

Successive Integer-Forcing and its Sum-Rate Optimality

Or Ordentlich
Tel Aviv University
ordent@eng.tau.ac.il

Uri Erez
Tel Aviv University
uri@eng.tau.ac.il

Bobak Nazer
Boston University
bobak@bu.edu

Abstract—Integer-forcing receivers generalize traditional linear receivers for the multiple-input multiple-output channel by decoding integer-linear combinations of the transmitted streams, rather than the streams themselves. Previous works have shown that the additional degree of freedom in choosing the integer coefficients enables this receiver to approach the performance of maximum-likelihood decoding in various scenarios. Nonetheless, even for the optimal choice of integer coefficients, the additive noise at the equalizer’s output is still correlated. In this work we study a variant of integer-forcing, termed successive integer-forcing, that exploits these noise correlations to improve performance. This scheme is the integer-forcing counterpart of successive interference cancellation for traditional linear receivers. Similarly to the latter, we show that successive integer-forcing is capacity achieving when it is possible to optimize the rate allocation to the different streams. In comparison to standard successive interference cancellation receivers, the successive integer-forcing receiver offers more possibilities for capacity achieving rate tuples, and in particular, ones that are more balanced.

I. INTRODUCTION

The integer-forcing (IF) linear receiver architecture, proposed in [1], provides an alternative to standard linear receivers for the Gaussian multiple-input multiple-output (MIMO) channel. Classical architectures, such as zero-forcing (ZF) and linear minimum mean-squared error (MMSE) receivers, first equalize the channel to the identity matrix \mathbf{I} and then decode each data stream separately via single-user decoders. While this reduces the implementation complexity (as compared to jointly decoding the data streams), it comes at the cost of a significant rate loss. This is due to the fact that, after equalization, the total noise power is spread unevenly across data streams. If there is no channel state information at the transmitter (CSIT), it is not possible to allocate rates to compensate for this noise perturbation. The main advantage of the IF receiver over classical linear receivers is that it has the freedom to equalize the channel to any full-rank integer-valued matrix \mathbf{A} . This helps the receiver reduce the correlations between the noises experienced by each of its single-user decoders, and balance the noise power across them. Using the

compute-and-forward strategy [2], each of these decoders then recovers an integer-linear combination of the data streams. Finally, the resulting noise-free linear combinations are solved for the desired data streams. We note that the complexity of the IF receiver is comparable¹ to that of a classical ZF or linear MMSE receiver.

Recent work [3] has shown that the IF receiver can attain the capacity of the Gaussian MIMO channel to within a constant number of bits in an open-loop scenario (no CSIT), provided that an appropriate universal linear precoding operation is applied at the transmitter. Moreover, even without precoding at the transmitter, it is shown in [3] that for almost every channel matrix the IF receiver attains the total degrees-of-freedom (DoF) offered by the channel, even when the number of receive antennas is smaller than the number of transmit antennas and is unknown at the transmitter. This is in sharp contrast to standard linear receivers that cannot achieve any DoF in such scenarios. As an example consider the M -user Gaussian multiple-access channel (MAC) where each user is equipped with one transmit antenna and the receiver is also equipped with a single antenna. Obviously, applying the linear MMSE equalizer on the channel’s output would result in highly suboptimal performance, as there are not enough observations to separate the transmitted signals at the receiver. With IF equalization, on the other hand, the ratios between the individual rates achieved by each user and the symmetric capacity tend to one for almost all channel gains as the signal-to-noise ratio (SNR) increases [4].

Beyond its role as a low-complexity receiver architecture, IF also has several theoretical advantages. In particular, IF equalization exploits the closure of linear/lattice codebooks w.r.t. integer-linear combinations. In the last decade, lattice codes were found to play a key role in characterizing the fundamental limits of certain communication networks, see e.g. [2], [4]–[8]. A common feature of several of these lattice-based coding schemes is that, from the perspective of each receiver, they induce effective multiple-access channels with a reduced number of users, all of which employ the same lattice codebook. The achievable rates for a MAC where all users use the same lattice codebook is difficult to analyze [9], but can

The work of U. Erez was supported in part by the Israel Science Foundation under Grant No. 1557/13. The work of O. Ordentlich was supported by the Adams Fellowship Program of the Israel Academy of Sciences and Humanities, a fellowship from The Yitzhak and Chaya Weinstein Research Institute for Signal Processing at Tel Aviv University and the Feder Family Award. The work of B. Nazer was supported by NSF grant CCF-1253918.

¹The additional complexity comes from computing the target integer-valued matrix \mathbf{A} . This is required only once per coherence interval, meaning that the added complexity is negligible for long coherence times.

be lower bounded by the rates attained via the IF receiver [4].

The performance of standard linear receivers can be improved using successive interference cancellation (SIC). The key idea is to use decoded streams to improve the channel quality for decoding subsequent streams. In this paper, we develop and analyze an analogous scheme for IF, dubbed *successive integer-forcing*. That is, the receiver will use decoded linear combinations in order to improve the channel quality for decoding the remaining linear combinations. The idea of applying SIC to IF has been partially explored in the literature. In [10], a successive decoding procedure was developed for the IF receiver in the setting where the number of receive antennas is at least as high as the number of transmit antennas. However, the optimal filter design was not found, meaning that the obtained achievable rates are suboptimal. In [11], a successive procedure was developed for decoding two linear combinations over an M -user Gaussian MAC. The optimal filters and the highest achievable rates were found for this scenario.

The contribution of the present work is a successive IF scheme that is suitable for any number of transmit and receive antennas, and any number of desired linear combinations. Through standard linear filtering theory, we derive closed-form expressions for the optimal filters and characterize the corresponding achievable rates. We also show that the optimal integer coefficients for successive IF can be obtained using Korkin-Zolotarev lattice basis reduction. Thus, in contrast to standard IF, the optimal integer-valued matrix \mathbf{A} (in terms of achievable rate) for successive IF is always unimodular.

The IF scheme is most advantageous in an open-loop scenario where the transmitter does not know the channel gains. In this case, it does not know how to allocate rates to the different streams, and therefore a single codebook is usually used for encoding each of the transmitted streams. However, as mentioned above, the IF scheme is also of theoretical interest in the context of network communication problems, where it is commonly assumed that all transmitters know all channel gains. In this case, the rates of the different streams transmitted in the IF scheme can be appropriately allocated. We show that with a judicious rate allocation, under several technical conditions, successive IF can achieve rate tuples whose sum equals the channel's multiple-access sum-capacity. While this property is shared with the standard MMSE-SIC equalizer [12], successive IF equalization achieves additional sum-rate optimal rate tuples that are not attained by MMSE-SIC equalization without rate-splitting or time-sharing. These rate tuples lie closer to the symmetric capacity than those attained by the MMSE-SIC equalizer.

II. PRELIMINARIES

In this section, we review some key results that will be useful in our derivation of the successive IF receiver. Throughout the paper, lowercase boldface variables will refer to column or row vectors (e.g., $\mathbf{x} \in \mathbb{R}^{n \times 1}$ or $\mathbf{x} \in \mathbb{R}^{1 \times n}$). In general, we use row vectors for vectors whose entries correspond to different

time indices and column vectors for vectors whose entries correspond to different spatial indices. Uppercase boldface variables will refer to matrices (e.g., $\mathbf{X} \in \mathbb{R}^{M \times n}$). For a given matrix \mathbf{X} , we denote its transpose by \mathbf{X}^T and its Frobenius norm as $\|\mathbf{X}\|_F$. We denote the identity matrix by \mathbf{I} where the dimensions will be clear from the context. All logarithms are taken to base 2 and rates are measured in bits per channel use.

We will focus on the real-valued Gaussian multiple-input multiple-output (MIMO) channel with M transmit and N receive antennas. The channel output is given by

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{Z} \quad (1)$$

where $\mathbf{H} \in \mathbb{R}^{N \times M}$ is the channel matrix, $\mathbf{X} \in \mathbb{R}^{M \times n}$ is the channel input across the M transmit antennas over n channel uses, and $\mathbf{Z} \in \mathbb{R}^{N \times n}$ is additive noise that is elementwise i.i.d. Gaussian with zero mean and unit variance. The channel input is subject to the power constraint

$$\frac{1}{n} \mathbb{E} \|\mathbf{X}\|_F^2 \leq M \cdot \text{SNR}.$$

Remark 1: Following the steps in [2, Appendix C], we can show that our results also hold under a strict power constraint $\frac{1}{n} \|\mathbf{X}\|_F^2 \leq M \cdot \text{SNR}$.

Remark 2: All of our results can be immediately extended to $M \times N$ complex-valued MIMO channels by expressing these channels in terms of their $2M \times 2N$ real-valued decomposition. See [1] for more details.

A. MIMO Capacity

The capacity of the MIMO channel is given by [13]

$$C = \max_{\substack{\mathbf{Q} \succ 0 \\ \text{trace}(\mathbf{Q}) \leq M \cdot \text{SNR}}} \frac{1}{2} \log \det (\mathbf{I} + \mathbf{Q}\mathbf{H}^T\mathbf{H}). \quad (2)$$

The choice of \mathbf{Q} that maximizes (2) is determined by the water-filling solution. Often, the suboptimal choice $\mathbf{Q} = \text{SNR} \cdot \mathbf{I}$ is used, resulting in the *white-input (WI) mutual information*

$$C_{\text{WI}} = \frac{1}{2} \log \det (\mathbf{I} + \text{SNR} \mathbf{H}^T\mathbf{H}).$$

Remark 3: Note that if we restrict the M rows of the channel input \mathbf{X} to be independent with power constraints $\frac{1}{n} \mathbb{E} \|\mathbf{x}_m\|^2 \leq \text{SNR}$ for $m = 1, \dots, M$, the channel model (1) describes an M -user Gaussian MAC, where each user is equipped with a single transmit antenna and the receiver with N antennas. In this case, C_{WI} is the sum-capacity [14, Eq. (15.153)].

B. Successive Interference Cancellation via Noise-Prediction

In the sequel, we will show that successive IF can achieve C_{WI} , provided that the transmitter can allocate rates correctly to the different streams. In order to gain some intuition, we review the standard MMSE-SIC scheme, also known as V-BLAST. However, rather than describing the receiver's decoding procedure in the common way, where it successively decodes streams and subtracts them to get a "cleaner" channel,

we describe a receiver that performs *noise prediction*. These two variants are known to be equivalent [15].

Assume each of the M antennas transmits a stream $\mathbf{x}_m \in \mathbb{R}^{1 \times n}$ of length n taken from an i.i.d. Gaussian code with average power SNR, independent of the streams transmitted by the other antennas. The receiver decodes the transmitted streams in M successive steps, where in each step a single stream is decoded. The receiver first performs linear MMSE estimation of $\mathbf{X} = [\mathbf{x}_1^T \cdots \mathbf{x}_M^T]^T$ from \mathbf{Y} using the filter matrix

$$\mathbf{B} = \mathbf{H}^T \left(\frac{1}{\text{SNR}} \mathbf{I} + \mathbf{H}\mathbf{H}^T \right)^{-1}. \quad (3)$$

This gives rise to the effective channel

$$\mathbf{Y}_{\text{eff}} = \mathbf{B}\mathbf{Y} = \mathbf{X} + \mathbf{E},$$

where

$$\mathbf{E} = (\mathbf{B}\mathbf{H} - \mathbf{I})\mathbf{X} + \mathbf{B}\mathbf{Z},$$

is the estimation error. Since \mathbf{X} and \mathbf{Z} are statistically independent and all their entries are i.i.d. Gaussian, the columns of \mathbf{E} are Gaussian vectors, statistically independent of each other. Each column of \mathbf{E} , corresponding to a different time index, is a zero-mean Gaussian vector with covariance matrix

$$\mathbf{K}_{\text{ee}} = \text{SNR}(\mathbf{B}\mathbf{H} - \mathbf{I})(\mathbf{B}\mathbf{H} - \mathbf{I})^T + \mathbf{B}\mathbf{B}^T \quad (4)$$

$$= \text{SNR}(\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1}, \quad (5)$$

where (5) follows by substituting (3) into (4) and applying Woodbury's matrix identity (i.e., the Matrix Inversion Lemma) [16, Thm 18.2.8].

The matrix $(\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1}$ is symmetric and positive definite, and therefore admits a (unique) Cholesky decomposition

$$(\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1} = \mathbf{G}\mathbf{G}^T, \quad (6)$$

where $\mathbf{G} \in \mathbb{R}^{M \times M}$ is a lower triangular matrix with strictly positive diagonal entries. It follows that

$$\mathbf{K}_{\text{ee}} = \text{SNR} \mathbf{G}\mathbf{G}^T, \quad (7)$$

and \mathbf{E} can be written as $\mathbf{E} = \sqrt{\text{SNR}} \mathbf{G}\mathbf{W}$, where \mathbf{W} is an $M \times n$ matrix of i.i.d. Gaussian entries with zero mean and unit variance. Thus, the effective channel can be written as

$$\mathbf{Y}_{\text{eff}} = \mathbf{X} + \sqrt{\text{SNR}} \mathbf{G}\mathbf{W}. \quad (8)$$

Now, the receiver starts successively decoding the streams. First, it uses $\mathbf{y}_{\text{eff},1}$, the first row of \mathbf{Y}_{eff} , to decode the first stream \mathbf{x}_1 . Denoting the (i, j) -th entry of \mathbf{G} by g_{ij} , this can be done as long as the rate of this stream satisfies

$$\begin{aligned} R_1 &< \frac{1}{2} \log \left(1 + \frac{\text{SNR}}{g_{11}^2 \text{SNR}} - 1 \right) \\ &= -\frac{1}{2} \log (g_{11}^2). \end{aligned}$$

where the -1 term inside the logarithm compensates for the fact that \mathbf{E} and \mathbf{X} are correlated, as explained in [17, Lemma

2]. After correctly decoding \mathbf{x}_1 , the receiver can obtain \mathbf{w}_1 , the first row of \mathbf{W} , as

$$\mathbf{w}_1 = \frac{\mathbf{y}_{\text{eff},1} - \mathbf{x}_1}{\sqrt{\text{SNR}g_{11}}}, \quad (9)$$

and produce a less noisy channel

$$\begin{aligned} \mathbf{Y}_{\text{eff}}^{(2)} &= \mathbf{Y}_{\text{eff}} - \sqrt{\text{SNR}}\mathbf{g}_1\mathbf{w}_1 \\ &= \mathbf{X} + \sqrt{\text{SNR}} \cdot \mathbf{G}^{(2)}\mathbf{W}, \end{aligned}$$

where \mathbf{g}_1 is the first column of \mathbf{G} and $\mathbf{G}^{(2)} = \mathbf{G} - \mathbf{g}_1$ is the matrix \mathbf{G} with its first column nulled out. Now, the receiver can decode \mathbf{x}_2 from $\mathbf{y}_{\text{eff},2}^{(2)}$, the second row of $\mathbf{Y}_{\text{eff}}^{(2)}$, as long as its rate satisfies

$$R_2 < -\frac{1}{2} \log (g_{22}^2).$$

Continuing in the same manner, it follows that each stream can be decoded reliably as long as

$$R_m < -\frac{1}{2} \log (g_{mm}^2), \quad m = 1, \dots, M.$$

The described noise prediction scheme can therefore achieve the sum-rate

$$\begin{aligned} \sum_{m=1}^M R_m &= -\frac{1}{2} \sum_{m=1}^M \log (g_{mm}^2) \\ &= -\frac{1}{2} \log \left(\prod_{m=1}^M g_{mm}^2 \right) \\ &= -\frac{1}{2} \log \det (\mathbf{G}\mathbf{G}^T) \\ &= \frac{1}{2} \log \det (\mathbf{I} + \text{SNR}\mathbf{H}^T\mathbf{H}) \\ &= C_{\text{WI}}. \end{aligned}$$

In the sequel, we will see that a similar noise prediction scheme enables successive integer-forcing to achieve a sum-rate of C_{WI} . Rather than performing linear MMSE estimation for \mathbf{X} , in successive integer-forcing one estimates the linear combinations $\mathbf{A}\mathbf{X}$, and successively predicts the associated estimation errors.

C. Integer-Forcing

IF equalization is a low-complexity architecture for the MIMO channel, which was proposed by Zhan *et al.* [1]. The key idea underlying IF is to first decode integer-linear combinations of the signals transmitted by all antennas, and then, after the noise is removed, invert those linear combinations to recover the individual transmitted signals. This is made possible by transmitting codewords from the *same* linear/lattice code from all M transmit antennas, leveraging the property that linear codes are closed under (modulo) linear combinations with integer-valued coefficients.

We briefly recall the IF scheme. We begin by presenting several lattice definitions. A lattice Λ is a discrete subgroup of \mathbb{R}^n which is closed under reflection and real addition.

We denote the nearest neighbor quantizer associated with the lattice Λ by

$$Q_\Lambda(\mathbf{x}) = \arg \min_{\mathbf{t} \in \Lambda} \|\mathbf{x} - \mathbf{t}\|. \quad (10)$$

The basic Voronoi region of Λ , denoted by \mathcal{V} , is the set of all points in \mathbb{R}^n which are quantized to the zero vector, where ties in (10) are broken in a systematic manner. The modulo operation returns the quantization error w.r.t. the lattice,

$$[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x}),$$

and the second moment of Λ is defined as

$$\sigma^2(\Lambda) = \frac{1}{n} \frac{1}{\text{Vol}(\mathcal{V})} \int_{\mathbf{u} \in \mathcal{V}} \|\mathbf{u}\|^2 d\mathbf{u},$$

where $\text{Vol}(\mathcal{V})$ is the volume of \mathcal{V} . A lattice Λ is said to be nested in Λ_1 if $\Lambda \subseteq \Lambda_1$. The coding scheme presented in this paper utilizes a pair of n -dimensional nested lattices $\Lambda_c \subset \Lambda_f$, where Λ_c is referred to as the coarse lattice and Λ_f as the fine lattice. A nested lattice codebook $\mathcal{C} = \Lambda_f \cap \mathcal{V}_c$, with rate

$$R = \frac{1}{n} \log |\Lambda_f \cap \mathcal{V}_c|$$

is associated with the nested lattice pair. The codebook is scaled such that $\sigma^2(\Lambda_c) = \text{SNR}$. In Section III-A we extend the proposed coding scheme to one that uses a chain of $M+1$ nested lattices

$$\Lambda_c \subseteq \Lambda_{f_M} \subseteq \dots \subseteq \Lambda_{f_1}, \quad (11)$$

from which we construct M nested codebooks.

In the IF scheme, the information bits to be transmitted are partitioned into M streams. Each of these streams is encoded by the nested lattice code \mathcal{C} , producing M row vectors, each in $\mathcal{C} \subset \mathbb{R}^{1 \times n}$. In particular, the m th stream, consisting of nR information bits, is mapped to a lattice point $\mathbf{t}_m \in \mathcal{C}$. Then, a random dither² $\mathbf{d}_m \in \mathbb{R}^{1 \times n}$ uniformly distributed over \mathcal{V}_c and statistically independent of \mathbf{t}_m , known to both the transmitter and the receiver, is used to produce the signal

$$\mathbf{x}_m = [\mathbf{t}_m - \mathbf{d}_m] \bmod \Lambda_c.$$

The signal \mathbf{x}_m is uniformly distributed over \mathcal{V}_c and is statistically independent of \mathbf{t}_m due to the Crypto Lemma [18, Lemma 1]. It follows that

$$\frac{1}{n} \mathbb{E} \|\mathbf{x}_m\|^2 = \sigma^2(\Lambda_c) = \text{SNR}.$$

The m th antenna transmits the signal $\mathbf{x}_m \in \mathbb{R}^{1 \times n}$ over n consecutive channel uses.

Define $\mathbf{T} \triangleq [\mathbf{t}_1^T \dots \mathbf{t}_M^T]^T$ to be the $M \times n$ matrix whose rows consist of the lattice points corresponding to the M data streams, $\mathbf{D} \triangleq [\mathbf{d}_1^T \dots \mathbf{d}_M^T]^T$ be the $M \times n$ matrix whose rows correspond to the M dither vectors, and $\mathbf{X} \triangleq [\mathbf{x}_1^T \dots \mathbf{x}_M^T]^T$ be the matrix whose rows correspond to the M channel

²These random dithers can be replaced with deterministic dithers without affecting the achievable rate region, i.e., no common randomness is necessary. See [2, Appendix C] for more details.

input vectors. These inputs vectors are transmitted into the channel (1) to yield the $N \times n$ output \mathbf{Y} .

The IF receiver chooses an equalizing filter matrix $\mathbf{B} \in \mathbb{R}^{M \times N}$ and a full-rank target integer-valued matrix $\mathbf{A} \in \mathbb{Z}^{M \times M}$, and computes

$$\begin{aligned} \mathbf{Y}_{\text{eff}} &= [\mathbf{B}\mathbf{Y} + \mathbf{A}\mathbf{D}] \bmod \Lambda_c \\ &= [\mathbf{A}\mathbf{X} + \mathbf{A}\mathbf{D} + (\mathbf{B}\mathbf{H} - \mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z}] \bmod \Lambda_c \\ &= [\mathbf{A}\mathbf{T} + (\mathbf{B}\mathbf{H} - \mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z}] \bmod \Lambda_c \\ &= [\mathbf{V} + \mathbf{Z}_{\text{eff}}] \bmod \Lambda_c, \end{aligned} \quad (12)$$

where

$$\mathbf{V} \triangleq [\mathbf{A}\mathbf{T}] \bmod \Lambda_c \quad (13)$$

is an $M \times n$ real-valued matrix with each row being a codeword in \mathcal{C} owing to the linearity of the code,

$$\mathbf{Z}_{\text{eff}} \triangleq (\mathbf{B}\mathbf{H} - \mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z} \quad (14)$$

is additive noise statistically independent of \mathbf{V} (since \mathbf{X} and \mathbf{Z} are statistically independent of \mathbf{T}), and the notation $\bmod \Lambda_c$ is to be understood as reducing *each row* of the obtained matrix modulo the coarse lattice. Each row of \mathbf{Y}_{eff} , denoted by $\mathbf{y}_{\text{eff},m}$, $m = 1, \dots, M$, is the modulo sum of a codeword and effective noise. Thus, the IF receiver transforms the original MIMO channel into a set of M point-to-point modulo-additive sub-channels

$$\mathbf{y}_{\text{eff},m} = [\mathbf{v}_m + \mathbf{z}_{\text{eff},m}] \bmod \Lambda_c, \quad m = 1, \dots, M. \quad (15)$$

The IF receiver decodes the output of each sub-channel separately. If the decoding is successful over all M sub-channels, the receiver has access to $\mathbf{V} = [\mathbf{v}_1^T \dots \mathbf{v}_M^T]^T$, from which it can recover the matrix \mathbf{T} by solving the (modulo) set of equations.

Define the effective variance of $\mathbf{z}_{\text{eff},m}$ as

$$\sigma_{\text{eff},m}^2 \triangleq \frac{1}{n} \mathbb{E} \|\mathbf{z}_{\text{eff},m}\|^2.$$

It follows from [2], [18] that for a ‘‘good’’ (capacity-achieving) nested lattice code \mathcal{C} the integer-linear combination \mathbf{v}_m can be reliably decoded from $\mathbf{y}_{\text{eff},m}$ as long as

$$R < \frac{1}{2} \log \left(\frac{\text{SNR}}{\sigma_{\text{eff},m}^2} \right),$$

and all M equations can be decoded reliably if

$$R < \min_{m=1, \dots, M} \frac{1}{2} \log \left(\frac{\text{SNR}}{\sigma_{\text{eff},m}^2} \right).$$

Note that the additive noise vectors $\mathbf{z}_{\text{eff},1}, \dots, \mathbf{z}_{\text{eff},M}$ are not statistically independent. Thus, treating the M sub-channels as parallel is suboptimal, and some improvement can be obtained by exploiting this coupling. In the next section, we will show how successive IF exploits the aforementioned noise correlations to enhance performance, with only a slight increase in the decoding complexity, i.e., the receiver still decodes the linear combinations one-by-one.

D. Linear MMSE Estimation and Generalizations to Matrix Estimation

The derivation of the optimal filters for successive IF involves several results from linear MMSE estimation.

Consider a random vector $\mathbf{x} \in \mathbb{R}^{M \times 1}$ with zero mean and covariance matrix $\{\mathbf{K}_{\mathbf{x}\mathbf{x}}\}_{ij} = \mathbb{E}(x_i x_j)$ and a random vector of measurements $\mathbf{y} \in \mathbb{R}^{N \times 1}$ with zero mean and covariance matrix $\{\mathbf{K}_{\mathbf{y}\mathbf{y}}\}_{ij} = \mathbb{E}(y_i y_j)$. The cross-covariance matrix between \mathbf{x} and \mathbf{y} is given by $\{\mathbf{K}_{\mathbf{x}\mathbf{y}}\}_{ij} = \mathbb{E}(x_i y_j)$. The class of linear estimators for \mathbf{x} from \mathbf{y} consists of all estimators of the form $\hat{\mathbf{x}} = \mathbf{B}\mathbf{y}$, where $\mathbf{B} \in \mathbb{R}^{M \times N}$. The estimation error is defined as $\mathbf{e} = \mathbf{x} - \hat{\mathbf{x}}$, and the linear MMSE criterion corresponds to minimizing $\mathbb{E}(e_i^2)$ for all $i = 1, \dots, M$ over all filters $\mathbf{B} \in \mathbb{R}^{M \times N}$. It is well known that the optimal estimation filter under this criterion must satisfy the orthogonality principle

$$\mathbf{0} = \mathbb{E}(\mathbf{e}\mathbf{y}^T) = \mathbb{E}((\mathbf{x} - \mathbf{B}\mathbf{y})\mathbf{y}^T),$$

where $\mathbf{0}$ is a matrix of zeros with appropriate dimensions, and is given by

$$\mathbf{B}^* = \mathbf{K}_{\mathbf{x}\mathbf{y}}\mathbf{K}_{\mathbf{y}\mathbf{y}}^{-1}.$$

For the optimal estimator, the estimation error covariance matrix is given by

$$\mathbf{K}_{\mathbf{e}\mathbf{e}} \triangleq \mathbb{E}(\mathbf{e}\mathbf{e}^T) = \mathbf{K}_{\mathbf{x}\mathbf{x}} - \mathbf{K}_{\mathbf{x}\hat{\mathbf{x}}}.$$

In the previous subsection we have seen that the performance of the IF receiver is dictated by \mathbf{Z}_{eff} , which can be thought of as the estimation error of $\mathbf{A}\mathbf{X}$ from $\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{Z}$, when the filter \mathbf{B} is used. The achievable rate for IF over the m th sub-channel is maximized when $\sigma_{\text{eff},m}^2 = 1/n\mathbb{E}\|\mathbf{z}_{\text{eff},m}\|^2$ is minimized. Thus, \mathbf{B} should be chosen such as to minimize $\sigma_{\text{eff},m}^2$ for all $m = 1, \dots, M$. This criterion is similar to the MMSE criterion, except for the fact that here the goal is to minimize the effective variance of a (non-i.i.d.) vector, rather than the variance of a random variable. However, as we now show, the two problems are equivalent if we replace the covariance matrices of random vectors, whose entries correspond to the correlations between random variables, with *generalized covariance matrices* whose entries correspond to the effective correlations between random vectors.

Definition 1: For a random matrix $\mathbf{X} \in \mathbb{R}^{M \times n}$ with rows $\mathbf{x}_i^T \in \mathbb{R}^{1 \times n}$, $i = 1, \dots, M$, we define the generalized covariance matrix as

$$\{\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{X}}\}_{ij} \triangleq \frac{1}{n}\mathbb{E}(\mathbf{x}_i^T \mathbf{x}_j).$$

If $\mathbf{Y} \in \mathbb{R}^{N \times n}$ with rows $\mathbf{y}_j^T \in \mathbb{R}^{1 \times n}$, $j = 1, \dots, N$, is another random matrix, we define the generalized cross-covariance matrix of \mathbf{X} and \mathbf{Y} as

$$\{\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{Y}}\}_{ij} \triangleq \frac{1}{n}\mathbb{E}(\mathbf{x}_i^T \mathbf{y}_j).$$

Proposition 1: Let $\mathbf{X} \in \mathbb{R}^{M \times n}$ and $\mathbf{Y} \in \mathbb{R}^{N \times n}$ be two random matrices with generalized covariance matrices $\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{X}}$ and $\tilde{\mathbf{K}}_{\mathbf{Y}\mathbf{Y}}$, respectively, and cross-covariance matrix $\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{Y}}$. Let

$\mathbf{W} = \mathbf{G}\mathbf{X}$ and $\mathbf{U} = \mathbf{H}\mathbf{Y}$ for two deterministic matrices $\mathbf{G} \in \mathbb{R}^{K \times M}$ and $\mathbf{H} \in \mathbb{R}^{L \times N}$. Then, $\tilde{\mathbf{K}}_{\mathbf{W}\mathbf{U}} = \mathbf{G}\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{Y}}\mathbf{H}^T$, and in particular, $\tilde{\mathbf{K}}_{\mathbf{W}\mathbf{W}} = \mathbf{G}\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{X}}\mathbf{G}^T$ and $\tilde{\mathbf{K}}_{\mathbf{U}\mathbf{U}} = \mathbf{H}\tilde{\mathbf{K}}_{\mathbf{Y}\mathbf{Y}}\mathbf{H}^T$.

Proof:

$$\begin{aligned} \{\tilde{\mathbf{K}}_{\mathbf{W}\mathbf{U}}\}_{ij} &= \frac{1}{n}\mathbb{E}(\mathbf{w}_i^T \mathbf{u}_j) \\ &= \frac{1}{n}\mathbb{E}\left(\sum_{k=1}^K \sum_{\ell=1}^L g_{ik} \mathbf{x}_k^T \mathbf{y}_\ell h_{j\ell}\right) \\ &= \sum_{k=1}^K \sum_{\ell=1}^L g_{ik} \{\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{Y}}\}_{k\ell} h_{j\ell} \\ &= \left\{ \mathbf{G}\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{Y}}\mathbf{H}^T \right\}_{ij}. \end{aligned}$$

Lemma 1: Let $\mathbf{x} \in \mathbb{R}^{M \times 1}$ and $\mathbf{y} \in \mathbb{R}^{N \times 1}$ be two random vectors with zero mean, covariances $\mathbf{K}_{\mathbf{x}\mathbf{x}}$ and $\mathbf{K}_{\mathbf{y}\mathbf{y}}$ and cross-covariance matrix $\mathbf{K}_{\mathbf{x}\mathbf{y}}$. Let $\mathbf{X} \in \mathbb{R}^{M \times n}$ and $\mathbf{Y} \in \mathbb{R}^{N \times n}$ be two random matrices with zero mean and generalized covariance and cross-covariances as \mathbf{x} and \mathbf{y} , i.e., $\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{X}} = \mathbf{K}_{\mathbf{x}\mathbf{x}}$, $\tilde{\mathbf{K}}_{\mathbf{Y}\mathbf{Y}} = \mathbf{K}_{\mathbf{y}\mathbf{y}}$ and $\tilde{\mathbf{K}}_{\mathbf{X}\mathbf{Y}} = \mathbf{K}_{\mathbf{x}\mathbf{y}}$. Then, for any filter $\mathbf{B} \in \mathbb{R}^{M \times N}$

$$\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}} = \mathbf{K}_{\mathbf{e}\mathbf{e}},$$

where $\mathbf{E} = \mathbf{B}\mathbf{Y} - \mathbf{X}$ and $\mathbf{e} = \mathbf{B}\mathbf{y} - \mathbf{x}$. In particular, the linear MMSE estimator for x_m from \mathbf{y} also minimizes the effective variance of the estimation error vector of \mathbf{x}_m from \mathbf{Y} for all $m = 1, \dots, M$.

Proof: Follows immediately from Definition 1 and Proposition 1. ■

III. SUCCESSIVE INTEGER-FORCING

We now describe and analyze the successive integer-forcing receiver, which combines ideas from classical successive interference cancellation and integer-forcing. At a high level, the goal of the successive IF receiver is the same as that of the IF receiver: first recover a set of integer-linear combinations described by the coefficient matrix $\mathbf{A} \in \mathbb{Z}^{M \times M}$ and then solve for the desired messages. However, rather than decoding these integer-linear combinations in parallel, the successive IF receiver decodes them one at a time and uses decoded combinations to reduce the effective noise encountered in subsequent decoding steps (as in SIC).

The receiver begins by performing linear MMSE estimation of $\mathbf{A}\mathbf{X}$ from \mathbf{Y} , adding back the dithers and reducing the result modulo the coarse lattice, just as in standard IF. The resulting effective channel is given by (12), (13), and (14) where \mathbf{B} is chosen as

$$\mathbf{B} = \mathbf{A}\mathbf{H}^T \left(\frac{1}{\text{SNR}}\mathbf{I} + \mathbf{H}\mathbf{H}^T \right)^{-1}.$$

The resulting generalized covariance matrix of \mathbf{Z}_{eff} is

$$\tilde{\mathbf{K}}_{\mathbf{Z}_{\text{eff}}\mathbf{Z}_{\text{eff}}} = \text{SNR} \mathbf{A}(\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1} \mathbf{A}^T.$$

For a full-rank matrix $\mathbf{A} \in \mathbb{Z}^{M \times M}$, the matrix $\mathbf{A}(\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1} \mathbf{A}^T$ admits a Cholesky decomposition

$$\mathbf{A} (\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1} \mathbf{A}^T = \mathbf{L} \mathbf{L}^T, \quad (16)$$

where $\mathbf{L} \in \mathbb{R}^{M \times M}$ is a lower triangular matrix with strictly positive diagonal entries. Let

$$\mathbf{W} = \frac{1}{\sqrt{\text{SNR}}} \mathbf{L}^{-1} \mathbf{Z}_{\text{eff}}$$

and note that $\tilde{\mathbf{K}}_{\mathbf{W}\mathbf{W}} = \mathbf{I}$, by Proposition 1. Now, the effective channel is

$$\mathbf{Y}_{\text{eff}} = \left[\mathbf{V} + \sqrt{\text{SNR}} \mathbf{L} \mathbf{W} \right] \bmod \Lambda_c, \quad (17)$$

where \mathbf{W} is statistically independent of \mathbf{V} as it is a deterministic function of \mathbf{Z}_{eff} which is statistically independent of \mathbf{V} .

As in Section II-B, the receiver successively decodes the integer-linear combinations one-by-one. After decoding the m th combinations \mathbf{v}_m , it recovers \mathbf{w}_m and cancels its contribution to the effective noises that corrupt equations that are yet to be decoded. Specifically, the receiver begins by decoding \mathbf{v}_1 from $\mathbf{y}_{\text{eff},1}$. This can be done reliably if

$$R < \frac{1}{2} \log \left(\frac{\text{SNR}}{\text{SNR} \ell_{11}^2} \right) = -\frac{1}{2} \log(\ell_{11}^2). \quad (18)$$

Assuming \mathbf{v}_1 was decoded correctly, the receiver next computes

$$\begin{aligned} \hat{\mathbf{w}}_1 &= \frac{1}{\sqrt{\text{SNR} \ell_{11}}} [\mathbf{y}_{\text{eff},1} - \mathbf{v}_1] \bmod \Lambda_c \\ &= \frac{1}{\sqrt{\text{SNR} \ell_{11}}} \left[\sqrt{\text{SNR}} \ell_{11} \mathbf{w}_1 \right] \bmod \Lambda_c \\ &\stackrel{w.h.p.}{=} \mathbf{w}_1, \end{aligned} \quad (19)$$

where (19) follows from the fact that for a ‘‘good’’ nested lattice codebook (18) implies that $\sqrt{\text{SNR}} \ell_{11} \mathbf{w}_1 \in \mathcal{V}_f \subset \mathcal{V}_c$ with high probability. See Section III-B for a comprehensive discussion on this assumption. The receiver then uses \mathbf{w}_1 to produce a less noisy channel

$$\begin{aligned} \mathbf{Y}_{\text{eff}}^{(2)} &= \left[\mathbf{Y}_{\text{eff}} - \sqrt{\text{SNR}} \mathbf{l}_1 \mathbf{w}_1 \right] \bmod \Lambda_c \\ &= \left[\mathbf{V} + \sqrt{\text{SNR}} \mathbf{L}^{(2)} \mathbf{W} \right] \bmod \Lambda_c, \end{aligned}$$

where \mathbf{l}_1 is the first column of \mathbf{L} and $\mathbf{L}^{(2)} = \mathbf{L} - \mathbf{l}_1$ is the matrix \mathbf{L} with its first column nulled out. Now, the receiver can decode \mathbf{v}_2 from $\mathbf{y}_{\text{eff},2}^{(2)}$, the second row of $\mathbf{Y}_{\text{eff}}^{(2)}$, as long as

$$R < -\frac{1}{2} \log(\ell_{22}^2).$$

Continuing in the same manner, it follows that all equations can be decoded reliably as long as

$$R < -\frac{1}{2} \log \left(\max_{m=1, \dots, M} \ell_{mm}^2 \right). \quad (20)$$

This is summarized in the following theorem.

Theorem 1: There exist nested lattice codebooks such that, for any full-rank matrix $\mathbf{A} \in \mathbb{Z}^{M \times M}$, successive IF can achieve any rate satisfying

$$R_{\text{S-IF}} < -\frac{M}{2} \log \left(\max_{m=1, \dots, M} \ell_{mm}^2 \right),$$

where ℓ_{mm} are the diagonal entries of \mathbf{L} from (16).

Note that in the described scheme each antenna transmits an independent stream. Thus, the same coding scheme can be applied over an M -user Gaussian MAC, where the transmit antennas are distributed. Hence, for a Gaussian M -user MAC, with the m th column of \mathbf{H} representing the coefficients from the m th user to the receiver, each user can achieve any rate satisfying (20).

A. Sum Rate Optimality of Successive IF

In this subsection, we consider using a *chain* of nested lattice codebooks. Specifically, M nested lattice codebooks $\mathcal{C}_m = \Lambda_{f_m} \cap \mathcal{V}_c$, $m = 1, \dots, M$, are constructed from the lattice chain (11). Note that $\mathcal{C}_M \subseteq \dots \subseteq \mathcal{C}_1$ by construction, and the associated rates satisfy $R_M \leq \dots \leq R_1$. Each of the M streams is encoded by one of these codebooks. We show that with such a chain of nested lattice codebooks, successive IF can achieve C_{WI} if the transmitter judiciously allocates the rates to the different streams, and if the diagonal entries of \mathbf{L} from (16) are monotonically increasing.

The main idea is that each integer-linear combination \mathbf{v}_m can be decoded reliably if it is taken from a good nested lattice codebook of rate smaller than $-1/2 \log(\ell_{mm}^2)$. Thus, if we could ensure that \mathbf{v}_m belongs to the codebook \mathcal{C}_m , for all $m = 1, \dots, M$, we could just choose the rates of the M nested codebooks to satisfy $R_m < -1/2 \log(\ell_{mm}^2)$.

However, $\mathbf{v}_m = [\sum_{k=1}^M a_{mk} \mathbf{t}_k] \bmod \Lambda_c$ belongs to the densest lattice codebook from which the codewords $\mathbf{t}_1, \dots, \mathbf{t}_M$ are taken. This obstacle can be overcome by using the equations that were already decoded not only for estimating the noises corrupting the remaining equations, but also for *reducing the rates* of the remaining equations. This is essentially done by adding integer multiples of decoded equations to the remaining ones in a way that nulls out the effect of some of the lattice points \mathbf{t}_k participating in these equations.

The idea of using decoded equations for reducing the rates of the remaining ones was proposed and analyzed in [4, Section IV.B]. For sake of brevity, we do not repeat the details, and only briefly illustrate the idea by a simple example. Assume that the number of transmit antennas is $M = 2$ and $\mathcal{C}_2 \subset \mathcal{C}_1$ are two nested linear codes over the prime field \mathbb{Z}_p with rates $R_2 \leq R_1$. Two nested lattice codebooks are constructed by mapping \mathcal{C}_1 and \mathcal{C}_2 to a p -PAM constellation, and the coarse lattice, in this case, is taken as $\Lambda_c = p\mathbb{Z}^n$. The first antenna transmits a codeword $\mathbf{t}_1 \in \mathcal{C}_1$ and the second

transmits $\mathbf{t}_2 \in \mathcal{C}_2$. The effective channel (12) is

$$\begin{aligned}\mathbf{y}_{\text{eff},1} &= [a_{11}\mathbf{t}_1 + a_{12}\mathbf{t}_2 + \mathbf{z}_{\text{eff},1}] \bmod p \\ \mathbf{y}_{\text{eff},2} &= [a_{21}\mathbf{t}_1 + a_{22}\mathbf{t}_2 + \mathbf{z}_{\text{eff},2}] \bmod p,\end{aligned}$$

where we assume w.l.o.g. that $\sigma_{\text{eff},1}^2 \leq \sigma_{\text{eff},2}^2$. The first equation $\mathbf{v}_1 = [a_{11}\mathbf{t}_1 + a_{12}\mathbf{t}_2] \bmod p$ is a codeword in \mathcal{C}_1 and can be decoded if R_1 is small enough w.r.t. $\sigma_{\text{eff},1}^2$. After decoding \mathbf{v}_1 the receiver can scale it by $a_{21}a_{11}^{-1}$, where the inversion is over the field \mathbb{Z}_p , and subtract it from $\mathbf{y}_{\text{eff},2}$ to obtain

$$\begin{aligned}\tilde{\mathbf{y}}_{\text{eff},2} &= [a_{21}\mathbf{t}_1 + a_{22}\mathbf{t}_2 - a_{21}a_{11}^{-1}\mathbf{v}_1 + \mathbf{z}_{\text{eff},2}] \bmod p \\ &= [(a_{22} - a_{21}a_{11}^{-1}a_{12})\mathbf{t}_2 + \mathbf{z}_{\text{eff},2}] \bmod p.\end{aligned}$$

Now, $\mathbf{v}_2^{(2)} \triangleq [(a_{22} - a_{21}a_{11}^{-1}a_{12})\mathbf{t}_2] \bmod p$ is in \mathcal{C}_2 and it suffices that R_2 is small enough w.r.t. $\sigma_{\text{eff},2}^2$ to ensure correct decoding. Thus, the described procedure enables to ‘‘allocate’’ different rates to the different equations.

It was shown in [4] that for any full-rank $\mathbf{A} \in \mathbb{Z}^{M \times M}$ such procedure can always ensure that $\mathbf{v}_m \in \mathcal{C}_m$ for all m for at least one mapping between codebooks and transmit antennas. Here, we combine this ingredient with the idea of using the decoded equations also for performing noise prediction. Namely, in the m th successive decoding step we compute

$$\begin{aligned}\mathbf{Y}_{\text{eff}}^{(m)} &= \left[\mathbf{Y}_{\text{eff}} - \sum_{k=1}^{m-1} \left(\sqrt{\text{SNR}} \mathbf{l}_k \mathbf{w}_k - \mathbf{q}_k \mathbf{v}_k \right) \right] \bmod \Lambda_c \\ &= \left[\mathbf{V}^{(m)} + \sqrt{\text{SNR}} \mathbf{L}^{(m)} \mathbf{W} \right] \bmod \Lambda_c,\end{aligned}$$

where the role of the column vectors $\{\mathbf{l}_k\}$ is to perform noise prediction, as before, and the role of the integer-valued column vectors $\{\mathbf{q}_k\}$ is to reduce the number of lattice points participating in the remaining equations, such that only lattice points from $\mathcal{C}_m, \dots, \mathcal{C}_M$ participate in $\mathbf{V}^{(m)}$.

When doing so, however, one new issue arises. Reducing the rate of remaining equations using decoded ones is advantageous if the effective variances $\sigma_{\text{eff},1}^2, \dots, \sigma_{\text{eff},M}^2$ are monotonically increasing, such that the achievable computation rates are monotonically decreasing. Without noise prediction, one can always choose the decoding order such that this is satisfied, i.e., start with the best equation, then decode the second best and so on. When noise prediction is also applied, a situation that may occur is that after decoding the best equation and using it to predict the effective noise for the second equation, the second computation rate becomes higher than the first. This occurs if the diagonal entries of \mathbf{L} , corresponding to the effective variances of the prediction errors, are not monotonically increasing. In this case, using decoded equations for reducing the rates of the remaining ones is less effective.

When the diagonal entries of \mathbf{L} are monotonically increas-

ing, the described scheme can achieve any sum-rate satisfying

$$\begin{aligned}\sum_{m=1}^M R_m &= -\frac{1}{2} \sum_{m=1}^M \log(\ell_{mm}^2) \\ &= -\frac{1}{2} \log \left(\prod_{m=1}^M \ell_{mm}^2 \right) \\ &= -\frac{1}{2} \log \det(\mathbf{L}\mathbf{L}^T) \\ &= -\frac{1}{2} \log \det \left(\mathbf{A} (\mathbf{I} + \text{SNR} \mathbf{H}^T \mathbf{H})^{-1} \mathbf{A}^T \right) \\ &= C_{\text{WI}} - \log |\det(\mathbf{A})|.\end{aligned}$$

The following definition from [4] is needed for formally characterizing the performance of the described scheme.

Definition 2: For a full-rank $M \times M$ matrix \mathbf{A} with integer-valued entries we define the *pseudo-triangularization* process, which transforms the matrix \mathbf{A} to a matrix $\tilde{\mathbf{A}}$ which is upper triangular up to column permutation $\pi = [\pi(1) \pi(2) \dots \pi(M)]$. This is accomplished by left-multiplying \mathbf{A} by a lower triangular matrix \mathbf{R} with unit diagonal, such that $\tilde{\mathbf{A}} = \mathbf{R}\mathbf{A}$ is upper triangular up to column permutation π . Although the matrix \mathbf{A} is integer valued, the matrices \mathbf{R} and $\tilde{\mathbf{A}}$ need not necessarily be integer valued. Note that the pseudo-triangularization process is reminiscent of Gaussian elimination except that row switching and row multiplication are prohibited.

Remark 4: Any full-rank matrix can be triangularized using the Gaussian elimination process, and therefore any full-rank matrix can be pseudo-triangularized with at least one permutation vector π .

Theorem 2: Let $\mathbf{A} \in \mathbb{Z}^{M \times M}$ be a full-rank target integer-valued matrix that can be pseudo-triangularized with the permutation vector π , and let \mathbf{L} be the lower-triangular matrix from (16), whose diagonal entries are ℓ_{ii} . If $\ell_{11}^2 \leq \dots \leq \ell_{MM}^2$, then there exists a chain of nested lattice codebooks $\mathcal{C}_M \subseteq \dots \subseteq \mathcal{C}_1$ with rates $R_M \leq \dots \leq R_1$ such that if each m th antenna encodes its stream using the codebook $\mathcal{C}_{\pi^{-1}(m)}$ with rate $R_{\pi^{-1}(m)}$ and

$$R_{\pi^{-1}(m)} < -\frac{1}{2} \log(\ell_{\pi^{-1}(m)\pi^{-1}(m)}^2), \quad \forall m = 1, \dots, M$$

all streams can be decoded with a vanishing error probability using the successive integer-forcing receiver. In other words, all streams can be decoded if the rate of each m th stream is smaller than $-\frac{1}{2} \log(\ell_{\pi^{-1}(m)\pi^{-1}(m)}^2)$. Consequently, the successive integer-forcing receiver can achieve any rate satisfying

$$R_{\text{S-IF}} < C_{\text{WI}} - \log |\det(\mathbf{A})|.$$

In the described scheme each antenna transmits an independent stream. Thus, Theorem 2 remains valid for a Gaussian MAC with the m th column of \mathbf{H} representing the coefficients from the m th user to the receiver. In this case, the theorem implies that, if the stated conditions on \mathbf{A} are satisfied, there exists a chain of nested lattice codebooks

and a mapping $\pi^{-1} : \{1, \dots, M\} \rightarrow \{1, \dots, M\}$ between users and codebooks such that the m th user can achieve any rate below $-\frac{1}{2} \log(\ell_{\pi^{-1}(m)\pi^{-1}(m)}^2)$ with a vanishing error probability using the successive integer-forcing receiver. Since C_{WI} is the MAC's sum-capacity, under the conditions of Theorem 2, successive IF (which is usually termed successive compute-and-forward for a MAC) achieves the sum-capacity if \mathbf{A} is unimodular.

Remark 5: Note that for the choice $\mathbf{A} = \mathbf{I}$, successive IF corresponds to standard SIC. In this case, the monotonicity condition on the diagonal entries of \mathbf{L} is not needed. This is due to the fact that for the choice $\mathbf{A} = \mathbf{I}$ only one lattice point participates in each ‘‘linear combination’’. Therefore, the procedure from [4, Section IV.B], which induces this monotonicity condition, is not needed.

Example 1: Consider the two-user Gaussian MAC

$$\mathbf{y} = \sqrt{2}\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{z},$$

at SNR = 15dB. For the choice $\mathbf{A} = \mathbf{I}$ and its row permutation, successive IF reduces to standard SIC, and results in the achievable rate-regions

$$R_1 < 0.7776 \frac{\text{bits}}{\text{channel use}}, \quad R_2 < 2.5139 \frac{\text{bits}}{\text{channel use}},$$

and

$$R_1 < 3.0028 \frac{\text{bits}}{\text{channel use}}, \quad R_2 < 0.2887 \frac{\text{bits}}{\text{channel use}},$$

respectively. For the choice

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$$

we have $\ell_{11}^2 < \ell_{22}^2$, as Theorem 2 requires, and $-1/2 \log(\ell_{11}^2) = 1.8452$ and $-1/2 \log(\ell_{22}^2) = 1.4463$. In addition, \mathbf{A} can be pseudo-triangularized with the permutation vectors $\pi_1 = [1 \ 2]$ and $\pi_2 = [2 \ 1]$. It therefore follows that the two rate-regions

$$R_1 < 1.8452 \frac{\text{bits}}{\text{channel use}}, \quad R_2 < 1.4463 \frac{\text{bits}}{\text{channel use}},$$

and

$$R_1 < 1.4463 \frac{\text{bits}}{\text{channel use}}, \quad R_2 < 1.8452 \frac{\text{bits}}{\text{channel use}},$$

are achievable with successive IF. In addition, since $|\det(\mathbf{A})| = 1$, these points are sum-rate optimal. Figure 1 shows the capacity region of the MAC from this example, along with the rate region achieved by successive IF.

Remark 6: An interesting conclusion from Theorem 2 is that if \mathbf{A} is such that the conditions of the theorem are satisfied, then the compute-and-forward decoder used in [2] achieves the same rates as the optimal maximum-likelihood (ML) decoder for decoding the integer-linear combinations whose coefficients are the rows of \mathbf{A} . Recall that the decoder from [2] scales its observations, subtracts the dithers, quantizes

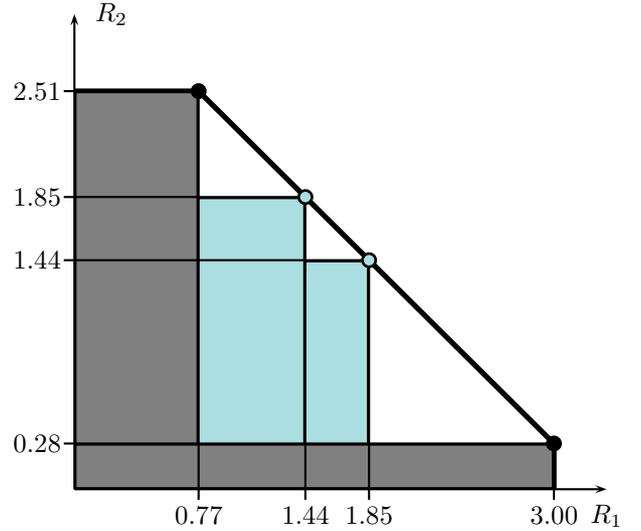


Fig. 1. The capacity region of the MAC from Example 1, and the rate region achieved by successive IF. The gray (dark shaded) area in the figure corresponds to the rate-region achievable by standard SIC, whereas the pale blue (bright shaded) area is the additional rate-region obtained by successive IF. Note that the plotted rate-region does not include time-sharing.

to the fine lattice and reduces the result modulo the coarse lattice. This is in contrast to the ML decoder that computes the likelihood of each possible outcome for the desired integer-linear combination given the channel's output, and chooses the one that is most likely. The achievable rates described by Theorem 2 are attained using the same decoder as in [2] at each decoding step (after noise prediction was applied). It is shown that the obtained sum-rate equals the MAC's sum-capacity. If the ML decoder could attain higher rates, than using the noise prediction scheme described in this section, with the ML decoder instead of the one from [2], higher rates could be obtained, contradicting the converse theorem for the MAC capacity region. We emphasize that this only shows that the decoder of [2] achieves the highest possible rate for *the described transmission scheme*, where each user transmits a dithered version of a lattice point taken from a chain of nested lattice codebook. Our results do not preclude the possibility that integer-linear combinations can be reliably decoded with a higher computation rate than that of [2] under *a different transmission scheme*.

B. From mod- Λ decoding to decoding over the reals

Successive IF uses the values of the effective noise vectors $\mathbf{z}_{\text{eff},1}, \dots, \mathbf{z}_{\text{eff},m-1}$ in order to estimate $\mathbf{z}_{\text{eff},m}$ and reduce its effective variance. However, correct decoding of the equation \mathbf{v}_k from $\mathbf{y}_{\text{eff},k} = [\mathbf{v}_k + \mathbf{z}_{\text{eff},k}] \bmod \Lambda_c$ only ensures that the receiver has access to $[\mathbf{z}_{\text{eff},k}] \bmod \Lambda_c$, whereas for the successive IF scheme $\mathbf{z}_{\text{eff},k}$ is needed. Correct decoding of \mathbf{v}_k from $\mathbf{y}_{\text{eff},k}$ only implies that $[\mathbf{z}_{\text{eff},k}] \bmod \Lambda_c \in \mathcal{V}_f$, but does not necessarily imply that $\mathbf{z}_{\text{eff},k} \in \mathcal{V}_f$. If the fine lattice Λ_f used for constructing \mathcal{C} is Poltyrev-good and Λ_c is Rogers-

good [18], we have

$$\Pr(\mathbf{z}_{\text{eff},k} \notin \mathcal{V}_f) < 2^{-n \left(\frac{1}{2} \log \left(\frac{\text{SNR}}{\sigma_{\text{eff},k}^2} \right) - R - o_1(n) \right)}, \quad (21)$$

and since $\mathcal{V}_f \subset \mathcal{V}_c$ the probability that $[\mathbf{z}_{\text{eff},k}] \bmod \Lambda_c \neq \mathbf{z}_{\text{eff},k}$ can be made arbitrarily small by increasing the block length n . In (19) we assumed that Λ_f is Poltyrev-good and Λ_c is Rogers-good to obtain the relation $[\mathbf{z}_{\text{eff},k}] \bmod \Lambda_c \stackrel{w.h.p.}{=} \mathbf{z}_{\text{eff},k}$.

In practice, however, a “good” nested lattice codebook is hard to implement, and suboptimal nested lattice codebooks are constructed. A commonly used construction for a nested lattice codebook is one where the fine lattice is built from a linear code of block length n over a prime field \mathbb{Z}_p with moderate cardinality (e.g., an LDPC code or a turbo code) using Construction A [19], [20], and the coarse lattice is the scaled integer-lattice $p\mathbb{Z}^n$. In this case, although $\Pr([\mathbf{z}_{\text{eff},k}] \bmod \Lambda_c \notin \mathcal{V}_f)$ can be made as small as desired for n large enough and an appropriate choice of R , $\Pr([\mathbf{z}_{\text{eff},k}] \bmod \Lambda_c \neq \mathbf{z}_{\text{eff},k})$ cannot be made arbitrarily small, as Λ_c is the scaled integer lattice whose Euclidean minimum distance does not increase with n . In other words, Λ_f is not Poltyrev good. Thus, for construction A nested lattice codebooks, correct decoding of \mathbf{v}_k does not ensure correct decoding of $\mathbf{z}_{\text{eff},k}$. This may degrade the performance of successive IF, as the predictions of subsequent effective noises may also be impaired.

Nevertheless, we claim that for moderate (not too small) rates of the codebook \mathcal{C} , this type of error will have a negligible effect on the total error probability. It can be shown that for a Construction A nested lattice codebook, if R is such that \mathbf{v}_k can be decoded reliably from $\mathbf{y}_{\text{eff},k}$, then

$$\Pr([\mathbf{z}_{\text{eff},k}(i)] \bmod p \neq \mathbf{z}_{\text{eff},k}(i)) < \exp \left\{ -\frac{\pi e}{4} 2^{2R} \right\}$$

for each of the n components of $\mathbf{z}_{\text{eff},k}$. Thus, the expected number of components where $[\mathbf{z}_{\text{eff},k}] \bmod p \neq \mathbf{z}_{\text{eff},k}$ is fairly small for moderate R , and these erroneous components will not degrade the performance of successive IF by much.

IV. FINDING THE OPTIMAL INTEGER-VALUED MATRIX \mathbf{A}

Thus far, we have described the successive IF scheme for some predefined integer-valued matrix \mathbf{A} . The performance of IF, as well as successive IF, critically depends on the choice of \mathbf{A} and we now discuss a procedure for finding its optimal value.

We would like to find the matrix \mathbf{A} that maximizes the computation rate for the worst equation when noise prediction is used. Mathematically, this problem can be formulated as

$$\mathbf{A}_{\text{S-IF}}^{\text{opt}} = \arg \min_{\substack{\mathbf{A} \in \mathbb{Z}^{M \times M} \\ \det(\mathbf{A}) \neq 0}} \max_{k=1, \dots, M} \ell_{kk}^2, \quad (22)$$

where ℓ_{kk} are the diagonal entries of the lower triangular matrix \mathbf{L} defined in (16). Note that this problem is different than the optimization problem for standard IF, which can be

written as

$$\mathbf{A}_{\text{IF}}^{\text{opt}} = \arg \min_{\substack{\mathbf{A} \in \mathbb{Z}^{M \times M} \\ \det(\mathbf{A}) \neq 0}} \max_{k=1, \dots, M} \sum_{i=1}^k \ell_{ik}^2. \quad (23)$$

As a result, the solution of (22) may be different that that of (23). We now show that for successive IF we can restrict \mathbf{A} to the class of unimodular matrices (matrices with integer entries and determinant ± 1) without loss of generality, and its optimal value can be obtained using the Korkin-Zolotarev basis reduction procedure.

Definition 3 (Korkin-Zolotarev basis [21]): Let

$\mathbf{F} = [\mathbf{f}_1 \ \dots \ \mathbf{f}_M]$ be a lattice basis of rank M , and let $\mathbf{F}^* = [\mathbf{f}_1^* \ \dots \ \mathbf{f}_M^*]$ be its corresponding Gram-Schmidt orthogonalization, i.e., $\mathbf{F} = \mathbf{F}^* \cdot \mathbf{R}$ for some upper triangular matrix \mathbf{R} with unit diagonal. Define the projection functions $\mathcal{P}_i(\mathbf{x}) = \sum_{j \geq i} (\mathbf{x}^T \mathbf{f}_j^* / \|\mathbf{f}_j^*\|^2) \mathbf{f}_j^*$ that project \mathbf{x} onto $\text{span}(\mathbf{f}_i^*, \dots, \mathbf{f}_M^*)$. The basis \mathbf{F} is Korkin-Zolotarev (KZ) reduced if and only if for all $i = 1, \dots, M$

- \mathbf{f}_i^* is a shortest nonzero vector in $\mathcal{P}_i(\Lambda(\mathbf{F}))$
- for all $j > i$, the Gram-Schmidt coefficients $r_{j,i} = \mathbf{f}_j^T \mathbf{f}_i^* / \|\mathbf{f}_i^*\|^2$ of \mathbf{F} satisfy $|r_{j,i}| \leq 1/2$.

Theorem 3: Let \mathbf{G} be defined as in (6) and let \mathbf{A} be a unimodular matrix. If $\mathbf{G}^T \mathbf{A}^T$ is a KZ basis of the lattice $\Lambda(\mathbf{G}^T) \triangleq \{\mathbf{G}^T \mathbf{x} : \mathbf{x} \in \mathbb{Z}^M\}$ then \mathbf{A} is an optimal integer-valued matrix for successive IF.

Proof: Let \mathbf{A} be a unimodular matrix such that $\mathbf{G}^T \mathbf{A}^T$ is a KZ basis of the lattice $\Lambda(\mathbf{G}^T)$. Such a matrix always exists [21]. Let \mathbf{a}_i^T be the i th row of \mathbf{A} , and let \mathbf{L} be the lower triangular matrix defined in (16). Note that ℓ_{ii} depends only on $\{\mathbf{a}_1, \dots, \mathbf{a}_i\}$, and is independent of $\{\mathbf{a}_{i+1}, \dots, \mathbf{a}_M\}$.

We first show that out of all integer-valued vectors that are linearly independent of $\{\mathbf{a}_1, \dots, \mathbf{a}_{i-1}\}$, \mathbf{a}_i yields the minimum value of ℓ_{ii}^2 . Let $\mathbf{F} = [\mathbf{f}_1 \ \dots \ \mathbf{f}_M] = \mathbf{G}^T \mathbf{A}^T$ and let $\mathbf{F}^* = [\mathbf{f}_1^* \ \dots \ \mathbf{f}_M^*]$ be the corresponding Gram-Schmidt orthogonalized basis, such that $\mathbf{F} = \mathbf{F}^* \cdot \mathbf{R}$ for an upper triangular matrix \mathbf{R} with unit diagonal. We further define the unitary matrix $\mathbf{U} \triangleq \mathbf{F}^* \cdot \text{diag}(\|\mathbf{f}_1^*\|^{-1}, \dots, \|\mathbf{f}_M^*\|^{-1})$ and the upper triangular matrix $\mathbf{L}^T \triangleq \text{diag}(\|\mathbf{f}_1^*\|, \dots, \|\mathbf{f}_M^*\|) \cdot \mathbf{R}$, such that $\mathbf{F} = \mathbf{U} \mathbf{L}^T$ and

$$\mathbf{F}^T \mathbf{F} = \mathbf{A} \mathbf{G}^T \mathbf{A}^T = \mathbf{L} \mathbf{L}^T.$$

From the uniqueness of the Cholesky decomposition, it follows that the \mathbf{L} defined above is the same as in (16). Define the projection functions $\mathcal{P}_i(\mathbf{x}) = \sum_{j \geq i} (\mathbf{x}^T \mathbf{f}_j^* / \|\mathbf{f}_j^*\|^2) \mathbf{f}_j^*$ that project \mathbf{x} onto $\text{span}(\mathbf{f}_i^*, \dots, \mathbf{f}_M^*)$. We have

$$\ell_{ii}^2 = \|\mathbf{f}_i^*\|^2 = \|\mathcal{P}_i(\mathbf{f}_i)\|^2 = \|\mathcal{P}_i(\mathbf{G}^T \mathbf{a}_i)\|^2. \quad (24)$$

By definition of the KZ reduction, $\mathcal{P}_i(\mathbf{G}^T \mathbf{a}_i)$ is a shortest nonzero vector in $\mathcal{P}_i(\Lambda(\mathbf{G}^T))$, which means that

$$\mathbf{a}_i = \arg \min_{\substack{\mathbf{a} \in \mathbb{Z}^M \\ \text{rank}(\mathbf{a}_1, \dots, \mathbf{a}_{i-1}, \mathbf{a}) = i}} \|\mathcal{P}_i(\mathbf{G}^T \mathbf{a})\|^2 = \arg \min_{\substack{\mathbf{a} \in \mathbb{Z}^M \\ \text{rank}(\mathbf{a}_1, \dots, \mathbf{a}_{i-1}, \mathbf{a}) = i}} \ell_{ii}^2, \quad (25)$$

as desired, where the last equality follows from (24).

To establish the optimality of \mathbf{A} for successive IF, it remains to show that a greedy procedure that for each i selects the \mathbf{a}_i as in (25) also minimizes the value of $\max_{k=1,\dots,M} \ell_{kk}^2$. Let $\tilde{\mathbf{A}} = [\tilde{\mathbf{a}}_1 \ \dots \ \tilde{\mathbf{a}}_M]$ be a ‘‘competing’’ full-rank matrix with integer-valued entries. Define the matrix $\tilde{\mathbf{F}} = [\tilde{\mathbf{f}}_1 \ \dots \ \tilde{\mathbf{f}}_M] = \mathbf{G}^T \tilde{\mathbf{A}}$ and define the matrix $\tilde{\mathbf{L}}$ as the lower triangular matrix in the Cholesky decomposition of $\tilde{\mathbf{F}}^T \tilde{\mathbf{F}}$, i.e., $\tilde{\mathbf{F}}^T \tilde{\mathbf{F}} = \tilde{\mathbf{L}} \tilde{\mathbf{L}}^T$. For the choice \mathbf{A} , the achievable rate for successive IF is dictated by $\max_{k=1,\dots,M} \ell_{kk}^2$, where ℓ_{kk} are the diagonal entries of $\tilde{\mathbf{L}}$. Let $\tilde{\mathbf{F}}^* = [\tilde{\mathbf{f}}_1^* \ \dots \ \tilde{\mathbf{f}}_M^*]$ be the Gram-Schmidt orthogonalized basis corresponding to $\tilde{\mathbf{F}}$ and define the projection functions $\tilde{\mathcal{P}}_i(\mathbf{x}) = \sum_{j \geq i} (\mathbf{x}^T \tilde{\mathbf{f}}_j^* / \|\tilde{\mathbf{f}}_j^*\|^2) \tilde{\mathbf{f}}_j^*$ that project \mathbf{x} onto $\text{span}(\tilde{\mathbf{f}}_i^*, \dots, \tilde{\mathbf{f}}_M^*)$. Note that we have $\tilde{\ell}_{ii}^2 = \|\tilde{\mathcal{P}}_i(\mathbf{G}^T \tilde{\mathbf{a}}_i)\|^2$.

In order to prove that \mathbf{A} is optimal, we show by induction that for each $m = 1, \dots, M$

$$\max_{k=1,\dots,m} \ell_{kk}^2 \leq \max_{k=1,\dots,m} \tilde{\ell}_{kk}^2. \quad (26)$$

The induction hypothesis (26) holds for $m = 1$ since $\ell_{11}^2 = \|\mathbf{f}_1\|^2$, and by definition of the KZ reduction \mathbf{f}_1 is a shortest vector in $\Lambda(\mathbf{G}^T)$. We assume (26) holds for $m - 1$ and show that it also holds for m . We have

$$\begin{aligned} \max_{k=1,\dots,m} \ell_{kk}^2 &= \max \left(\ell_{mm}^2, \max_{k=1,\dots,m-1} \ell_{kk}^2 \right) \\ &\leq \max \left(\ell_{mm}^2, \max_{k=1,\dots,m-1} \tilde{\ell}_{kk}^2 \right) \\ &= \max \left(\|\mathcal{P}_m(\mathbf{G}^T \mathbf{a}_m)\|^2, \max_{k=1,\dots,m-1} \tilde{\ell}_{kk}^2 \right) \end{aligned} \quad (27)$$

$$(28)$$

where (27) follows from the induction hypothesis.

If $\text{span}(\mathbf{a}_1, \dots, \mathbf{a}_{m-1}) = \text{span}(\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_{m-1})$ we have $\|\mathcal{P}_m(\mathbf{x})\| = \|\tilde{\mathcal{P}}_m(\mathbf{x})\|$ for any $\mathbf{x} \in \mathbb{R}^M$. Therefore,

$$\|\mathcal{P}_m(\mathbf{G}^T \mathbf{a}_m)\|^2 \leq \|\mathcal{P}_m(\mathbf{G}^T \tilde{\mathbf{a}}_m)\|^2 = \|\tilde{\mathcal{P}}_m(\mathbf{G}^T \tilde{\mathbf{a}}_m)\|^2 = \tilde{\ell}_{mm}^2, \quad (29)$$

where the first inequality follows from the definition of the KZ reduction. Substituting (29) into (28) gives (26).

If $\text{span}(\mathbf{a}_1, \dots, \mathbf{a}_{m-1}) \neq \text{span}(\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_{m-1})$, let j be the smallest index for which $\tilde{\mathbf{a}}_j \notin \text{span}(\mathbf{a}_1, \dots, \mathbf{a}_{m-1})$. It follows that $\text{span}(\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_{j-1}) \subset \text{span}(\mathbf{a}_1, \dots, \mathbf{a}_{m-1})$ and therefore $\|\mathcal{P}_m(\mathbf{x})\| \leq \|\tilde{\mathcal{P}}_j(\mathbf{x})\|$ for any $\mathbf{x} \in \mathbb{R}^M$. We have

$$\|\mathcal{P}_m(\mathbf{G}^T \mathbf{a}_m)\|^2 = \min_{\substack{\mathbf{a} \in \mathbb{Z}^m \\ \text{rank}(\mathbf{a}_1, \dots, \mathbf{a}_{m-1}, \mathbf{a})=m}} \|\mathcal{P}_m(\mathbf{G}^T \mathbf{a})\|^2 \quad (30)$$

$$\leq \|\mathcal{P}_m(\mathbf{G}^T \tilde{\mathbf{a}}_j)\|^2 \quad (31)$$

$$\leq \|\tilde{\mathcal{P}}_j(\mathbf{G}^T \tilde{\mathbf{a}}_j)\|^2 \quad (32)$$

$$= \tilde{\ell}_{jj}^2, \quad (33)$$

where (30) follows from (25), (31) follows since $\tilde{\mathbf{a}}_j \notin \text{span}(\mathbf{a}_1, \dots, \mathbf{a}_{m-1})$ and is therefore included in the minimization space, and (32) follows since $\|\mathcal{P}_m(\mathbf{x})\| \leq \|\tilde{\mathcal{P}}_j(\mathbf{x})\|$ for any $\mathbf{x} \in \mathbb{R}^M$. Substituting (33) into (28) gives (26). ■

It is well known [21], and not too difficult to verify, that if a linearly independent set of lattice vectors $\mathbf{S} = [\mathbf{s}_1 \ \dots \ \mathbf{s}_M]$ is KZ reduced, then \mathbf{S} is a basis for the original lattice. For this reason, in contrast to standard IF where the optimal \mathbf{A} is not necessarily unimodular, for successive IF there is no loss (in terms of achievable rate) in restricting \mathbf{A} to the class of unimodular matrices. It follows that for uncoded PAM transmission (or equivalently using the $1 - D$ integer lattice as codebook), successive IF and lattice-reduction (LR) aided SIC [22] are in fact equivalent. Although the advantages of the KZ reduction for lattice-reduction-aided SIC were pointed out in the literature [23], to the best of our knowledge, there is no prior work on its optimality in terms of minimizing the error probability.

Finding a KZ basis for a lattice is known to be NP-hard in general, as it involves finding a shortest lattice vector, which is itself NP-hard. The following is a recursive procedure for finding a KZ basis $\mathbf{F} = [\mathbf{f}_1 \ \dots \ \mathbf{f}_M]$ for a rank M lattice Λ . Let \mathbf{f}_1 be a shortest vector in Λ , and let Λ' be the lattice given by the orthogonal projection of Λ on the subspace of $\text{span}(\Lambda)$ orthogonal to \mathbf{f}_1 (it can be verified that Λ' is indeed a lattice). Let $\mathbf{c}_2, \dots, \mathbf{c}_M$ be the KZ basis of Λ' . Define $\mathbf{f}_i = \mathbf{c}_i + \alpha_i \mathbf{f}_1$, where $\alpha_i \in (-1/2, 1/2]$ is the unique number such that $\mathbf{f}_i \in \Lambda$, for $i = 2, \dots, M$.

For channels of small dimensions the KZ basis can be computed exactly. For large dimensions, it can be approximated by applying the LLL algorithm M successive times, where the dimension of the lattice for which LLL is applied decreases at each iteration. Such an algorithm is described in [24, Section VI.D], and Matlab code for finding an approximation for the optimal \mathbf{A} based on this method can be found in [25].

APPENDIX A SUCCESSIVE IF VIA MMSE-GDFE

In Section III, we described the implementation of successive IF via noise-prediction. In this appendix, we show an equivalent implementation of successive IF where the decoded equations themselves, instead of the effective noises, are used for improving the achievable rates for decoding subsequent equations. As for successive IF via noise-prediction, the derivation relies on linear MMSE estimation theory, and in particular on the MMSE-GDFE framework.

A key fact used in the derivation is that if a certain equation $\mathbf{v} = [\mathbf{a}^T \mathbf{T}] \bmod \Lambda_c$ can be decoded from \mathbf{Y} , then with high probability $\mathbf{a}^T \mathbf{X}$ can also be recovered from \mathbf{Y} . This fact is proved in [11, Lemma 1], and follows from the same considerations discussed in Section III-B. Therefore, when attempting to decode the equation $\mathbf{v}_k = [\mathbf{a}_k^T \mathbf{T}] \bmod \Lambda_c$, the receiver already has access to $\mathbf{a}_1^T \mathbf{X}, \dots, \mathbf{a}_{k-1}^T \mathbf{X}$. Thus, for any lower-triangular matrix \mathbf{C} with diagonal entries equal to zero, the successive IF receiver can produce the effective channel

$$\begin{aligned} \mathbf{Y}_{\text{eff}} &= [\mathbf{B}\mathbf{Y} - \mathbf{C}\mathbf{A}\mathbf{X} + \mathbf{A}\mathbf{D}] \bmod \Lambda_c \\ &= [\mathbf{A}\mathbf{T} + (\mathbf{B}\mathbf{H} - \mathbf{A} - \mathbf{C}\mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z}] \bmod \Lambda_c \\ &= [\mathbf{V} + \mathbf{E}] \bmod \Lambda_c, \end{aligned} \quad (34)$$

where

$$\mathbf{E} \triangleq (\mathbf{B}\mathbf{H} - \mathbf{R}\mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z} \quad (35)$$

is statistically independent of \mathbf{T} , and $\mathbf{R} \triangleq \mathbf{I} + \mathbf{C}$. Note that the constrained structure of \mathbf{C} ensures that in all steps of the successive decoding procedure the receiver only uses values of $\mathbf{a}_i^T \mathbf{X}$ that are already available to it. The filter matrix \mathbf{R} is monic, i.e., a lower-triangular matrix with unit diagonal entries, and together with \mathbf{B} can be optimized such as to minimize the generalized covariance matrix $\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}}$. For a given choice of \mathbf{R} , the filter \mathbf{B} should be chosen as the optimal linear MMSE estimation filter of $\mathbf{R}\mathbf{A}\mathbf{X}$ from \mathbf{Y} , which is given by

$$\mathbf{B} = \mathbf{R}\mathbf{A}\mathbf{H}^T \left(\frac{1}{\text{SNR}}\mathbf{I} + \mathbf{H}\mathbf{H}^T \right)^{-1},$$

and the resulting estimation-error generalized covariance matrix is

$$\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}} = \text{SNR} \cdot (\mathbf{R}\mathbf{A}) (\mathbf{I} + \text{SNR}\mathbf{H}^T\mathbf{H})^{-1} (\mathbf{R}\mathbf{A})^T. \quad (36)$$

Comparing (36) to the estimation error covariance matrix obtained in standard IF

$$\text{SNR} \cdot \mathbf{A} (\mathbf{I} + \text{SNR}\mathbf{H}^T\mathbf{H})^{-1} \mathbf{A}^T$$

reveals the advantage of successive IF over standard IF. It essentially allows to decode any full rank-set of equations of the form $\mathbf{R}\mathbf{A}\mathbf{X}$, where \mathbf{R} is some monic filter, rather than just equations of the form $\mathbf{A}\mathbf{X}$.

Recall that the performance of the IF receiver are dictated by the effective variances of the effective noises, i.e., by the diagonal entries of $\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}}$. Thus, for a given choice of \mathbf{A} , \mathbf{R} should be chosen such as to minimize the values of these entries. Note that,

$$\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}} = \text{SNR} \cdot (\mathbf{R}\mathbf{L})(\mathbf{R}\mathbf{L})^T,$$

where \mathbf{L} is the lower triangular matrix defined in (16). The i th diagonal entry of $\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}}$ is therefore equal to SNR times the squared Euclidean norm of the i th row in the matrix $\mathbf{R}\mathbf{L}$. Now, since \mathbf{R} is monic, we must have $\{\mathbf{R}\mathbf{L}\}_{ii} = \ell_{ii}$, which implies that

$$\left\{ \tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}} \right\}_{ii} \geq \text{SNR} \ell_{ii}^2, \quad \forall i = 1, \dots, M. \quad (37)$$

The choice

$$\mathbf{R} = \text{diag}(\ell_{11}, \dots, \ell_{MM})\mathbf{L}^{-1}, \quad (38)$$

attains the bound from (37), and is therefore optimal. The resulting estimation-error generalized covariance matrix is

$$\tilde{\mathbf{K}}_{\mathbf{E}\mathbf{E}} = \text{SNR} \cdot \text{diag}(\ell_{11}^2, \dots, \ell_{MM}^2),$$

and as a result the achievable rates are exactly as in Theorem 1, which shows that successive IF via noise-prediction or via MMSE-GDFE are indeed equivalent.

REFERENCES

- [1] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," *IEEE Transactions on Information Theory*, Submitted Jan. 2012, see <http://arxiv.org/abs/1003.5966>.
- [2] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.
- [3] O. Ordentlich and U. Erez, "Precoded integer-forcing universally achieves the MIMO capacity to within a constant gap," *IEEE Transactions on Information Theory*, Submitted Apr. 2013, see <http://arxiv.org/abs/1301.6393>.
- [4] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric Gaussian K -user interference channel," *IEEE Trans. Information Theory*, Submitted May 2012, see <http://arxiv.org/abs/1206.0197>.
- [5] T. Philosof, R. Zamir, U. Erez, and A. J. Khisti, "Lattice strategies for the dirty multiple access channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5006–5035, Aug. 2011.
- [6] G. Bresler, A. Parekh, and D. Tse, "The approximate capacity of the many-to-one and one-to-many Gaussian interference channels," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4566–4592, Sept. 2010.
- [7] M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Transactions on Information Theory*, vol. 11, no. 56, pp. 5641–5654, Nov. 2010.
- [8] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the Gaussian two-way relay channel to within 1/2 bit," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5488–5494, Nov. 2010.
- [9] O. Ordentlich and U. Erez, "On the robustness of lattice interference alignment," *IEEE Transactions on Information Theory*, vol. 59, May 2013.
- [10] J. Zhan, B. Nazer, O. Ordentlich, U. Erez, and M. Gastpar, "Integer-forcing architectures for MIMO: Distributed implementation and SIC," in *Proceedings of the Forty Fourth Asilomar Conference on Signals, Systems and Computers*, Nov. 2010, pp. 322–326.
- [11] B. Nazer, "Successive compute-and-forward," in *Proceedings of the International Zurich Seminar on Communications (IZS 2012)*, Zurich, Switzerland, Mar. 2012.
- [12] M. Varanasi and T. Guess, "Optimum decision feedback multiuser equalization with successive decoding achieves the total capacity of the Gaussian multiple-access channel," in *Proceedings of the 31st Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Nov. 1997.
- [13] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585–595, Nov. - Dec. 1999.
- [14] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: Wiley-Interscience, 2006.
- [15] R. F. Fischer, *Precoding and Signal Shaping for Digital Transmission*. John Wiley and Sons, Inc., 2005.
- [16] D. A. Harville, *Matrix Algebra From a Statistician's Perspective*. New York, NY: Springer-Verlag, 1997.
- [17] J. Cioffi, G. Dudevoir, M. Vedat Eyuboglu, and J. Forney, G.D., "MMSE decision-feedback equalizers and coding. I. equalization results," *IEEE Transactions on Communications*, vol. 43, Oct. 1995.
- [18] U. Erez and R. Zamir, "Achieving $\frac{1}{2} \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.
- [19] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1988.
- [20] H.-A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1767–1773, Nov. 1997.
- [21] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. Cambridge, UK: Kluwer Academic Publishers, 2002, vol. 671 of The Kluwer International International Series in Engineering and Computer Science.
- [22] D. Wubben, R. Bohnke, V. Kuhn, and K. D. Kammeyer, "Near-maximum-likelihood detection of MIMO systems using MMSE-based lattice reduction," in *IEEE International Conference on Communications*, vol. 2, Paris, France, June 2004, pp. 798 – 802.

- [23] C. Ling, "On the proximity factors of lattice reduction-aided decoding," *IEEE Transactions on Signal Processing*, vol. 59, no. 6, pp. 2795–2808, June 2011.
- [24] 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.
- [25] <http://www.eng.tau.ac.il/~ordent/publications/IFsic.m>.