 0$ for all $i = 1, \ldots, n_\mathrm{T}$.

The following proof is structured as follows: First, in Sections B-A and B-B, it is established that (55) represent sufficient conditions for the number of nodes N_k visited in layer $k = qT$ to be close to $\rho^{\bar{c}(r)}$. Then, in Section B-C, it is established that the set of conditions in (55) are simultaneously satisfied with a probability that is large with respect to the probability of error.

A. The Constellation boundary

We begin by proving that, given (55), the constellation boundary may be ignored, i.e., that $\mathbb{S}_\eta$ may be replaced by $\mathbb{S}_\infty$ in (16) without changing the result, thus making the lower bound (27) in Lemma 1 applicable. To this end, let $\hat{\boldsymbol{s}}_k \in \mathbb{S}_\infty^k$ be an arbitrary point in the k-dimensional infinite constellation (i.e., the Gaussian integer lattice) and assume that $\hat{\boldsymbol{s}}_k$ satisfies the sphere constraint at layer k, i.e.

$$\|\boldsymbol{r}_k - \boldsymbol{R}_k\hat{\boldsymbol{s}}_k\| \leq \xi.$$

Note that $\boldsymbol{r}_k = \boldsymbol{R}_k\boldsymbol{s}_k + \boldsymbol{v}_k$, where $\boldsymbol{s}_k$ denotes the last k components of the transmitted symbol vector $\boldsymbol{s} \in \mathbb{S}_\eta^\kappa$ and where $\boldsymbol{v}_k$ denotes the last k components of $\boldsymbol{v} \triangleq \boldsymbol{Q}^\mathrm{H}\boldsymbol{w}$. It follows that

$$\|\boldsymbol{r}_k - \boldsymbol{R}_k\hat{\boldsymbol{s}}_k\| = \|\boldsymbol{R}_k(\boldsymbol{s}_k - \hat{\boldsymbol{s}}_k) + \boldsymbol{v}_k\|$$
$$\geq \sigma_1(\boldsymbol{R}_k)\|\hat{\boldsymbol{s}}_k - \boldsymbol{s}_k\| - \|\boldsymbol{v}_k\|$$

which implies that

$$\|\hat{\boldsymbol{s}}_k - \boldsymbol{s}_k\| \leq \frac{1}{\sigma_1(\boldsymbol{R}_k)}(\xi + \|\boldsymbol{v}_k\|)$$

and

$$\|\hat{\boldsymbol{s}}_k\| \leq \frac{1}{\sigma_1(\boldsymbol{R}_k)}(\xi + \|\boldsymbol{v}_k\|) + \|\boldsymbol{s}_k\| . \qquad (56)$$

By the interlacing property of singular values (cf. (29)) it further follows that

$$\sigma_1(\boldsymbol{R}_k) \geq \theta\gamma\sigma_1(\boldsymbol{H}) \doteq \rho^{\frac{1}{2} - \frac{rT}{2\kappa} - \frac{1}{2}\alpha_1} \geq \rho^{\frac{1}{2}\delta - \frac{rT}{2\kappa}}$$

where we recall that $\theta \doteq \rho^{\frac{1}{2} - \frac{rT}{2\kappa}}$ is the power scaling and $\gamma = \sigma_1(\boldsymbol{G}) > 0$, and where the last inequality is implied by (55a) and $\alpha_1^\star \leq 1$. As $\xi \doteq \rho^0$ and $\|\boldsymbol{v}_k\| \leq \|\boldsymbol{Q}^{\mathrm{H}}\boldsymbol{w}\| \leq 1$ by (55c) it follows that

$$\frac{1}{\sigma_1(\boldsymbol{R}_k)}(\xi + \|\boldsymbol{v}_k\|) \dot{\leq} \rho^{\frac{rT}{2\kappa} - \frac{1}{2}\delta} .$$

By (56), (55d), $\|\boldsymbol{s}_k\| \leq \|\boldsymbol{s}\| \leq \eta$ and since $\rho^{\frac{rT}{2\kappa} - \frac{1}{2}\delta} < \frac{1}{2}\eta$, it follows that

$$\|\hat{\boldsymbol{s}}_k\| \leq \eta$$

given that ρ is sufficiently large. This implies that $\hat{\boldsymbol{s}}_k \in \mathbb{S}_\eta^k$. Thus, any integer point that satisfies the sphere constraint must also belong to the constellation, and we can proceed using (27) to lower bound the complexity.

B. Singular value bounds

We proceed to provide bounds on the singular values of $\boldsymbol{R}_k$ in order to lower bound the number of nodes visited in layer $k = qT$. However, as stated previously the interlacing theorem is, unlike in the derivation of the upper bound, not sufficient for our purposes. Instead, we consider the following lemma, proven in Appendix C.

Lemma 3: Let $\boldsymbol{A} \in \mathbb{C}^{m \times n}$, $m \geq n$ be an arbitrary matrix and $\boldsymbol{QR} = \boldsymbol{A}$ be the QR decomposition of $\boldsymbol{A}$. Partition $\boldsymbol{A}$, $\boldsymbol{Q}$ and $\boldsymbol{R}$ according to

$$\begin{bmatrix} \boldsymbol{A}_1 & \boldsymbol{A}_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{Q}_1 & \boldsymbol{Q}_2 \end{bmatrix} \begin{bmatrix} \boldsymbol{R}_{11} & \boldsymbol{R}_{12} \\ \boldsymbol{0} & \boldsymbol{R}_{22} \end{bmatrix} .$$

where $\boldsymbol{A}_1 \in \mathbb{C}^{m \times n-k}$ and $\boldsymbol{R}_{22} \in \mathbb{C}^{k \times k}$. Then, assuming that $\sigma_i(\boldsymbol{A}) < \sigma_1(\boldsymbol{A}_1)$ for $i = 1, \dots, k$, it holds that

$$\sigma_i(\boldsymbol{R}_{22}) \leq \left[\frac{\sigma_n(\boldsymbol{A})}{\sigma_1(\boldsymbol{A}_1)} + 1\right] \sigma_i(\boldsymbol{A}) . \qquad (57)$$

Applied to the effective channel matrix $\boldsymbol{M}$ it follows that

$$\sigma_i(\boldsymbol{R}_k) \leq \left[\frac{\sigma_\kappa(\boldsymbol{M})}{\sigma_1(\boldsymbol{M}_1)} + 1\right] \sigma_i(\boldsymbol{M}) \qquad (58)$$

where $\boldsymbol{M}_1$ contains the first pT columns $(p = n_{\mathrm{T}} - q)$ of $\boldsymbol{M}$, assuming that $\sigma_i(\boldsymbol{M}) < \sigma_1(\boldsymbol{M}_1)$ as will be shown for $i = 1, \dots, qT$ later. In order to lower bound $\sigma_1(\boldsymbol{M}_1)$ note that

$$\boldsymbol{M}_1 = \theta(\boldsymbol{I}_T \otimes \boldsymbol{H})\boldsymbol{G}_{|p} ,$$

where $\boldsymbol{G}_{|p}$ denotes the first pT columns of $\boldsymbol{G}$ and

$$\boldsymbol{M}_1^{\mathrm{H}}\boldsymbol{M}_1 = \theta^2 \boldsymbol{G}_{|p}^{\mathrm{H}}(\boldsymbol{I}_T \otimes \boldsymbol{H}^{\mathrm{H}}\boldsymbol{H})\boldsymbol{G}_{|p} .$$

As

$$\boldsymbol{H}^{\mathrm{H}}\boldsymbol{H} \succeq \lambda_{q+1}(\boldsymbol{H}^{\mathrm{H}}\boldsymbol{H})\boldsymbol{U}_p\boldsymbol{U}_p^{\mathrm{H}}$$

where $\succeq$ denotes the partial ordering induced by the positive semidefinite cone it follows that

$$\boldsymbol{M}_1^{\mathrm{H}}\boldsymbol{M}_1 \succeq \theta^2\lambda_{q+1}(\boldsymbol{H}^{\mathrm{H}}\boldsymbol{H})\boldsymbol{G}_{|p}^{\mathrm{H}}(\boldsymbol{I}_T \otimes \boldsymbol{U}_p\boldsymbol{U}_p^{\mathrm{H}})\boldsymbol{G}_{|p} .$$

Considering the smallest eigenvalue of $\boldsymbol{M}_1^{\mathrm{H}}\boldsymbol{M}_1$ yields

$$\lambda_1(\boldsymbol{M}_1^{\mathrm{H}}\boldsymbol{M}_1) \geq \theta^2\lambda_{q+1}(\boldsymbol{H}^{\mathrm{H}}\boldsymbol{H})\lambda_1(\boldsymbol{G}_{|p}^{\mathrm{H}}(\boldsymbol{I}_T \otimes \boldsymbol{U}_p\boldsymbol{U}_p^{\mathrm{H}})\boldsymbol{G}_{|p})$$

and for the smallest singular value

$$\sigma_1(\boldsymbol{M}_1) \geq u\theta\sigma_{q+1}(\boldsymbol{H}) = u\theta\rho^{-\frac{1}{2}a_{q+1}} \dot{\geq} \rho^{\frac{1}{2} - \frac{rT}{2\kappa} - \frac{1}{2}\delta} , \quad (59)$$

where the first inequality follows by (55b) and the last inequality follows by (55a) together with $\theta \doteq \rho^{\frac{1}{2} - \frac{rT}{2\kappa}}$ and as $u > 0$ is fixed (independent of ρ). Further,

$$\sigma_i(\boldsymbol{M}) = \theta\sigma_i((\boldsymbol{I}_T \otimes \boldsymbol{H})\boldsymbol{G}) \leq \theta\Gamma\sigma_{\iota_T(i)}(\boldsymbol{H})$$

where $\Gamma \triangleq \sigma_{\max}(\boldsymbol{G}) = \sigma_\kappa(\boldsymbol{G})$, and it follows from (55a) that

$$\sigma_i(\boldsymbol{M}) \dot{\leq} \rho^{\frac{1}{2} - \frac{rT}{2\kappa} - \frac{1}{2}\alpha_{\iota_T(i)}^\star + \delta} \qquad (60)$$

for $i = 1, \dots, qT$. As $\alpha_i^\star > 0$ for $i = 1, \dots, q$, it follows by comparing (59) and (60) that $\sigma_i(\boldsymbol{M}) \leq \sigma_1(\boldsymbol{M}_1)$ for $i = 1, \dots, qT$, given that δ is sufficiently small and that ρ is sufficiently large, making Lemma 3 applicable for $k = qT$.

For the maximal singular value of $\boldsymbol{M}$ we have (cf. (59))

$$\sigma_\kappa(\boldsymbol{M}) \dot{\leq} \rho^{\frac{1}{2} - \frac{rT}{2\kappa} - \frac{1}{2}\alpha_{n_{\mathrm{T}}}} \leq \rho^{\frac{1}{2} - \frac{rT}{2\kappa}}$$

where the last inequality follows as $\alpha_{n_{\mathrm{T}}} > 0$. Combined with (59) it follows that

$$\left[\frac{\sigma_\kappa(\boldsymbol{M})}{\sigma_1(\boldsymbol{M}_1)} + 1\right] \dot{\leq} \rho^{\frac{1}{2}\delta} ,$$

and from (58) and (60) that

$$\sigma_i(\boldsymbol{R}_k) \dot{\leq} \rho^{\frac{1}{2} - \frac{rT}{2\kappa} - \frac{1}{2}\alpha_{\iota_T(i)}^\star + \frac{3}{2}\delta}$$

for $i = 1, \dots, qT$. Consequently (cf. (27)),

$$\frac{2\xi}{\sqrt{2k}\sigma_i(\boldsymbol{R}_k)} \dot{\geq} \rho^{\frac{rT}{2\kappa} + \frac{1}{2}\alpha_{\iota_T(i)}^\star - \frac{1}{2} - \frac{3}{2}\delta} , \qquad (61)$$

given that δ is sufficiently small. Further, as

$$\frac{rT}{2\kappa} + \frac{1}{2}\alpha_{\iota_{2T}(i)}^\star - \frac{1}{2} = \frac{1}{2}\left(\frac{r}{n_{\mathrm{T}}} - 1 + \alpha_{\iota_T(i)}^\star\right) > 0$$

for $i = 1, \dots, k$ where $k = 2qT$ by the condition for q in (54), it follows that the lower bound in (61) tends to infinity with increasing ρ provided that δ is small, and we may conclude that

$$\left[\frac{2\xi}{\sqrt{2k}\sigma_i(\boldsymbol{R}_k)} - \sqrt{2k}\right]^2 \dot{\geq} \rho^{\frac{rT}{\kappa} + \alpha_{\iota_T(i)}^\star - 1 - 3\delta} > 0 \qquad (62)$$

where the last inequality holds, again, provided δ is small.

Combining (27) in Lemma 1 and (62), and making the real valued expansion as we did for Theorem 2, yields a lower bound on the number of nodes visited by the sphere decoder in layer $k = qT$ given by

$$N_k \geq \prod_{i=1}^{k} \rho^{\frac{rT}{\kappa} + \alpha_{\iota_T(i)}^\star - 1 - 3\delta} = \rho^{\upsilon - 3k\delta} \qquad (63)$$

where

$$v \triangleq \sum_{i=1}^{k} \frac{rT}{\kappa} + \alpha_{\iota_T(i)}^{\star} - 1$$

$$= \sum_{i=1}^{q} T\left(\frac{r}{n_T} + \alpha_i^{\star} - 1\right). \tag{64}$$

By noting that

$$0 \leq \frac{r}{n_T} + \alpha_i^{\star} - 1 \leq \frac{r}{n_T}$$

for $i = 1, \ldots, q$ by the assumption that $\alpha_i^{\star} \leq 0$ and the definition of q, it follows that

$$T\left(\frac{r}{n_T} + \alpha_i^{\star} - 1\right) = T \min\left(\frac{r}{n_T} - 1 + \alpha_i^{\star}, \frac{r}{n_T}\right)^{+} \tag{65}$$

for $i = 1, \ldots, q$. Further, as

$$\frac{r}{n_T} + \alpha_i^{\star} - 1 \leq 0$$

for $i > q$, also by the definition of q, the right hand side of (65) is equal to 0 for $i > q$. Thus, it follows that

$$v = \sum_{i=1}^{n_T} T \min\left(\frac{r}{n_T} - 1 + \alpha_i^{\star}, \frac{r}{n_T}\right)^{+} = \bar{c}(r)$$

where the last equality follows due to the optimality of $\alpha^{\star}$ in (45), and we then obtain from (63) that

$$N \geq N_k \geq \rho^{\bar{c}(r) - 3k\delta},$$

given that ρ is sufficiently large and that $\delta > 0$ is small. However, as $\delta > 0$ can be chosen arbitrarily small it is concluded that (55) represents sufficient conditions under which the number of nodes visited is arbitrarily close to the upper bound of $\rho^{\bar{c}(r)}$ given by Theorem 2.

C. Probabilities

We now turn to the probability that the conditions imposed by (55) are simultaneously satisfied. The events in (55) are independent[8]. As (55) imply $N \geq \rho^{\bar{c}(r) - \frac{3}{2}k\delta}$ it follows that

$$P\left(N \geq \rho^{\bar{c}(r) - 3k\delta}\right) \geq \prod_{i=1}^{4} P\left(\Omega_i\right),$$

given that ρ is sufficiently large.

The assumption made in Lemma 2, i.e., condition (48), guarantees that

$$\sigma_1((\boldsymbol{I} \otimes \boldsymbol{U}_p^{H})\boldsymbol{G}_{|p}) > 0$$

for some $\boldsymbol{U}_p$. However, by the continuity of singular values [21] it follows for sufficiently small $u > 0$ (cf. (55b)) that $P(\Omega_2) > 0$, which implies $P(\Omega_2) \doteq \rho^0$ as Ω_2 is independent of ρ. The same is true for Ω_3, i.e., $P(\Omega_3) \doteq \rho^0$. It may also

be shown that $P(\Omega_4)$ converges to a strictly positive limit[9] and that therefore $P(\Omega_4) \doteq \rho^0$. It follows that

$$P(N \geq \rho^{\bar{c}(r) - 3k\delta}) \stackrel{.}{\geq} P(\Omega_1).$$

The probability of Ω_1 may again be assessed by using large deviation techniques as in [5]. In particular, it is noted that the condition imposed by Ω_1 (cf. (55a)) specifies an open set of admissible $\boldsymbol{\alpha}$. Applying (38) and (40) yields

$$-\lim_{\rho \to \infty} \frac{\log P(\Omega_1)}{\log \rho} \leq \sum_{i=1}^{q} (n_R - n_T + 2i - 1)(\alpha_i^{\star} - 2\delta)$$

$$\leq d(r) - 2(n_R - n_T + q)q\delta < d(r), \tag{66}$$

where the second inequality follows from (45b) and the feasibility of $\boldsymbol{\alpha}^{\star}$, and where $d(r)$ is the diversity of the code. Thus,

$$-\lim_{\rho \to \infty} \frac{\log P(N \geq \rho^{\bar{c}(r) - 3k\delta})}{\log \rho} < d(r). \tag{67}$$

By the definition of the complexity exponent $c(r)$ (cf. (21)) it follows by (67) that $c(r) \geq \bar{c}(r) - 3k\delta$. As the bound holds for arbitrarily small $\delta > 0$, it follows that $c(r) = \bar{c}(r)$, establishing the tightness of (45) and Lemma 2.

D. The extension to adaptive radius updates

The derivation above make the assumption that the search radius ξ is a non-random function of ρ that satisfies $\xi \doteq \rho^0$. It is thus natural to ask if the SD complexity exponent could be potentially be improved by choosing ξ adaptively based on the problem data $\boldsymbol{H}$ and $\boldsymbol{Y}$, as is done when using, e.g., the Schnorr-Euchner SD algorithm implementation [2], [3]. However, we shall end this appendix by arguing that it can not, and therefore that the assumption of a non-adaptive radius is made without loss of generality. The argument is similar to the one in [10].

The reason that adaptively choosing ξ cannot reduce the complexity exponent is that even if ξ is adaptively chosen, it cannot be chosen smaller than the distance to the closest codeword, i.e., the (square root of the) minimum metric in (13), if we wish find any codewords in the search. As was already argued in Section III-B, the distance to the *transmitted* codeword is always $\|\boldsymbol{Q}^{H}\boldsymbol{w}\|$ and $P(\|\boldsymbol{Q}^{H}\boldsymbol{w}\| \geq \epsilon)$ can be made arbitrarily close to one by appropriately choosing $\epsilon > 0$. Consequently, whenever the transmitted codeword $\boldsymbol{s}$ is the ML decision, i.e., yields the minimum metric in (13), we could use $\xi \geq \epsilon$ where $\epsilon \doteq \rho^0$ as an (arbitrarily likely) probabilistic lower bound on an adaptive search radius ξ in the proof of the lower bounds on the complexity (e.g., in (62)) and obtain the same SNR exponents in these bounds.

Thus, to complete the argument we must only rule out the possibility that the probability that $\boldsymbol{s}$ yields the minimum metric in (13) under the conditions of Ω imposed in (55) is small, as the lower bound is derived explicitly under Ω. To this

---

[8]The independence of Ω_1 and Ω_2 follows by the i.i.d. Rayleigh assumption on $\boldsymbol{H}$, which make the eigenvalues and eigenvectors of $\boldsymbol{H}^{H}\boldsymbol{H}$ independent [38].

[9]This is provided that $r > 0$ in which case the the subset of the constellation defined by Ω_4 contains an asymptotically deterministic and strictly positive fraction of the full constellation, cf. the proof of Lemma 1 in [8]. When $r = 0$ the statement that $\bar{c}(r)$ is tight is trivial as $\bar{c}(0) = 0$.

end, assume that it is false, i.e., that $\mathrm{P}(\boldsymbol{s}_{\mathrm{ML}} \neq \boldsymbol{s}|\Omega) \geq \epsilon$ for any (fixed and SNR independent) $\epsilon > 0$. In this case we could lower bound the probability of the ML decoder according to (cf. 66)

$$\mathrm{P}(\boldsymbol{s}_{\mathrm{ML}} \neq \boldsymbol{s}) \geq \mathrm{P}(\boldsymbol{s}_{\mathrm{ML}} \neq \boldsymbol{s}|\Omega)\mathrm{P}(\Omega) \geq \epsilon\mathrm{P}(\Omega) \dot{>} \rho^{-d(r)},$$

which would violate the definition of $d(r)$ as the diversity order of the ML decoder. Consequently, at sufficiently high SNR it must hold that $\mathrm{P}(\boldsymbol{s}_{\mathrm{ML}} = \boldsymbol{s}|\Omega) \geq 1 - \epsilon$ for any $\epsilon > 0$. We can thus choose $\epsilon > 0$ such that, under Ω, it follows that $\boldsymbol{s}_{\mathrm{ML}} = \boldsymbol{s}$ and $\|\boldsymbol{Q}^{\mathrm{H}}\boldsymbol{w}\| \geq \epsilon$ with arbitrary high probability, implying that $\xi_{\mathrm{ML}} > \epsilon$ where ξ_{ML}^2 is the minimum metric in (13). In other words, there is some $\epsilon > 0$ for which

$$\mathrm{P}(\Omega \cup \{\xi_{\mathrm{ML}} \geq \epsilon\}) \dot{>} \rho^{-d(r)}.$$

Completing the proof of Lemma 2 with $\epsilon \doteq \rho^0$ in place of ξ (as $\xi \geq \xi_{\mathrm{ML}} \geq \epsilon$ throughout the search) proves that $c(r) = \bar{c}(r)$ under (48) also if we allow for SD implementations that adaptively update choose and update the search radius ξ. Finally, it should be noted that what is shown here is not that adaptively choosing the search radius cannot reduce complexity – it does – but only that this reduction is not significant enough to reduce the complexity exponent.

APPENDIX C
PROOF OF LEMMA 3

Consider the matrix, $\underline{\boldsymbol{A}}$, given by

$$\underline{\boldsymbol{A}} \triangleq \boldsymbol{U}\underline{\boldsymbol{\Sigma}}\boldsymbol{V}^{\mathrm{H}},$$

where $\underline{\boldsymbol{\Sigma}} = \mathrm{Diag}(0, \ldots, 0, \sigma_{i+1}(\boldsymbol{A}), \ldots, \sigma_n(\boldsymbol{A}))$, and where $\boldsymbol{U}$ and $\boldsymbol{V}$ denote the right and left singular vector of $\boldsymbol{A}$ respectively. Partition $\underline{\boldsymbol{A}} \in \mathbb{C}^{m \times n}$ according to

$$\underline{\boldsymbol{A}} = \begin{bmatrix} \underline{\boldsymbol{A}}_1 & \underline{\boldsymbol{A}}_2 \end{bmatrix}$$

where $\underline{\boldsymbol{A}}_1 \in \mathbb{C}^{m \times n-k}$ and $\underline{\boldsymbol{A}}_2 \in \mathbb{C}^{m \times k}$.

By the nature of the QR decomposition, it holds that

$$\boldsymbol{P} \triangleq \boldsymbol{\Pi}_{\boldsymbol{A}_1}^{\perp}\boldsymbol{A}_2 = \boldsymbol{Q}_2\boldsymbol{R}_{22}$$

where $\boldsymbol{\Pi}_{\boldsymbol{A}_1}^{\perp}$ denotes the projection onto the orthogonal complement of the range of $\boldsymbol{A}_1$ (i.e. the nullspace of $\boldsymbol{A}_1^{\mathrm{H}}$). Additionally, let

$$\underline{\boldsymbol{P}} \triangleq \boldsymbol{\Pi}_{\underline{\boldsymbol{A}}_1}^{\perp}\underline{\boldsymbol{A}}_2.$$

As $\boldsymbol{Q}_2$ is a unitary matrix it follows that

$$\sigma_i(\boldsymbol{R}_{22}) = \sigma_i(\boldsymbol{P}).$$

In what follows, we will consider the singular values of $\boldsymbol{P}$ in order to establish the lemma. To this end, we will make use of two results due to Weyl and Stewart. For a modern proof of Theorem 8, see e.g. [21, Corollary 7.3.8]. The statement in Theorem 9 follows by combining [39, Theorem 2.3] and [39, Theorem 2.4]. In the following, $\|\boldsymbol{B}\| = \sigma_{\max}(\boldsymbol{B})$ denotes the spectral matrix norm.

Theorem 8 (Weyl): For arbitrary $\boldsymbol{B}, \boldsymbol{C} \in \mathbb{C}^{p \times q}$ it holds that

$$|\sigma_i(\boldsymbol{B}) - \sigma_i(\boldsymbol{C})| \leq \|\boldsymbol{B} - \boldsymbol{C}\|. \tag{68}$$

Theorem 9 (Stewart): For $\boldsymbol{B}, \boldsymbol{C} \in \mathbb{C}^{p \times q}$ such that $\mathrm{rank}(\boldsymbol{B}) = \mathrm{rank}(\boldsymbol{C})$,

$$\|\boldsymbol{\Pi}_{\boldsymbol{B}}^{\perp} - \boldsymbol{\Pi}_{\boldsymbol{C}}^{\perp}\| \leq \min(\|\boldsymbol{B}^{\dagger}\|, \|\boldsymbol{C}^{\dagger}\|)\|\boldsymbol{B} - \boldsymbol{C}\|, \tag{69}$$

where $(\cdot)^{\dagger}$ denotes the Moore-Penrose pseudo inverse [21].

By noting that

$$\|\boldsymbol{A}_l - \underline{\boldsymbol{A}}_l\| \leq \|\boldsymbol{A} - \underline{\boldsymbol{A}}\| = \sigma_i(\boldsymbol{A}), \tag{70}$$

for $l = 1, 2$ and using the assumption that $\sigma_1(\boldsymbol{A}_1) > \sigma_i(\boldsymbol{A})$ it follows by Theorem 8 that

$$\sigma_1(\underline{\boldsymbol{A}}_1) \geq \sigma_1(\boldsymbol{A}_1) - \|\boldsymbol{A}_1 - \underline{\boldsymbol{A}}_1\| \geq \sigma_1(\boldsymbol{A}_1) - \sigma_i(\boldsymbol{A}) > 0$$

implying that $\underline{\boldsymbol{A}}_1$ is full rank. As $\sigma_1(\boldsymbol{A}_1) > 0$ is directly implied by $\sigma_1(\boldsymbol{A}_1) > \sigma_i(\boldsymbol{A})$ it follows that $\mathrm{rank}(\underline{\boldsymbol{A}}_1) = \mathrm{rank}(\boldsymbol{A}_1)$ which makes Theorem 9 applicable to $\boldsymbol{\Pi}_{\boldsymbol{A}_1}^{\perp} - \boldsymbol{\Pi}_{\underline{\boldsymbol{A}}_1}^{\perp}$. As

$$\boldsymbol{P} - \underline{\boldsymbol{P}} = \boldsymbol{\Pi}_{\boldsymbol{A}_1}^{\perp}\boldsymbol{A}_2 - \boldsymbol{\Pi}_{\underline{\boldsymbol{A}}_1}^{\perp}\underline{\boldsymbol{A}}_2$$
$$= (\boldsymbol{\Pi}_{\boldsymbol{A}_1}^{\perp} - \boldsymbol{\Pi}_{\underline{\boldsymbol{A}}_1}^{\perp})\underline{\boldsymbol{A}}_2 + \boldsymbol{\Pi}_{\boldsymbol{A}_1}^{\perp}(\boldsymbol{A}_2 - \underline{\boldsymbol{A}}_2)$$

it follows that

$$\|\boldsymbol{P} - \underline{\boldsymbol{P}}\| \leq \|\boldsymbol{A}_1^{\dagger}\|\|\boldsymbol{A}_1 - \underline{\boldsymbol{A}}_1\|\|\underline{\boldsymbol{A}}_2\| + \|\boldsymbol{A}_2 - \underline{\boldsymbol{A}}_2\|,$$

where we used Theorem 9 and the fact that $\|\boldsymbol{BC}\| \leq \|\boldsymbol{B}\|\|\boldsymbol{C}\|$ and $\|\boldsymbol{\Pi}_{\boldsymbol{B}}^{\perp}\| \leq 1$ [21]. By noting that $\|\boldsymbol{A}_1^{\dagger}\| = 1/\sigma_1(\boldsymbol{A}_1)$, that $\|\underline{\boldsymbol{A}}_2\| \leq \|\underline{\boldsymbol{A}}\| = \sigma_n(\boldsymbol{A})$, that $\|\boldsymbol{A}_1 - \underline{\boldsymbol{A}}_1\| \leq \sigma_i(\boldsymbol{A})$ and that $\|\boldsymbol{A}_2 - \underline{\boldsymbol{A}}_2\| \leq \sigma_i(\boldsymbol{A})$ (cf. (70)), it follows that

$$\mu \triangleq \left[\frac{\sigma_n(\boldsymbol{A})}{\sigma_1(\boldsymbol{A}_1)} + 1\right]\sigma_i(\boldsymbol{A}) \geq \|\boldsymbol{P} - \underline{\boldsymbol{P}}\|. \tag{71}$$

By again applying Theorem 8 to (71) it follows that $\sigma_i(\boldsymbol{P}) \leq \sigma_i(\underline{\boldsymbol{P}}) + \mu$. Note however that

$$\mathrm{rank}(\underline{\boldsymbol{A}}) = \mathrm{rank}(\underline{\boldsymbol{A}}_1) + \mathrm{rank}(\underline{\boldsymbol{P}})$$

where $\underline{\boldsymbol{P}} \triangleq \boldsymbol{\Pi}_{\underline{\boldsymbol{A}}_1}^{\perp}\underline{\boldsymbol{A}}_2 \in \mathbb{C}^{m \times k}$. As $\mathrm{rank}(\underline{\boldsymbol{A}}_1) = n - k$ and $\mathrm{rank}(\underline{\boldsymbol{A}}) \leq n - i$ it follows that

$$\mathrm{rank}(\underline{\boldsymbol{P}}) \leq k - i$$

and $\sigma_i(\underline{\boldsymbol{P}}) = 0$. Thus, $\sigma_i(\boldsymbol{R}_{22}) = \sigma_i(\boldsymbol{P}) \leq \mu$ establishing the lemma.

APPENDIX D
PROOF OF THEOREM 7

Let $\mathcal{X}$ be the un-normalized extended codebook corresponding to the un-normalized lattice points $\boldsymbol{G}\mathbb{S}_{\infty}$, i.e., where $\mathcal{X} \subseteq \theta\underline{\mathcal{X}}$. A space-time code is said to satisfy the non-vanishing determinant (NVD) condition if (cf. [24])

$$\inf_{\underline{\boldsymbol{X}} \in \underline{\mathcal{X}} \backslash \mathbf{0}} |\underline{\boldsymbol{X}}| > 0, \tag{72}$$

i.e., if there are non-zero un-normalized codewords with arbitrarily small determinants. The proof of the theorem draws from the well known fact that the NVD condition is a necessary condition for achieving approximate universality, and divides the problem into a few (exhaustive) cases where either the condition in Lemma 2 is shown to hold, or the NVD property is shown to be violated, thus eliminating the possibility of NVD codes that would violate the rank condition

in Lemma 2. To this end, consider a partitioning of the 4×4 generator matrix according to

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{G}_{11} & \boldsymbol{G}_{12} \\ \boldsymbol{G}_{21} & \boldsymbol{G}_{22} \end{bmatrix}$$

where $\boldsymbol{G}_{ij} \in \mathbb{C}^{2 \times 2}$. First of all, let us note that the case where $p = 2$ is trivially satisfied as $\boldsymbol{G}$ is full rank, i.e., the matrix

$$(\boldsymbol{I}_2 \otimes \boldsymbol{U}_2^{\mathrm{H}}) \boldsymbol{G}$$

is full rank for any unitary $\boldsymbol{U}_2 \in \mathbb{C}^{2 \times 2}$. We can thus restrict attention to the case of $p = 1$ and consider the rank of

$$(\boldsymbol{I}_2 \otimes \boldsymbol{u}^{\mathrm{H}}) \boldsymbol{G}_{|1} = \begin{bmatrix} \boldsymbol{u}^{\mathrm{H}} \boldsymbol{G}_{11} \\ \boldsymbol{u}^{\mathrm{H}} \boldsymbol{G}_{21} \end{bmatrix} \in \mathbb{C}^{2 \times 2} \qquad (73)$$

where $\boldsymbol{u} = \boldsymbol{U}_1 \in \mathbb{C}^{2 \times 1}$. In the cases where the NVD property is shown to not hold, it is sufficient to consider non-zero (unnormalized) codewords of the form

$$\underline{\boldsymbol{x}} = \begin{bmatrix} \boldsymbol{G}_{11} & \boldsymbol{G}_{12} \\ \boldsymbol{G}_{21} & \boldsymbol{G}_{22} \end{bmatrix} \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \end{bmatrix}$$

where $\boldsymbol{s}_1 \in \mathbb{S}_{\infty}^2$, and $\boldsymbol{s}_1 \neq 0$, and where $\boldsymbol{s}_2 = 0$. The (un-normalized) codewords in matrix form are in this case given by $\underline{\boldsymbol{X}} = [\boldsymbol{G}_{11}\boldsymbol{s}_1 \ \boldsymbol{G}_{21}\boldsymbol{s}_1]$ and we have $\boldsymbol{u}^{\mathrm{H}}\underline{\boldsymbol{X}} = [\boldsymbol{u}^{\mathrm{H}}\boldsymbol{G}_{11}\boldsymbol{s}_1 \ \boldsymbol{u}^{\mathrm{H}}\boldsymbol{G}_{21}\boldsymbol{s}_1]$. All codewords discussed in what follows are assumed to have this structure.

We will now consider different cases depending on the rank of $\boldsymbol{G}_{11}$ and $\boldsymbol{G}_{21}$. However, as it is straightforward to see that $\underline{\boldsymbol{X}}$ has zero determinant (for any $\boldsymbol{s}_1$) if either $\boldsymbol{G}_{11} = 0$ or $\boldsymbol{G}_{21} = 0$, the cases that need consideration are those when the rank of both $\boldsymbol{G}_{11}$ and $\boldsymbol{G}_{21}$ is equal to one (case a), when the rank of both $\boldsymbol{G}_{11}$ and $\boldsymbol{G}_{21}$ is equal to two (case b), and when the rank or either $\boldsymbol{G}_{11}$ or $\boldsymbol{G}_{21}$ is equal to one and the rank of the other is equal to two (case c).

A. Case a

Consider the case where the rank of both $\boldsymbol{G}_{11}$ and $\boldsymbol{G}_{21}$ is one, i.e., where $\boldsymbol{G}_{11} = \boldsymbol{b}_1 \boldsymbol{a}_1^{\mathrm{H}}$ and $\boldsymbol{G}_{21} = \boldsymbol{b}_2 \boldsymbol{a}_2^{\mathrm{H}}$. If $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ are not linearly dependent, the condition in (73) is satisfied for any $\boldsymbol{u}$ such that $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{b}_1 \neq 0$ and $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{b}_2 \neq 0$, and we can thus restrict attention to the case where $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ are linearly dependent. Here, we may without loss of generality assume that $\boldsymbol{a}_1 = \boldsymbol{a}_2 = \boldsymbol{a}$ by absorbing any complex scalars into $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$.

Note however that given any $\epsilon > 0$ we can always find a point $\boldsymbol{s}_1 \in \mathbb{S}_{\infty}^2$, where $\boldsymbol{s}_1 \neq 0$ such that[10] $\|\boldsymbol{a}^{\mathrm{H}}\boldsymbol{s}_1\|^2 < \epsilon$. For any such $\boldsymbol{s}_1$ it follows that (cf. [21, Theorem 7.3.10])

$$\sigma_{\max}^2(\underline{\boldsymbol{X}}) = \max_{\boldsymbol{u} \in \mathbb{C}^2 : \|\boldsymbol{u}\| = 1} \|\boldsymbol{u}^{\mathrm{H}}\underline{\boldsymbol{X}}\|^2 \leq (\|\boldsymbol{b}_1\|^2 + \|\boldsymbol{b}_2\|^2)\epsilon \,,$$

i.e., the maximal singular value of $\underline{\boldsymbol{X}}$ can be made arbitrarily small. However, this violates the assumed NVD property of the code as a small maximal singular value implies a small determinant, and concludes case a.

[10] Since $\boldsymbol{a}^{\mathrm{H}} \mathbb{S}_{\infty}^2$ is the projection of the two dimensional Gaussian integer lattice onto a one dimensional space, one can also view the statement as an application of Dirichlet's box principle, cf. [7]. In general, the problem of finding non-zero integer vectors that are approximately orthogonal to a given vector is known as approximate integer relations (IRs), and is related to simultaneous Diophantine approximations [40].

B. Case b

When $\boldsymbol{G}_{11}$ and $\boldsymbol{G}_{21}$ are full rank we can always find a vector $\boldsymbol{u}$ such that $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{G}_{11}$ and $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{G}_{21}$ are linearly independent (thus satisfying the condition of Lemma 2) unless $\boldsymbol{G}_{11}$ and $\boldsymbol{G}_{21}$ are linearly dependent, i.e., when $\boldsymbol{G}_{11} = a\boldsymbol{G}_{21}$ for some $a \in \mathbb{C}$. However, in this case we have that $\boldsymbol{G}_{11}\boldsymbol{s}_1 = a\boldsymbol{G}_{21}\boldsymbol{s}_1$ for any $\boldsymbol{s}_1$ which implies that the columns of $\underline{\boldsymbol{X}}$ are linearly dependent, and the rank of $\underline{\boldsymbol{X}}$ is zero. This concludes case b.

C. Case c

In this case we may assume that $\boldsymbol{G}_{11} = \boldsymbol{b}_1 \boldsymbol{a}_1^{\mathrm{H}}$ has rank one and $\boldsymbol{G}_{21}$ has rank two (the opposite case is handled equivalently). Here, as both the set of $\boldsymbol{u}$ for which $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{b}_1 = 0$ and where $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{G}_{21}$ is linearly dependent of $\boldsymbol{a}_1^{\mathrm{H}}$ have zero measure, we may pick $\boldsymbol{u}$ such that $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{b}_1 \neq 0$ and such that $\boldsymbol{u}^{\mathrm{H}}\boldsymbol{G}_{21}$ is linearly independent of $\boldsymbol{a}_1^{\mathrm{H}}$, thus satisfying the conditions of Lemma 2. Actually, case c is not that interesting in the first place as one can easily show that in this case the code cannot satisfy the NVD condition either. Anyhow, this concludes the proof of Theorem 7.

REFERENCES

[1] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1639–1642, July 1999.

[2] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.

[3] M. O. Damen, H. E. Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2389–2401, Oct. 2003.

[4] A. D. Murugan, H. E. Gamal, M. O. Damen, and G. Caire, "A unified framework for tree search decoding: rediscovering the sequential decoder," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 933– 953, Mar. 2006.

[5] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[6] K. Kumar, G. Caire, and A. Moustakas, "Asymptotic performance of linear receivers in mimo fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4398–4418, October 2009.

[7] M. Taherzadeh and A. K. Khandani, "On the limitations of the naive lattice decoding," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 4820–4826, October 2010.

[8] J. Jaldén and P. Elia, "DMT optimality of LR-aided linear decoders for a general class of channels, lattice designs, and system models," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 4765–4780, October 2010.

[9] J. Jaldén and B. Ottersten, "On the complexity of sphere decoding in digital communications," *IEEE Trans. Signal Processing*, vol. 53, no. 4, pp. 1474–1484, Apr. 2005.

[10] J. Jaldén and B. Ottersten, "On the limits of sphere decoding," in *Proc. IEEE International Syposium on Information Theory*, Adelaide, Australia, September 2005, pp. 1691–1695.

[11] D. Seethaler, J. Jalden, C. Studer, and H. Bolcskei, "Tail behavior of sphere-decoding complexity in random lattices," in *Proc. IEEE International Symposium on Information Theory, ISIT*, June 2009, pp. 729 – 733.

[12] H. Yao and G. W. Wornell, "Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay," San Francisco, CA, Dec. 2003.

[13] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The golden code: A 2 x 2 full-rate space-time code with non-vanishing determinants," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1432–1436, Apr. 2005.

[14] T. Kiran and B. Sundar Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2984–2992, Aug. 2005.

[15] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 3869–3884, September 2006.

[16] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3885–3902, Sept. 2006.

[17] P. Elia, B. A. Sethuraman, and P. Vijay Kumar, "Perfect space-time codes for any number of transmit antennas," *IEEE Trans. Inform. Theory*, vol. 53, no. 11, pp. 3853–3868, Nov. 2007.

[18] B. Hassibi and H. Vikalo, "On the sphere-decoding algorithm I. expected complexity," *IEEE Trans. Signal Processing*, vol. 53, no. 8, pp. 2806–2818, Aug. 2005.

[19] ——, "On the sphere-decoding algorithm II. generalizations, second-order statistics, and applications to communications," *IEEE Trans. Signal Processing*, vol. 53, no. 8, pp. 2819–2834, Aug. 2005.

[20] W. Abediseid and M. Damen, "Lattice sequential decoder for coded MIMO channel: Performance and complexity analysis," Jan. 2011, submitted to the IEEE Trans. on Information Theory. Available as arXiv:1101.0339v1.

[21] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1985.

[22] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 1804–1824, July 2002.

[23] H. El Gamal, G. Caire, and M. O. Damen, "Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of MIMO channels," *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 968–985, June 2004.

[24] F. Oggier, J.-C. Belfiore, and E. Viterbo, "Cyclic division algebras: A tool for space-time coding," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 1, pp. 1–95, 2007.

[25] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*. Cambridge University Press, 1991.

[26] E. Krätzel, *Lattice Points*. Berlin: Kluwer Academic Publishers, 1988.

[27] P. Gritzmann and J. M. Wills, "Lattice points," in *Handbook of Convex Geometry*, P. M. Gruber and J. M. Wills, Eds. North-Holland, 1993, vol. B, ch. 3.2.

[28] A. H. Banihashemi and A. K. Khandani, "On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis," *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 162–171, Jan. 1998.

[29] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed. Springer-Verlag New York Inc., 1998.

[30] H. El Gamal and M. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.

[31] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar, "Full-diversity, high-rate, space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

[32] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. IEEE Information Theory Workshop, ITW*, Paris, France, Mar. 2003.

[33] S. Tavildar and P. Viswanath, "Approximately universal codes over slow-fading channels," *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 3233–3258, July 2006.

[34] O. Tirkkonen and R. Kashaev, "Combined information and performance optimization of linear MIMO modulations," Lausanne, Switzerland, June 2002.

[35] J. Paredes, A. B. Gershman, and M. Gharavi-Alkhansari, "A 2x2 space-time code with non-vanishing determinant and fast maximum likeli-hood decoding," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP*, Honolulu, Hawaii, April 2007, pp. 877–880.

[36] M. Samuel and M. P. Fitz, "Reducing the detection complexity by using 2×2 multi-strata space-time codes," Nice, France, June 2007.

[37] E. Biglieri, Y. Hong, and E. Viterbo, "On fast-decodable space-time block codes," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 524–530, Feb. 2009.

[38] A. Tulino and S. Verdú, "Random matrix theory and wireless communi-cations," *Foundations and Trends in Communications and Information Theory*, vol. 1, no. 1, June 2004.

[39] G. W. Stewart, "On the perturbation of pseudo-inverses, projections and linear least squared problems," *SIAM Review*, vol. 19, no. 4, pp. 634–662, October 1977.

[40] I. Vaughan L. Clarkson, "Approximation of linear forms by lattice points with applications to signal processing," Ph.D. dissertation, The Australian National University, 1997.