A Closed-Form Symbol Error Rate Analysis for Successive Interference Cancellation Decoders

Jinming Wen, Keyu Wu, and Chintha Tellambura

Department of Electrical and Computer Engineering, University of Alberta, Edmonton T6G 2V4, Canada
(e-mail: jinming1@ualberta.ca, keyu2@ualberta.ca, chintha@ece.ualberta.ca)

***Abstract*—Wireless and digital communications applications require the detection of an integer vector $\hat{\boldsymbol{x}}$ from $\boldsymbol{y} = \boldsymbol{A}\hat{\boldsymbol{x}} + \boldsymbol{v}$, where $\boldsymbol{A} \in \mathbb{R}^{m\times n}$ is a random matrix whose entries are independent and identically distributed (i.i.d.) standard Gaussian $\mathcal{N}(0,1)$ entries, and $\boldsymbol{v} \in \mathbb{R}^m$ is a noise vector following the Gaussian distribution $\mathcal{N}(0,\sigma^2)$ with given σ. The successive interference cancellation (SIC) decoders are frequently used to detect $\hat{\boldsymbol{x}}$ due to their high accuracy and low implementation complexity. However, to accurately characterize their performance, we need to analyze their symbol error rates (SER). In this paper, we derive a closed-form expression for the SER of the SIC decoders and investigate its properties. Simulated error probabilities of the SIC decoders agree closely with our theoretical expressions.**

***Index Terms*—Symbol error rate, successive interference cancellation, Babai's nearest plane algorithm, integer least squares problems.**

I. Introduction

In many applications, we need to detect an integer parameter vector $\hat{\boldsymbol{x}} \in \mathbb{Z}^n$ from

$$\boldsymbol{y} = \boldsymbol{A}\hat{\boldsymbol{x}} + \boldsymbol{v}, \quad \boldsymbol{v} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2\boldsymbol{I}), \tag{1}$$

where $\boldsymbol{y} \in \mathbb{R}^m$ is an observation vector, $\boldsymbol{A} \in \mathbb{R}^{m\times n}$ is a random matrix whose entries independent and identically follow the standard Gaussian distribution $\mathcal{N}(0,\boldsymbol{I})$, and $\boldsymbol{v} \in \mathbb{R}^m$ is a noise vector following the Gaussian distribution $\mathcal{N}(\boldsymbol{0},\sigma^2\boldsymbol{I})$ with given σ.

One of the widely used methods to detect $\hat{\boldsymbol{x}}$ in (1) is to solve the following ordinary integer least squares (OILS) problem:

$$\min_{\boldsymbol{x}\in\mathbb{Z}^n} \|\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}\|_2^2, \tag{2}$$

whose solution is the maximum-likelihood estimator of $\hat{\boldsymbol{x}}$. As (2) is equivalent to finding the point in the lattice $\{\boldsymbol{A}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\}$ that is closest to $\boldsymbol{y}$, the OILS problem is also referred to as the closest point problem in cryptography (see, e.g., [1]).

One of the most popular methods to solve (2) in communications is the sphere decoder, which is implemented via the Schnorr-Euchner algorithm [2], which is an improved version of the Fincke-Pohst algorithm [3], or its variants, see e.g. [1], [4]–[8]. Although lattice reductions, such as the Lenstra-Lenstra-Lovász (LLL) reduction [9], can decrease the computational cost of solving (2) by sphere decoding [10], it has been shown in [11] that (2) is an NP-hard problem. Hence, for many applications, a suboptimal algorithm of (2) may be utilized to detect $\hat{\boldsymbol{x}}$ instead of completely solving (2). One frequently used suboptimal algorithms is the ordinary successive interference cancellation (SIC) decoder which is actually the Babai's nearest plane algorithm [12]. The solution obtained by a SIC decoder is also referred to as an ordinary Babai point (e.g., [1], [10]), which is actually the first integer vector found by the Schnorr-Euchner algorithm for solving (2). For more details, see [1], [13].

In order to accurately characterize the performance of a decoder, we utilize the probability of the solution, obtained by the decoder, that is not equal to the true integer vector $\hat{\boldsymbol{x}}$, which is referred to as symbol error rate (SER). The probability of correct detection is referred to as the success probability of the decoder, see, e.g., [10], [14]–[16].

As showed in [10], [15] and [16], the SER characterization of the SIC decoder is very important. Indeed, when using an SIC decoder to detect $\hat{\boldsymbol{x}}$, the SER P_e^{OSIC} serves as an important quality parameter. Specifically, if the SER is sufficiently low, say fairly close to 0, the decoder can be used with confidence. In this case, the additional effort to optimally solve the OILS (2) yields diminishing returns. However, if the P_e^{OSIC} is high, then other more effective decoders, such as the maximum-likelihood estimator, should be used. Even if one intends to solve the OILS (2) to get the maximum-likelihood estimator of $\hat{\boldsymbol{x}}$, it is still of vital importance to compute P_e^{OSIC} since P_e^{OSIC} is often used to approximate its SER. Moreover, generally speaking, the lower the P_e^{OSIC}, the lower the complexity of solving (2) by sphere decoding [10].

Although a closed-form expression for the SER of the ordinary SIC decoder has been given in [10] for deterministic $\boldsymbol{A}$, to the best of our knowledge, the SER has not been derived for the common case where $\boldsymbol{A}$ is a random matrix, which is required in many applications. This paper fills this gap and derives closed-form SER expression for the SIC decoder. Some properties of the SER will also be discussed.

The rest of the paper is organized as follows. In Section II, we introduce the computational details of the ordinary SIC decoder. In Section III, we develop a closed-form expression for the SER of the ordinary SIC decoder and investigate its properties. In Section IV, we provide numerical simulations to illustrate the proposed formula. Finally, the paper is summarized and discussed in Section V.

In this paper, for a vector $\boldsymbol{x}$, we use $\lfloor \boldsymbol{x} \rceil$ to denote its nearest integer vector, i.e., each entry of $\boldsymbol{x}$ is rounded to its nearest integer (if there is a tie, the one with smaller magnitude is chosen), and we use x_i to denote the i-th element of $\boldsymbol{x}$. Let

a_{ij} be the element of matrix $\boldsymbol{A}$ at row i and column j. Let P_e^{OSIC} denote the SER of the ordinary SIC decoders

II. QR Reduction and transformation of the ILS Problems

We briefly introduce the computational details of the ordinary SIC decoder.

Suppose that $\boldsymbol{A}$ in (1) has the following QR factorization

$$\boldsymbol{A} = [\boldsymbol{Q}_1, \boldsymbol{Q}_2] \begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{0} \end{bmatrix}, \tag{3}$$

where $[\underset{n}{\boldsymbol{Q}_1}, \underset{m-n}{\boldsymbol{Q}_2}] \in \mathbb{R}^{m\times m}$ is an orthogonal matrix and $\boldsymbol{R} \in \mathbb{R}^{n\times n}$ is an upper triangular matrix.

Let $\bar{\boldsymbol{y}} = \boldsymbol{Q}_1^T \boldsymbol{y}$ and $\bar{\boldsymbol{v}} = \boldsymbol{Q}_1^T \boldsymbol{v}$. Since $\boldsymbol{v} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2 \boldsymbol{I})$, $\bar{\boldsymbol{v}} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2 \boldsymbol{I})$. By (3), (1) can be transformed to

$$\bar{\boldsymbol{y}} = \boldsymbol{R}\hat{\boldsymbol{x}} + \bar{\boldsymbol{v}}, \quad \bar{\boldsymbol{v}} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2 \boldsymbol{I}). \tag{4}$$

Let $\boldsymbol{x}^{\text{OSIC}} \in \mathbb{Z}^n$ denote the output of the ordinary SIC decoder which is actually the Babai nearest plane algorithm [12], then it can be computed as follows:

$$c_i^{\text{OSIC}} = (\bar{y}_i - \sum_{j=i+1}^{n} r_{ij} x_j^{\text{OSIC}})/r_{ii}, \quad x_i^{\text{OSIC}} = \lfloor c_i^{\text{OSIC}} \rceil, \tag{5}$$

for $i = n, n-1, \ldots, 1$, where $\sum_{n+1}^{n} \cdot = 0$. Clearly, the entries of $\boldsymbol{x}^{\text{OSIC}}$ are determined from the last one to the first one.

III. SER analysis for the ordinary SIC Decoders

In this section, we derive the SER of the ordinary SIC decoder and investigate its properties.

A. SER analysis the ordinary SIC Decoders

This subsection presents a closed-form SER expression P_e^{OSIC} for the SIC decoder.

We begin with the following lemma which derives P_e^{OSIC} for the one dimensional case.

Lemma 1: Suppose that we have the following linear model:

$$\bar{y} = r\hat{x} + \bar{v}, \quad \bar{v} \sim \mathcal{N}(0, \sigma^2), \tag{6}$$

where $\hat{x} \in \mathbb{Z}$ is a fixed unknown parameter number, $\bar{v} \in \mathbb{R}$ is a noise number following the Gaussian distribution $\mathcal{N}(0, \sigma^2)$, and $r^2 > 0$, which is independent with $\bar{v}$, follows the chi-square distribution with degree k. Let $x = \lfloor \bar{y}/r \rceil$, then

$$\Pr(x = \hat{x}) = C_k \int_0^{\arctan(1/(2\sigma))} \cos^{k-1}(\theta) d\theta, \tag{7}$$

where

$$C_k = \frac{2\Gamma((k+1)/2)}{\sqrt{\pi}\Gamma(k/2)}. \tag{8}$$

Proof: See Appendix A. ∎

Before developing the main theorem to compute P_e^{OSIC}, we need to introduce the following lemma from [17, P. 99].

Lemma 2: Suppose that the entries of $\boldsymbol{A}$ are independent and identically distributed as the standard Gaussian distribution $\mathcal{N}(0,1)$, then all $r_{ij}, 1 \le i \le j \le n$, are independent. Moreover, $r_{ii}^2 \sim \chi_{m-i+1}^2$ and $r_{ij} \sim \mathcal{N}(0,1)$ for $1 \le i \le j \le n$.

Based on Lemmas 1 and 2, the following theorem for P_e^{OSIC} can be obtained.

Theorem 1: The symbol error rate P_e^{OSIC} of the ordinary SIC decoder (see (5)) satisfies

$$P_e^{\text{OSIC}} \equiv \Pr(\boldsymbol{x}^{\text{OSIC}} \neq \hat{\boldsymbol{x}}) = 1 - \prod_{i=m-n+1}^{m} R_i, \tag{9}$$

where

$$R_i = \frac{2}{\sqrt{\pi}} \frac{\Gamma((i+1)/2)}{\Gamma(i/2)} \int_0^{\arctan(1/(2\sigma))} \cos^{i-1}(\theta) d\theta. \tag{10}$$

Similar to the proof of [10, Theorem 1], we first use the chain rule of conditional probabilities to transform $1 - P_e^{\text{OSIC}}$ to the product of n terms with each of them representing a conditional success probability for one dimensional. Then, we use Lemma 1 to compute each term, and finally we obtain (9). For more details, see the following proof.

Proof: Let

$$P_s^{\text{OSIC}} = \Pr(\boldsymbol{x}^{\text{OSIC}} = \hat{\boldsymbol{x}}),$$

then by the chain rule of conditional probabilities, we have

$$P_s^{\text{OSIC}} = \Pr\left(\bigcap_{i=1}^{n} (x_i^{\text{OSIC}} = \hat{x}_i)\right) = \Pr(x_n^{\text{OSIC}} = \hat{x}_n) \times \prod_{i=1}^{n-1} \Pr\left(x_i^{\text{OSIC}} = \hat{x}_i | \bigcap_{j=i+1}^{n} (x_j^{\text{OSIC}} = \hat{x}_j)\right).$$

Thus, by (9) to show the theorem, it suffices to show

$$\Pr(x_n^{\text{OSIC}} = \hat{x}_n) = R_{m-n+1}, \tag{11}$$

$$\Pr\left(x_i^{\text{OSIC}} = \hat{x}_i | \bigcap_{j=i+1}^{n} (x_j^{\text{OSIC}} = \hat{x}_j)\right) = R_{m-i+1}, \tag{12}$$

for $i = n-1, n-2, \ldots, 1$.

By (4), we have

$$\bar{y}_n = r_{nn}\hat{x}_n + \bar{v}_n, \quad \bar{v}_n \sim \mathcal{N}(0, \sigma^2), \tag{13}$$

$$\bar{y}_i - \sum_{j=i+1}^{n} r_{ij}\hat{x}_j = r_{ii}\hat{x}_i + \bar{v}_i, \quad \bar{v}_i \sim \mathcal{N}(0, \sigma^2) \tag{14}$$

for $i = n-1, \ldots, 1$. Moreover, if $x_{i+1}^{\text{OSIC}} = \hat{x}_{i+1}, \cdots, x_n^{\text{OSIC}} = \hat{x}_n$, by (5) and (14), we can see that, for $i = n-1, \ldots, 1$,

$$r_{ii}\, c_i^{\text{OSIC}} = r_{ii}\hat{x}_i + \bar{v}_i, \quad \bar{v}_i \sim \mathcal{N}(0, \sigma^2). \tag{15}$$

By Lemma 2,

$$r_{ii}^2 \sim \chi_{m-i+1}^2, \quad i = n, n-1, \ldots, 1.$$

Thus, by (15) and Lemma 1, we can see that both (11) and (12) hold. Hence, the theorem holds. ∎

Since

$$\prod_{i=m-n+1}^{m} \frac{2}{\sqrt{\pi}} \frac{\Gamma((i+1)/2)}{\Gamma(i/2)} = \left(\frac{2}{\sqrt{\pi}}\right)^n \frac{\Gamma((m+1)/2)}{\Gamma((m-n+1)/2)}. \tag{16}$$

By Theorem 1, we can immediately obtain the following result which computes P_e^{OSIC} in a more efficient way than that by using Theorem 1.

Corollary 1: The symbol error rate P_e^{OSIC} of the ordinary SIC decoder $\boldsymbol{x}^{\text{OSIC}}$ (see (5)) satisfies

$$P_e^{\text{OSIC}} = 1 - \alpha \prod_{i=m-n+1}^{m} \int_0^{\arctan(1/(2\sigma))} \cos^{i-1}(\theta) d\theta,$$

where

$$\alpha = \left(\frac{2}{\sqrt{\pi}}\right)^n \frac{\Gamma((m+1)/2)}{\Gamma((m-n+1)/2)}.$$

B. Properties of the ordinary SIC Decoders

In this subsection, we investigate some properties of P_e^{OSIC}.

We begin with the following important lemma which essentially shows that P_e^{OSIC} tends to 0 if σ tends to 0 for one dimensional case.

Lemma 3: For each fixed integer k, R_k (see (10)) satisfies

$$\lim_{\sigma \to 0} R_k = 1. \tag{17}$$

Proof: See Appendix B. ∎

By Lemma 3, we have the following result.

Theorem 2: The SER P_e^{OSIC} of the OSIC decoder is an increasing function of both σ and n. Moreover it satisfies

$$\lim_{\sigma \to 0} P_e^{\text{OSIC}} = 0. \tag{18}$$

where P_e^{OSIC} is defined in (9).

Proof: By (9) and (10), the first part of the result obviously holds.

By (17), we have

$$\begin{aligned}\lim_{\sigma \to 0} P_e^{\text{OSIC}} =& 1 - \lim_{\sigma \to 0} \prod_{i=m-n+1}^{m} R_i \\ =& 1 - \prod_{i=m-n+1}^{m} \lim_{\sigma \to 0} R_i = 0.\end{aligned}$$

Thus, (18) holds. ∎

Note that, Theorem 2 also holds for deterministic $\boldsymbol{A}$. For more details, see [16, Corollary 2].

In many application domains, the matrix $\boldsymbol{A}$ in (1) is a square matrix. For the convenience of writing, we denote the SER of the ordinary SIC decoder corresponding to the $n \times n$ square matrix $\boldsymbol{A}$ as $P_e^{\text{OSIC}}(n)$, then the following result can be directly obtained from Theorem 1.

Theorem 3: Let $n_1 < n_2$ be two integers, then $P_e^{\text{OSIC}}(n_1)$ and $P_e^{\text{OSIC}}(n_2)$, which are respectively the SER of the ordinary SIC decoders corresponding to $n_1 \times n_1$ and $n_2 \times n_2$ matrices $\boldsymbol{A}$, satisfy

$$\frac{1 - P_e^{\text{OSIC}}(n_2)}{1 - P_e^{\text{OSIC}}(n_1)} = \prod_{k=n_1+1}^{n_2} R(k). \tag{19}$$

Note that the significance of Theorem 3 is it quantifies the gap between two P_e^{OSIC}. Specifically, if σ is close to 0, then R_k is close to 1 for any integer k (for more details, see (10) and (17)). As a result, both $P_e^{\text{OSIC}}(n_2)$ and $P_e^{\text{OSIC}}(n_1)$ are close to 0 which implies that their gap is very small even if $n_2 - n_1$ is very large as long as σ is close to 0. This contradicts with the intuition that the gap is very large no matter how small is σ. For more details, see the numerical experiments in Sec. IV.

IV. Numerical Experiments

In this section, we provide simulation results to illustrate the effectiveness of the SER formula (9) by comparing the average theoretical SER and experimental SER over 10^4 samples. For simplicity, we assume $m = n$ in all the following tests (note that we did lots of simulations and found that (9) is always an effective formula for the SER of the ordinary SIC decoder no matter whether $m = n$ or not).

We did the simulations by choosing a range of n and σ. For each fixed n and σ, we randomly generated 10^4 $\boldsymbol{A}$'s whose entries independent and identically follow the standard Gaussian distribution $\mathcal{N}(0,1)$ and $\boldsymbol{v}$'s with each of them following the Gaussian distribution $\mathcal{N}(\boldsymbol{0}, \sigma^2 \boldsymbol{I})$. To illustrate the effectiveness of (9), we randomly generated only one $\hat{\boldsymbol{x}} \in \mathbb{Z}^n$ corresponding to these 10^4 $\boldsymbol{A}$'s and $\boldsymbol{v}$'s for each fixed n and σ. As a result, we got 10^4 linear models in the form of (1). Then, we found the outputs $\boldsymbol{x}^{\text{OSIC}}$ of the ordinary SIC decoders corresponding to each ordinary linear model according to (5). Finally, we computed the ratio of the number of events $\boldsymbol{x}^{\text{OSIC}} \neq \hat{\boldsymbol{x}}$ to 10^4 as the experimental SER for ordinary SIC decoders which is denoted as "Exp.". To compute the average theoretical SERs, for each generated $\boldsymbol{A}$, we used (9) to compute the theoretical SER of the ordinary SIC decoder, and took their averages which is denoted as "Theo.".

Table I shows the average theoretical and experimental SER of the ordinary SIC decoder for $\sigma = 0.05 : 0.05 : 0.5$ with $n = 4, 8, 64$ over 10^4 samples, and Table II displays the results for $n = 2 : 2 : 20$ with $\sigma = 0.05, 0.1, 0.5$.

TABLE I
AVERAGE THEORETICAL AND EXPERIMENTAL SER OF THE ORDINARY SIC DECODER OVER 10000 SAMPLES

σ	n=4		n=8		n=64	
	Theo.	Exp.	Theo.	Exp.	Theo.	Exp.
0.05	0.0685	0.0680	0.0685	0.0683	0.0685	0.0712
0.10	0.1459	0.1454	0.1460	0.1466	0.1460	0.1496
0.15	0.2300	0.2347	0.2307	0.2317	0.2307	0.2318
0.20	0.3176	0.3272	0.3202	0.3185	0.3202	0.3211
0.25	0.4049	0.4046	0.4113	0.4093	0.4116	0.4102
0.30	0.4883	0.4930	0.5009	0.4986	0.5016	0.4986
0.35	0.5652	0.5637	0.5856	0.5783	0.5874	0.5865
0.40	0.6338	0.6309	0.6627	0.6598	0.6665	0.6711
0.45	0.6934	0.6887	0.7303	0.7343	0.7368	0.7422
0.50	0.7443	0.7432	0.7877	0.7815	0.7974	0.8000

From Tables I-II, one can see that the average theoretical and experimental SER are almost the same, which confirms the effectiveness of the formula (9) from simulation point of view. Note that the small differences between these SERs are due to the fact that there are some differences between the theoretical probability and its realizations.

Tables I-II show that P_e^{OSIC} increases when σ or n increases. Indeed this is true and can be explained with Theorem 2.

TABLE II
AVERAGE THEORETICAL AND EXPERIMENTAL SER OF THE ORDINARY SIC DECODER OVER 10000 SAMPLES

n	$\sigma = 0.05$		$\sigma = 0.10$		$\sigma = 0.50$	
	Theo.	Exp.	Theo.	Exp.	Theo.	Exp.
2	0.0681	0.0660	0.1426	0.1494	0.6464	0.6560
4	0.0685	0.0660	0.1459	0.1464	0.7443	0.7451
6	0.0685	0.0679	0.1460	0.1445	0.7754	0.7805
8	0.0685	0.0660	0.1460	0.1401	0.7877	0.7885
10	0.0685	0.0687	0.1460	0.1444	0.7929	0.7880
12	0.0685	0.0695	0.1460	0.1499	0.7953	0.7927
14	0.0685	0.0730	0.1460	0.1432	0.7964	0.7953
16	0.0685	0.0646	0.1460	0.1445	0.7969	0.8002
18	0.0685	0.0705	0.1460	0.1443	0.7972	0.7895
20	0.0685	0.0658	0.1460	0.1429	0.7973	0.7919

Intuitively, for a fixed σ, P_e^{OSIC} increases significantly if n largely increases. But interestingly, from the Table I, one can see that the gap between $P_e^{\text{OSIC}}(4)$ and $P_e^{\text{OSIC}}(64)$ (i.e., P_e^{OSIC} for $n = 4$ and $n = 64$) is small. Moreover, Table II shows that P_e^{OSIC} seems does not change with n when $\sigma = 0.05$ (note that actually, as showed in Theorem 2, P_e^{OSIC} increases as n increases, but the differences are too small to be seen clearly when $\sigma = 0.05$).

In the following, we use Theorem 3 to explain the above phenomena. To quantify their gaps, we show $\frac{1-P_e^{\text{OSIC}}(64)}{1-P_e^{\text{OSIC}}(4)}$ and $\frac{1-P_e^{\text{OSIC}}(8)}{1-P_e^{\text{OSIC}}(4)}$, which are respectively denoted as "64/4" and "8/4", in Figure 1. From Figure 1, one can see that $\frac{1-P_e^{\text{OSIC}}(64)}{1-P_e^{\text{OSIC}}(4)}$ is around 0.79 even when $\sigma = 0.5$ which means the gap between them is not large.

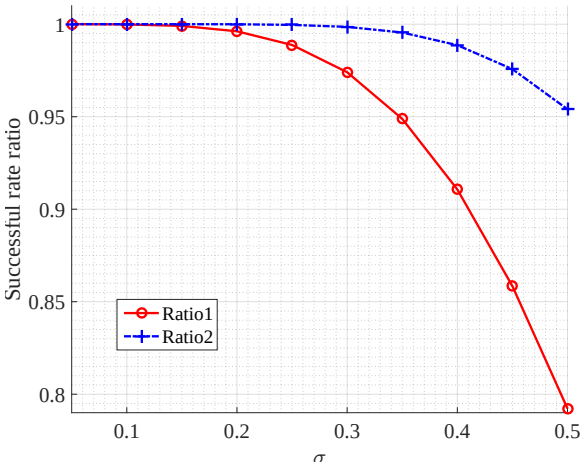

Fig. 1. Success rate ratio for ordinary SIC decoder

We use (19) to explain it. Specifically, we have

$$\frac{1-P_e^{\text{OSIC}}(64)}{1-P_e^{\text{OSIC}}(4)} = \prod_{k=5}^{64} R_k, \quad \frac{1-P_e^{\text{OSIC}}(8)}{1-P_e^{\text{OSIC}}(4)} = \prod_{k=5}^{8} R_k. \quad (20)$$

From Figure 2, one can see that, $R_5 \approx 0.924$ even when $\sigma = 0.5$. Moreover, R_k are very close to 1 when $k > 16$ and $\sigma = 0.5$, and this explains why the gap between $P_e^{\text{OSIC}}(64)$ and

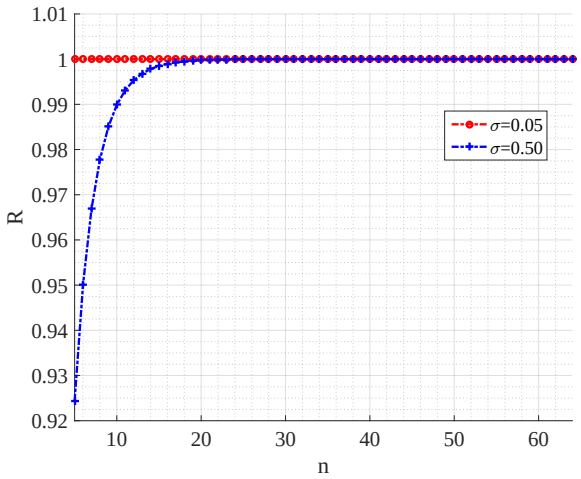

Fig. 2. R_k for ordinary SIC decoder

$P_e^{\text{OSIC}}(4)$ is small even when $\sigma = 0.5$. From Figure 2, one can also see that when $\sigma = 0.05$, R_k are very close to 1 for all integers k, so by (20), $1 - P_e^{\text{OSIC}}(64)$ and $1 - P_e^{\text{OSIC}}(4)$ are very close, and this explains why $P_e^{\text{OSIC}}(64)$ and $P_e^{\text{OSIC}}(4)$ are almost the same when $\sigma = 0.05$.

V. SUMMARY AND DISCUSSIONS

In this paper, we have developed a closed-form expression for computing the SER P_e^{OSIC} of the ordinary SIC decoder, and investigated its properties. Simulation results have also been given to illustrate the proposed formula.

It has been theoretically shown in [10] that the LLL reduction can always decrease (not strictly) P_e^{OSIC}. So it is of vital importance to develop a formula for computing P_e^{OSIC} after the LLL reduction is performed. But to do this, we need to find the distribution of the entries of $\bar{\boldsymbol{R}}$, which is the LLL reduced matrix of $\boldsymbol{R}$ (see (3)). However, to the best of our knowledge, this is still an open problem due to the complication of the process of the LLL reduction.

On the other hand, although the LLL reduction can reduce the integer lattices (i.e., the lattices with their basis vectors being integer vectors) in polynomial time (see [9], [18]), and the average complexity of reducing a matrix $\boldsymbol{A}$ whose entries are independent and identically distributed as the standard normal distribution is also a polynomial of the column rank of $\boldsymbol{A}$ (see [19], [20]), its worst-case complexity is not even finite. Thus, from this point of view, having a closed-form expression for P_e^{OSIC} is of crucial importance. Indeed, if P_e^{OSIC} is already very low, it is not need to spend time to do the LLL reduction to decrease the SER which can save some computation time in practical applications.

APPENDIX A
PROOF OF LEMMA 1

Proof: By (6),

$$x = \lfloor \bar{y}/r \rceil = \lfloor \hat{x} + \bar{v}/r \rceil = \hat{x} + \lfloor \bar{v}/r \rceil,$$

thus, $x = \hat{x}$ if and only if $|\bar{v}/r| \leq 1/2$.

Let $X = \bar{v}^2$, $Y = r^2$, $U = X/Y$ and $V = Y$. Then $x = \hat{x}$ if and only if $U \leq 1/4$. Thus, to show (7), it is equivalent to show:

$$\Pr(U \leq \frac{1}{4}) = C_k \int_0^{\arctan(1/(2\sigma))} \cos^{k-1}(\theta) d\theta, \tag{21}$$

where C_k is defined in (8).

In the following, we find the probability density function (PDF) of U. We first find the PDF of X. Since $X = \bar{v}^2$ and $\bar{v} \sim \mathcal{N}(0, \sigma^2)$, for $x \geq 0$, we have

$$\begin{aligned}\Pr(X \leq x) &= \Pr(-\sqrt{x} \leq \bar{v} \leq \sqrt{x}) \\ &= \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\sqrt{x}}^{\sqrt{x}} \exp\left(-\frac{t^2}{2\sigma^2}\right) dt \\ &= \frac{2}{\sqrt{2\pi\sigma^2}} \int_0^{\sqrt{x}} \exp\left(-\frac{t^2}{2\sigma^2}\right) dt.\end{aligned}$$

Thus,

$$f_X(x) = \frac{d\Pr(X \leq x)}{dx} = \frac{1}{\sqrt{2\pi\sigma^2}} x^{-1/2} \exp\left(-\frac{x}{2\sigma^2}\right).$$

Since $Y = r^2 \sim \chi_k^2$, we obtain

$$f_Y(y) = \frac{1}{2^{k/2}\Gamma(k/2)} y^{k/2-1} \exp\left(-\frac{y}{2}\right).$$

By the fact that X and Y are independent, the joint distribution of (X, Y) is:

$$f_{X,Y}(x, y) = C x^{-1/2} y^{k/2-1} \exp\left(-\frac{x + \sigma^2 y}{2\sigma^2}\right),$$

where

$$C = \frac{1}{\sqrt{2\pi\sigma^2}} \frac{1}{2^{k/2}\Gamma(k/2)}. \tag{22}$$

Since $X = UV$ and $Y = V$,

$$J = \begin{bmatrix} \frac{\partial X}{\partial U} & \frac{\partial X}{\partial V} \\ \frac{\partial Y}{\partial U} & \frac{\partial Y}{\partial V} \end{bmatrix} = \begin{bmatrix} V & U \\ 0 & 1 \end{bmatrix}.$$

Thus, $|\det(J)| = |V| = V$ (note that V is always nonnegative). Therefore, the PDF of the joint distribution of U and V is:

$$f_{U,V}(u, v) = C u^{-1/2} v^{(k-1)/2} \exp\left(-\frac{(u + \sigma^2)v}{2\sigma^2}\right),$$

where C is defined in (22).

By the aforementioned equation, the marginal distribution of U is:

$$\begin{aligned} f_U(u) &= \int_0^\infty f_{U,V}(u, v) dv \\ &\overset{(a)}{=} \frac{C}{\sqrt{u}} \left(\frac{2\sigma^2}{u + \sigma^2}\right)^{(k+1)/2} \int_0^\infty t^{(k-1)/2} \exp(-t) dt \\ &\overset{(b)}{=} \frac{C}{\sqrt{u}} \left(\frac{2}{u/\sigma^2 + 1}\right)^{(k+1)/2} \Gamma((k+1)/2) \\ &= \frac{2^{(k+1)/2}\Gamma((k+1)/2)C}{\sqrt{u}(u/\sigma^2 + 1)^{(k+1)/2}} \\ &\overset{(c)}{=} \frac{C_k}{2\sigma} \frac{1}{\sqrt{u}(u/\sigma^2 + 1)^{(k+1)/2}}, \end{aligned}$$

where (a) follows from the integral transformation with $t = \frac{(u+\sigma^2)v}{2\sigma^2}$, (b) is due to the definition of Gamma function, and (c) is because of (8) and (22).

Therefore, by some fundamental calculations, we obtain

$$\begin{aligned}\Pr(U \leq \frac{1}{4}) &= \int_0^{1/4} f_U(u) du \\ &= \frac{C_k}{2\sigma} \int_0^{1/4} \frac{du}{\sqrt{u}(u/\sigma^2 + 1)^{(k+1)/2}} \\ &= C_k \int_0^{\arctan(1/(2\sigma))} \cos^{k-1}(\theta) d\theta,\end{aligned}$$

where the last equality follows from the integral transformation with $u = \sigma^2 \tan^2(\theta)$. Thus, the lemma holds. ■

APPENDIX B
PROOF OF LEMMA 3

Proof: By (8) and (10), to show (17), it suffices to show

$$\int_0^{\pi/2} \cos^{k-1}(\theta) d\theta = \frac{1}{C_k}, \tag{23}$$

where C_k is defined in (8).

If $k = 1$, then the left-hand side of (23) is $\pi/2$. By direct computation, one can verify that $C_1 = \frac{2\Gamma(1)}{\sqrt{\pi}\Gamma(1/2)} = \frac{2}{\pi}$, thus (23) holds.

If $k = 2$, then the left-hand side of (23) is 1. By direct computation, we have $C_2 = \frac{2\Gamma(3/2)}{\sqrt{\pi}\Gamma(1)} = 1$, thus (23) holds.

In the following, we show (23) holds for $k \geq 3$.

By some basic calculations, one can show that

$$\begin{aligned} &\int_0^{\pi/2} \cos^{k-1}(\theta) d\theta \\ =&\int_0^{\pi/2} \cos^{k-2}(\theta)\cos(\theta) d\theta \\ =&\int_0^{\pi/2} \cos^{k-2}(\theta) d\sin(\theta) \\ =&\cos^{k-2}(\theta)\sin(\theta)\Big|_0^{\pi/2} - \int_0^{\pi/2} \sin(\theta) d\cos^{k-2}(\theta) \\ =&(k-2)\int_0^{\pi/2} \cos^{k-3}(\theta)\sin^2(\theta) d\theta \\ =&(k-2)\int_0^{\pi/2} \cos^{k-3}(\theta)(1 - \cos^2(\theta)) d\theta \\ =&(k-2)\left[\int_0^{\pi/2} \cos^{k-3}(\theta) d\theta - \int_0^{\pi/2} \cos^{k-1}(\theta) d\theta\right]. \end{aligned}$$

Thus,

$$\int_0^{\pi/2} \cos^{k-1}(\theta) d\theta = \frac{k-2}{k-1} \int_0^{\pi/2} \cos^{k-3}(\theta) d\theta. \tag{24}$$

In the following, we prove (23) by considering two difference cases. If k is a even number, then by (24), we have

$$\begin{aligned}&\int_0^{\pi/2}\cos^{k-1}(\theta)d\theta\\=&\frac{(k-2)\dots 2}{(k-1)\dots 3}\int_0^{\pi/2}\cos(\theta)d\theta\\=&\frac{(k-2)\dots 2}{(k-1)\dots 3}=\frac{(k-2)!!}{(k-1)!!}.\end{aligned}$$

Thus, by (8), to show (23) holds for any even number k, it is equivalent to show

$$\frac{\Gamma((k+1)/2)}{\Gamma(k/2)}=\frac{\sqrt{\pi}}{2}\frac{(k-1)!!}{(k-2)!!}. \tag{25}$$

By using the basic fact that $\Gamma(t+1)=t\Gamma(t)$ for any $t>0$, we obtain

$$\begin{aligned}&\frac{\Gamma((k+1)/2)}{\Gamma(k/2)}\\=&\frac{(k-1)/2}{(k-2)/2}\frac{\Gamma((k-1)/2)}{\Gamma((k-2)/2)}\\=&\dots\\=&\frac{(k-1)(k-3)\dots 3}{(k-2)(k-4)\dots 2}\frac{\Gamma(3/2)}{\Gamma(1)}\\=&\frac{(k-1)!!}{(k-2)!!}\frac{\sqrt{\pi}}{2}.\end{aligned}$$

Clearly, (25) holds.

In the following, we show (23) also holds for odd numbers k. Similarly, if k is an odd number, then by (24), we have

$$\begin{aligned}&\int_0^{\pi/2}\cos^{k-1}(\theta)d\theta\\=&\frac{(k-2)(k-4)\dots 1}{(k-1)(k-3)\dots 2}\int_0^{\pi/2}\cos^{0}(\theta)d\theta\\=&\frac{(k-2)!!}{(k-1)!!}\frac{\pi}{2}.\end{aligned}$$

Thus, by (8), to show (23) holds for any odd number k, it is equivalent to show

$$\frac{\Gamma((k+1)/2)}{\Gamma(k/2)}=\frac{1}{\sqrt{\pi}}\frac{(k-1)!!}{(k-2)!!}. \tag{26}$$

Similarly, when k is an odd number, we have

$$\begin{aligned}&\frac{\Gamma((k+1)/2)}{\Gamma(k/2)}\\=&\frac{(k-1)(k-3)}{(k-2)(k-4)}\frac{\Gamma((k-3)/2)}{\Gamma((k-4)/2)}\\=&\dots\\=&\frac{(k-1)(k-3)\dots 2}{(k-2)(k-4)\dots 1}\frac{\Gamma(1)}{\Gamma(1/2)}\\=&\frac{(k-1)!!}{(k-2)!!}\frac{1}{\sqrt{\pi}}.\end{aligned}$$

Clearly, (26) holds. ■

REFERENCES

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

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

[3] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, no. 170, pp. 463–471, 1985.

[4] M. O. Damen, H. E. Gamal, and G. Caire, "On maximum likelihood detection and the search for the closest lattice point," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2389–2402, 2003.

[5] T. Cui and C. Tellambura, "Approximate ml detection for MIMO systems using multistage sphere decoding," *IEEE Signal Process. Lett.*, vol. 12, no. 3, 2005.

[6] A. Ghaderipoor and C. Tellambura, "A statistical pruning strategy for schnorr-euchner sphere decoding," *IEEE Wireless Commun. Lett.*, vol. 12, no. 2, pp. 121–123, 2008.

[7] T. Cui, S. Han, and C. Tellambura, "Probability-distribution-based node pruning for sphere decoding," *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1586–1596, 2013.

[8] J. Wen, B. Zhou, W. H. Mow, and X.-W. Chang, "An efficient algorithm for optimally solving a shortest vector problem in compute-and-forward design," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6541–6555, 2016.

[9] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.*, vol. 261, no. 4, pp. 515–534, 1982.

[10] X.-W. Chang, J. Wen, and X. Xie, "Effects of the LLL reduction on the success probability of the babai point and on the complexity of sphere decoding," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4915–4926, 2013.

[11] D. Micciancio, "The hardness of the closest vector problem with preprocessing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1212–1215, 2001.

[12] L. Babai, "On lovasz lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.

[13] X.-W. Chang and Q. Han, "Solving box-constrained integer least squares problems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 277–287, 2008.

[14] A. Hassibi and S. Boyd, "Integer parameter estimation in linear models with applications to GPS," *IEEE Trans. Signal Process.*, vol. 46, no. 11, pp. 2938–2952, 1998.

[15] J. Wen, C. Tong, and S. Bai, "Effects of some lattice reductions on the success probability of the zero-forcing decoder," *IEEE Commun. Lett.*, vol. 20, no. 10, p. 2031, 2016.

[16] J. Wen and X.-W. Chang, "The success probability of the Babai point estimator and the integer least squares estimator in box-constrained integer linear models," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 631–648, 2017.

[17] R. I. Muirhead, *Aspects of Multivariate Statistical Theory*. New York: Wiley, 1982.

[18] H. Daudé and B. Vallée, "An upper bound on the average number of iterations of the LLL algorithm," *Theor. Comput. Sci.*, vol. 123, no. 1, pp. 95–115, 1994.

[19] C. Ling, W. Mow, and N. Howgrave-Graham, "Reduced and fixed-complexity variants of the LLL algorithm for communications," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1040–1050, 2013.

[20] J. Jaldén, D. Seethaler, and G. Matz, "Worst-and average-case complexity of LLL lattice reduction in MIMO wireless systems," in *Proceedings of the 2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008, pp. 2685–2688.