Lattice-Reduction-Aided Precoding for Coded Modulation over Algebraic Signal Constellations

Sebastian Stern and Robert F.H. Fischer
Institute of Communications Engineering, Ulm University, Ulm, Germany
Email: {sebastian.stern, robert.fischer}@uni-ulm.de

***Abstract*—Lattice-reduction-aided preequalization or precoding are powerful techniques for handling the interference on the multiuser MIMO broadcast channel as the channel's diversity order can be achieved. However, recent advantages in the closely related field of integer-forcing equalization raise the question, if the unimodularity constraint on the integer equalization matrix in LRA schemes is really necessary or if it can be dropped, yielding an additional factorization gain. In this paper, so-called algebraic signal constellations are presented, where the unimodularity is not required anymore. Assuming complex-baseband transmission, particularly q-ary fields of Gaussian primes (complex integer lattice) and Eisenstein primes (complex hexagonal lattice) are considered. Given the signal constellation and the channel code in the same arithmetic over a finite field of order q, a coded modulation approach with straightforward soft-decision decoding metric is proposed. Moreover, LRA precoding over algebraic constellations and its advantages as opposed to LRA preequalization are discussed. The theoretical considerations in the paper are covered by means of numerical simulations.**

I. INTRODUCTION

In the field of multiuser multiple-input/multiple output (MIMO) communications, the principle of *lattice-reduction-aided* (LRA) equalization has gained significant interest as the respective schemes are able to achieve the diversity order of the multiuser MIMO channel [28]—in contrast to well-known traditional techniques like linear (pre-)equalization, decision-feedback-equalization (DFE) [10] or Tomlinson-Harashima precoding (THP) [29], [15], which have been adapted from the singleuser to the multiuser scenario [10], [7].

In LRA schemes, the equalization is performed in a *suited basis* w.r.t. the lattice described by the MIMO channel matrix. This is achieved by factorizing the channel matrix into an unimodular integer part and a "more suited" description of the lattice with basis vectors close to orthogonal and of small norm. This approach has first been presented for receiver-side equalization (multiple-access channel) [35] but could rapidly—via the uplink/downlink duality [31], [32]—be extended to downlink transmission (MIMO broadcast channel) [33], [34], [26].

Recently, inspired by so-called *compute-and-forward* [23], [17] or *integer-forcing* (IF) [36] schemes where the final resolution of the interference is performed over finite fields, the philosophy of LRA equalization has been considered from a modified perspective [25]: applying signal constellations with algebraic property [9], or more specifically, constellations which represent finite fields over the complex plane, the *shortest basis problem* present in LRA equalization is generalized to the *shortest independent vector problem*. This task, which is always given in IF equalization, drops the unimodularity constraint on the integer matrix. Fields of Gaussian primes [19], [1], [3] (complex integer lattice) or Eisenstein primes [3], [27], [30] (complex hexagonal lattice) are suited algebraic structures [25], not only providing the desired finite-field property, but also directly yielding the precoding lattice or modulo operation inherently accompanied by LRA preequalization or precoding.

In this paper, the approach of applying algebraic signal constellations for LRA preequalization over the MIMO broadcast channel as proposed in [25] is reviewed and extended. This includes a factorization according to the shortest independent vector problem and the assessment of the achievable factorization gain. A coded modulation approach where both the channel code and the signal constellation operate over the same arithmetic, specifically a finite field of order q, is presented and implemented via non-binary q-ary LDPC codes. Moreover, the LRA linear preequalization in [25] is replaced by (Tomlinson-Harashima-type) LRA precoding and its advantages w.r.t. signal properties and resulting transmission performance are discussed.

The paper is organized as follows: In Sec. II, the system model of coded modulation in combination with LRA preequalization or precoding for the MIMO broadcast channel is given. Sec. III details the aspects of LRA encoding over algebraic constellations, coded modulation over these constellations and the advantages of precoding instead of preequalization. Numerical results are provided in Sec. IV. The paper closes with a summary and outlook in Sec. V.

II. SYSTEM MODEL

A discrete-time complex baseband multiuser MIMO broadcast channel is considered. At the transmitter-side, a joint processing is present to supply N_{R} non-cooperating single-antenna users via $N_{\mathrm{T}} \geq N_{\mathrm{R}}$ transmit antennas. The system model of LRA precoding in combination with (soft-decision) channel coding is depicted in Fig. 1.

A. Transmitter-Side Processing

Source information symbols i_u are transmitted to user $u = 1, \dots, N_{\mathrm{R}}$. Since usually bits are communicated, we restrict

This work was supported by Deutsche Forschungsgemeinschaft (DFG) within the framework COIN under grant FI 982/4-3.

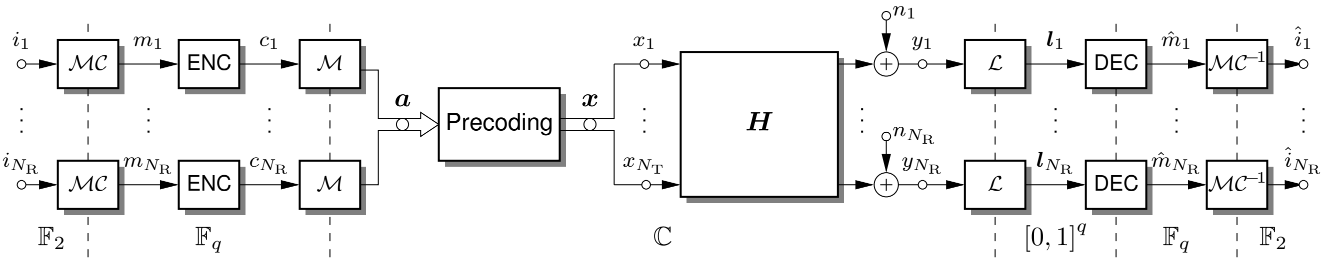

Fig. 1. System model of LRA precoding (transmitter- and receiver-side processing) for the MIMO broadcast channel with N_T transmit antennas and N_R single-antenna users in combination with soft-decision channel coding.

to the binary case ($i_u \in \mathbb{F}_2$). For each time step, the symbols are summarized in the vector $\boldsymbol{i} = [i_1, \dots, i_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{F}_2^{N_\mathrm{R}}$.

If the source and channel coding do not share the same arithmetic, i.e., the channel code is represented over a field $\mathbb{F}_q = \{\varphi_1, \dots, \varphi_q\}$ with $q \neq 2$, a *modulus conversion* (denoted as $\mathcal{MC}$) has to be applied [12], [10], [25]: a block of serial μ source symbols $\in \mathbb{F}_2$ is converted to a block of ν message symbols $\in \mathbb{F}_q$ ($q^\nu \geq 2^\mu$). These symbols are combined in $\boldsymbol{m} = [m_1, \dots, m_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{F}_q^{N_\mathrm{R}}$.

Subsequently, performing the channel encoding (ENC), k_c (serial) message symbols are encoded to a codeword of length n_c via a $k_\mathrm{c} \times n_\mathrm{c}$ generator matrix $\boldsymbol{G}_\mathrm{c}$ of a linear block code (rate $R_\mathrm{c} \stackrel{\text{def}}{=} k_\mathrm{c}/n_\mathrm{c}$), yielding the vector of encoded messages $\boldsymbol{c} = [c_1, \dots, c_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{F}_q^{N_\mathrm{R}}$. All users are assumed to have the same code properties (length, rate, and code class).

Given the encoded symbols, a predefined mapping $\mathcal{M} : c \in \mathbb{F}_q \to a \in \mathcal{A}$ to the data symbols is performed, where $\mathcal{A} \subset \mathbb{C}$ denotes a zero-mean signal constellation with cardinality $M \stackrel{\text{def}}{=} |\mathcal{A}|$ and variance σ_a^2.

The vector of data symbols $\boldsymbol{a} = [a_1, \dots, a_{N_\mathrm{R}}]^\mathsf{T} \in \mathcal{A}^{N_\mathrm{R}}$ is finally precoded to a vector of transmit symbols $\boldsymbol{x} = [x_1, \dots, x_{N_\mathrm{T}}]^\mathsf{T} \in \mathbb{C}^{N_\mathrm{T}}$ that are radiated from the antennas (sum-power constraint $N_\mathrm{T}\sigma_x^2 = N_\mathrm{R}\sigma_a^2$, where σ_x^2 is the transmit symbols' variance). The process of precoding will further be explained in Sec. III.

B. Channel Model

The MIMO broadcast channel is expressed by

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{n} \; . \tag{1}$$

The $N_\mathrm{R} \times N_\mathrm{T}$ channel matrix $\boldsymbol{H}$ is assumed to have i.i.d. complex Gaussian zero-mean unit-variance coefficients. A block-fading channel is assumed, i.e., the channel matrix is constant over a block of n_c symbols (block length of the channel code). The vector $\boldsymbol{n} = [n_1, \dots, n_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{C}^{N_\mathrm{R}}$ represents the additive white noise present at each receiver. It is assumed to be i.i.d. zero-mean complex Gaussian with variance σ_n^2. Finally, $\boldsymbol{y} = [y_1, \dots, y_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{C}^{N_\mathrm{R}}$ denotes the vector of receive symbols.

The signal-to-noise ratio (SNR) is expressed as transmitted energy *per bit* in relation to the noise power spectral density N_0, given by

$$\frac{E_\mathrm{b,TX}}{N_0} = \frac{\sigma_a^2}{\sigma_n^2 \log_2(R_\mathrm{c} q_\mathrm{s} \mu/\nu)} \; . \tag{2}$$

C. Receiver-Side Processing

At the receiver side, each user u, $u = 1, \dots, N_\mathrm{R}$, calculates a metric for soft-decision decoding from its incoming signal y_u (metric calculation denoted as $\mathcal{L}$). It is represented as q-dimensional vector $\boldsymbol{l}_u = [l_{u,1}, \dots, l_{u,q}]$ per time step. Thereby, $l_{u,\rho} \stackrel{\text{def}}{=} \Pr\{c_u = \varphi_\rho \,|\, y_u\}$, $\rho = 1, \dots, q$, i.e., $\boldsymbol{l}_u$ is a probability mass function (pmf) of the encoded message at the transmitter side w.r.t. all possible elements $\varphi_\rho \in \mathbb{F}_q$.

Using the metric, a soft-decision decoding (DEC) is performed. The resulting decoded messages are denoted as $\hat{\boldsymbol{m}} = [\hat{m}_1, \dots, \hat{m}_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{F}_q^{N_\mathrm{R}}$.

In a final step, inverse modulus conversion is applied to obtain the estimated initial information symbols (blocks of ν message symbols are converted to blocks of μ source symbols). This yields the vector $\hat{\boldsymbol{i}} = [\hat{i}_1, \dots, \hat{i}_{N_\mathrm{R}}]^\mathsf{T} \in \mathbb{F}_2^{N_\mathrm{R}}$.

III. LRA Precoding for Coded Modulation over Algebraic Signal Constellations

In order to handle the multiuser interference present on the MIMO broadcast channel, both LRA preequalization and (Tomlinson-Harashima-type) precoding share the principle of performing the interference cancellation in a *suited basis*, i.e., a change in basis is realized to reduce the related increase in transmit power. The optimal solution is found by solving a *shortest basis problem* [33], [34]. In the following, the basic idea behind LRA schemes is reviewed.

Solving the shortest basis problem is equivalent to a factorization of the channel matrix. More precisely, a factorization of the augmented channel matrix [11]

$$\bar{\boldsymbol{H}} = \begin{bmatrix}\boldsymbol{H} & \sqrt{\zeta}\boldsymbol{I}\end{bmatrix}_{N_\mathrm{R} \times (N_\mathrm{R}+N_\mathrm{T})} = \boldsymbol{Z}\bar{\boldsymbol{H}}_\mathrm{red} \tag{3}$$

is performed, where $\bar{\boldsymbol{H}}_\mathrm{red}$ denotes the augmented reduced channel matrix, $\boldsymbol{I}$ the identity matrix and $\zeta = \sigma_n^2/\sigma_a^2$. $\boldsymbol{Z}$ is an integer matrix w.r.t. the given signal point lattice $\boldsymbol{\Lambda}_\mathrm{a}$ [10], [25] (signal grid of $\mathcal{A}$) which has to be unimodular ($|\det(\boldsymbol{Z})| = 1$) for the existence of an inverse integer matrix $\boldsymbol{Z}^{-1}$.

Given the channel factorization, the LRA preequalization can be performed as depicted in Fig. 2: The LRA preequalization is realized by an integer equalization matrix

$$\boldsymbol{Z}_\mathrm{p} \stackrel{\text{def}}{=} \boldsymbol{P}\boldsymbol{Z}^{-1} \tag{4}$$

to obtain equalized symbols $\tilde{\boldsymbol{a}} = [\tilde{a}_1, \dots, \tilde{a}_{N_\mathrm{R}}]^\mathsf{T}$ from the data symbols $\boldsymbol{a}$. Thereby, $\boldsymbol{P}$ is a permutation matrix enabling an

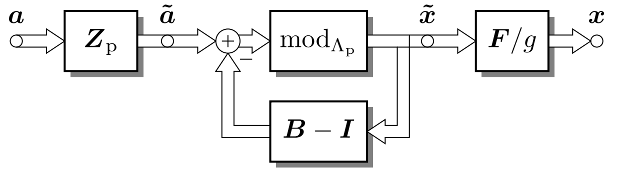

Fig. 2. Block diagramm of LRA preequalization (feedback part inactive, i.e., $\boldsymbol{B} = \boldsymbol{I}$) and precoding for the MIMO broadcast channel.

optimized precoding order among the data symbols (detailed below). Employing the component-wise modulo reduction

$$\mathrm{mod}_{\boldsymbol{\Lambda}_\mathrm{p}}(z) \stackrel{\text{def}}{=} z - \mathcal{Q}_{\boldsymbol{\Lambda}_\mathrm{p}}(z) \ , \quad z \in \mathbb{C} \ , \qquad (5)$$

where $\mathcal{Q}_{\boldsymbol{\Lambda}_\mathrm{p}}(\cdot)$ is the quantization to the predefined precoding lattice $\boldsymbol{\Lambda}_\mathrm{p}$ [10], [25], encoded symbols $\tilde{\boldsymbol{x}} = [\tilde{x}_1, \ldots, \tilde{x}_{N_\mathrm{R}}]^\mathsf{T}$ are created. In case of LRA precoding, this is done in a successive way as the interference from previously encoded symbols is canceled via feedback matrix $\boldsymbol{B}$ (for LRA preequalization: $\boldsymbol{B} = \boldsymbol{I}$). Noteworthy, due to the modulo reduction a *periodically extendable* constellation [10], [25]

$$\mathcal{A} \stackrel{\text{def}}{=} \mathcal{R}_\mathrm{V}(\boldsymbol{\Lambda}_\mathrm{p}) \cap \boldsymbol{\Lambda}_\mathrm{a} \qquad (6)$$

is required, where $\mathcal{R}_\mathrm{V}(\boldsymbol{\Lambda}_\mathrm{p})$ denotes the Voronoi region [10] of the precoding lattice. In the last step, the feedforward matrix $\boldsymbol{F}$ handles the remaining (non-integer) interference; the factor g ensures that the sum-power constraint is fulfilled when obtaining the vector of transmit symbols $\boldsymbol{x}$.

A. Unimodularity Constraint and Algebraic Constellations

Initially, for LRA preequalization and precoding, conventional square-QAM constellations have been employed [34]: utilizing the Gaussian integers $\mathbb{G}$ [1], [3] (i.e., the integer lattice in the complex plane) as the signal point lattice[1] $\boldsymbol{\Lambda}_\mathrm{a}$, the demanded property of a periodical extensibility can be provided by setting $\boldsymbol{\Lambda}_\mathrm{p} = \sqrt{M}\mathbb{G}$ [25], i.e., a scaled version of the signal point lattice (cf. (6)).

Quite recently, an alternative strategy [25] inspired by *integer-forcing* schemes [23], [17], [16], [36] was proposed: In IF, the integer interference is canceled over the arithmetic of a finite field, setting the requirement to have a signal constellation which can be represented as algebraic structure [9] over the complex numbers. In turn, the unimodularity constraint can be dropped, as $\boldsymbol{Z}^{-1}$ always exists over $\mathbb{F}_q$. Utilizing these structures in LRA equalization/precoding, the factorization according to (3) can be performed w.r.t. the *shortest independent vector problem*: neglecting the unimodularity constraint, a factorization gain may be achieved.

1) Fields of Gaussian Primes: Specifically, for the lattice $\mathbb{G}$, fields of *Gaussian primes* [1], [3] are convenient algebraic structures. A Gaussian prime is a Gaussian integer $\Theta = a + \mathrm{j}\, b$, $a, b \in \mathbb{Z}$, which fulfills the equation $\Theta\Theta^* = |\Theta|^2 = p$, where p is a real-valued prime and $\Theta^* = a - \mathrm{j}\, b$ denotes the complex conjugate of Θ. In particular, primes of the form[2] $\mathrm{rem}_4(p) = 1$, i.e., $p = 5, 13, 17, \ldots$ are suited. In addition, for real-valued primes of the form $\mathrm{rem}_4(p) = 3$, i.e., $p = 3, 7, 11, \ldots$, a related real-valued Gaussian prime is directly given by $\Theta = p$.

Choosing the precoding lattice as $\boldsymbol{\Lambda}_\mathrm{p} = \Theta\mathbb{G}$ [25], the respective zero-mean signal constellation $\mathcal{A}_\Theta^{(\mathbb{G})} \stackrel{\text{def}}{=} \mathcal{R}_\mathrm{V}(\Theta\mathbb{G}) \cap \mathbb{G}$ (cf. (6)) represents a finite field over $\mathbb{C}$. The constellation's cardinality always reads $M = |\Theta|^2$.

2) Fields of Eisenstein Primes: As an alternative choice of the signal point lattice, the Eisenstein integers $\mathbb{E}$ represent the hexagonal lattice over $\mathbb{C}$ ($\boldsymbol{\Lambda}_\mathrm{a} = \mathbb{E}$). By analogy to the Gaussian primes, *Eisenstein primes* [3], [27], [30] of the form $\Theta = a + \omega\, b$ can be found that fulfill $\Theta\Theta^* = p$. Thereby, $\omega = (-1 + \mathrm{j}\sqrt{3})/2 = \mathrm{e}^{\mathrm{j}2\pi/3}$ is the Eisenstein unit. In this case, $\mathrm{rem}_6(p) = 1$ has to hold for the real-valued prime p, i.e., $p = 7, 13, 19, \ldots$. When $\mathrm{rem}_3(p) = 2$ is fulfilled instead, i.e., for the case when $p = 2, 5, 11, \ldots$, real-valued Eisenstein primes of the form $\Theta = p$ are given.

Since the precoding lattice is now given as $\boldsymbol{\Lambda}_\mathrm{p} = \Theta\mathbb{E}$, where Θ is an Eisenstein prime, a zero-mean finite-field constellation is formed by $\mathcal{A}_\Theta^{(\mathbb{E})} \stackrel{\text{def}}{=} \mathcal{R}_\mathrm{V}(\Theta\mathbb{E}) \cap \mathbb{E}$. The cardinality again reads $M = |\Theta|^2$.

The use of Eisenstein constellations additionally enables a packing and shaping gain compared to the Gaussian prime ones [25]: due to the higher packing density of the signal points as well as the hexagonal shaping region $\mathcal{R}_\mathrm{V}(\Theta\mathbb{E})$ instead of the square one $\mathcal{R}_\mathrm{V}(\Theta\mathbb{G})$ the power efficiency is increased.

B. Coded Modulation over Algebraic Constellations

Utilizing the property of q-ary (complex-valued) fields of Gaussian and Eisenstein primes being isomorphic to $\mathbb{F}_q$ [19], [3], [25], a coded modulation approach is straightforward. Performing the channel coding over the finite field $\mathbb{F}_q$, the elements $\varphi_1, \ldots, \varphi_q$ are mapped to the q-ary constellation $\mathcal{A}_\Theta^{(\mathbb{G})} \simeq \mathbb{F}_q$ or $\mathcal{A}_\Theta^{(\mathbb{E})} \simeq \mathbb{F}_q$, respectively, where a natural mapping $\mathbb{F}_q \rightarrow \mathcal{A}_\Theta^{(\cdot)}$ via modulo reduction (5) can be used [25]. This strategy gives the possibility to operate in the same arithmetic for both channel coding and (integer) channel equalization (a precondition for the application of IF schemes).

Non-binary LDPC codes are a suitable code class for the above coded modulation strategy due to the possibility of soft-decision decoding via non-binary belief-propagation (BP) decoding over $\mathbb{F}_q$ [4] and the flexible code length (e.g., in contrast to Reed-Solomon codes).[3] In particular, the subclass of *irregular repeat-accumulate codes* [20] adapted to the non-binary case [22] is of interest, as the parity-check matrix $\boldsymbol{H}_\mathrm{c}$ is guaranteed to have full rank and thus a systematic linear encoding with the related generator matrix $\boldsymbol{G}_\mathrm{c}$ can be employed.

[1] If $\sqrt{M}$ is even, a shifted version of $\mathbb{G}$ has to be applied, cf. [25].

[2] $\mathrm{rem}_d(c) \stackrel{\text{def}}{=} c - d\lfloor c/d \rfloor$, with $c, d \in \mathbb{Z}$.

[3] Literature on non-binary BP decoding is usually focused on the case $q = 2^b$, $b \in \mathbb{N}$, e.g., [5]. For arbitrary fields $\mathbb{F}_q$, a standard probability-domain BP decoding as explained in [4] can be performed over the related arithmetic. It should be noted that for each element of $\mathbb{F}_q$, additionally the probability of its additive inverse has to be calculated in the sum-product step (check-node message update). When choosing $q = 2^b$, this is typically neglected as the additive inverse is the element itself.

An approximate metric for soft-decision decoding can be derived in the following way: According to Bayes' theorem, each element $l_{u,\rho}$, $\rho = 1, \ldots, q$, of the q-dimensional probability vector (pmf) is given by

$$l_{u,\rho} = \Pr\{c_u = \varphi_\rho \,|\, y_u\} = \frac{\Pr\{y_u \,|\, c_u = \varphi_\rho\} \cdot \Pr\{c_u = \varphi_\rho\}}{\Pr\{y_u\}} \tag{7}$$

(cf. Sec. II, receiver-side processing), where $\Pr\{c_u = \varphi_\rho\}$ and $1/\Pr\{y_u\}$ are constant $\forall \varphi_\rho$. The first factor reads

$$\Pr\{y_u \,|\, c_u = \varphi_\rho\} = \sum\nolimits_{\boldsymbol{\lambda} \in \boldsymbol{\Lambda}_\mathrm{p}} f_N \left(y_u - (\mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda})\right) \cdot \Pr\nolimits_{\boldsymbol{\lambda},\rho} \tag{8}$$

since an infinite number of modulo congruent signal points is present at the receiver side [10]. Thereby,

$$f_N(n) = \frac{1}{\pi g^2 \sigma_n^2} \exp\left(\frac{-|n|^2}{g^2 \sigma_n^2}\right), \quad n \in \mathbb{C}\,, \tag{9}$$

is the probability density function (pdf) of the scaled noise (factor g) and $\Pr_{\boldsymbol{\lambda},\rho} \overset{\text{def}}{=} \Pr\{y_u - n_u = \mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda} \,|\, \boldsymbol{Z}_\mathrm{p}\}$ the probability of occurrence for each modulo-congruent signal point which depends on the actual integer equalization matrix. Due to the infinite number of congruent points, (8) has to be approximated. For mid-to-high SNRs, it is sufficient to assume

$$\Pr\{y_u \,|\, c_u = \varphi_\rho\} \approx f_N \left(y_u - (\mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda}_{\min,\rho})\right) \cdot \Pr\nolimits_{\boldsymbol{\lambda}_{\min,\rho}}\,, \tag{10}$$

i.e., for each element of $\mathbb{F}_q$, only the neighboring modulo-congruent representative

$$\boldsymbol{\lambda}_{\min,\rho} \overset{\text{def}}{=} \underset{\boldsymbol{\lambda} \in \boldsymbol{\Lambda}_\mathrm{p}}{\operatorname{argmin}} \left|y_u - (\mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda})\right|^2 \tag{11}$$

is taken into account [10], where $\Pr_{\boldsymbol{\lambda}_{\min,\rho}} \approx 1/q$. In summary, the vector $\tilde{\boldsymbol{l}}_u = [\tilde{l}_{u,1}, \ldots, \tilde{l}_{u,q}]$ with

$$\tilde{l}_{u,\rho} \overset{\text{def}}{=} f_N \left(\min_{\boldsymbol{\lambda} \in \boldsymbol{\Lambda}_\mathrm{p}} \left|y_u - (\mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda})\right|\right) \tag{12}$$

is calculated and normalized to $\boldsymbol{l}_u = \tilde{\boldsymbol{l}}_{\boldsymbol{u}} / \sum_{\rho=1}^q \tilde{l}_{u,\rho}$.

C. LRA Precoding over Algebraic Constellations

As a modulo reduction—in case of LRA equalization inherently defined by the precoding lattice $\boldsymbol{\Lambda}_\mathrm{p}$—is one of the basic ideas behind Tomlinson-Harashima-type precoding [29], [15], [10], the combination of LRA (integer) equalization and non-integer precoding / successive interference cancellation is a promising strategy.

1) LRA Preequalization: Given the channel factorization $\bar{\boldsymbol{H}} = \boldsymbol{Z}\bar{\boldsymbol{H}}_\mathrm{red}$ (cf. (3)), the integer equalization matrix directly reads $\boldsymbol{Z}_\mathrm{p} = \boldsymbol{Z}^{-1}$, i.e., $\boldsymbol{P} = \boldsymbol{I}$. The feedback part (cf. Fig. 2) is deactivated; the feedforward matrix for the residual non-integer equalization according to the minimum mean-square error (MMSE) criterion is the $N_\mathrm{T} \times N_\mathrm{R}$ upper part $\boldsymbol{F}$ of

$$\bar{\boldsymbol{F}} \overset{\text{def}}{=} \begin{bmatrix} \boldsymbol{F}_{(N_\mathrm{T} \times N_\mathrm{R})} \\ \tilde{\boldsymbol{F}}_{(N_\mathrm{R} \times N_\mathrm{R})} \end{bmatrix} = \bar{\boldsymbol{H}}_\mathrm{red}^\mathsf{H} \left(\bar{\boldsymbol{H}}_\mathrm{red} \bar{\boldsymbol{H}}_\mathrm{red}^\mathsf{H}\right)^{-1}\,. \tag{13}$$

The factorization task (3) can be solved by any lattice reduction / shortest independent vector algorithm. Employing fields of Gaussian primes ($\boldsymbol{\Lambda}_\mathrm{a} = \mathbb{G}$), a complex-valued factorization has to be supported. As an example, the complex variant [13] of the LLL algorithm [21] is suited, however, resulting in an (unnecessarily) unimodular Gaussian integer matrix $\boldsymbol{Z}$. For fields of Eisenstein primes ($\boldsymbol{\Lambda}_\mathrm{a} = \mathbb{E}$), an adapted version has recently been proposed [25], resulting in an unimodular Eisenstein integer matrix $\boldsymbol{Z}$.

2) LRA Precoding: For the application of LRA precoding, additionally a sorted LQ decomposition according to [11]

$$\boldsymbol{P}\bar{\boldsymbol{H}}_\mathrm{red} = \boldsymbol{L}\begin{bmatrix}\boldsymbol{Q} & \tilde{\boldsymbol{Q}}\end{bmatrix} \overset{\text{def}}{=} \boldsymbol{L}\bar{\boldsymbol{Q}} \tag{14}$$

is necessary. Thereby, $\boldsymbol{P}$ is a $N_\mathrm{R} \times N_\mathrm{R}$ permutation matrix describing the optimum encoding order among the users. Usually—due to the uplink-downlink duality [31], [32]—the reversed *VBLAST* [14] sorting is used. The lower triangular $N_\mathrm{R} \times N_\mathrm{R}$ matrix $\boldsymbol{L}$ with unit main diagonal directly yields the feedback matrix (i.e., $\boldsymbol{B} = \boldsymbol{L}$), and $\boldsymbol{Q}$ is a $N_\mathrm{R} \times (N_\mathrm{R} + N_\mathrm{T})$ matrix with orthogonal rows. The MMSE feedforward matrix for the residual equalization is given by the upper part $\boldsymbol{F}$ of

$$\bar{\boldsymbol{F}} = \begin{bmatrix} \boldsymbol{F}_{(N_\mathrm{T} \times N_\mathrm{R})} \\ \tilde{\boldsymbol{F}}_{(N_\mathrm{R} \times N_\mathrm{R})} \end{bmatrix} = \bar{\boldsymbol{Q}}^\mathsf{H} \left(\bar{\boldsymbol{Q}}\bar{\boldsymbol{Q}}^\mathsf{H}\right)^{-1}\,. \tag{15}$$

The integer preequalization now reads $\boldsymbol{Z}_\mathrm{p} = \boldsymbol{P}\boldsymbol{Z}^{-1}$, including both the LRA equalization and the permutation for the optimized encoding order.

In contrast to LRA linear preequalization, two different factorization tasks have to be solved: first, the (complex-valued) shortest basis / shortest independent vector problem and afterwards, the sorted LQ decomposition. Both steps can be combined into a single factorization algorithm [11], however, the state-of-the-art approaches are limited to the shortest basis problem.

3) Comparison of Preequalization and Precoding: Though both LRA preequalization and precoding are performing the same integer-based equalization they differ in how to treat the residual non-integer interference. In the following, this will be discussed with the help of Fig. 3, where preequalization and precoding are exemplarily illustrated for a 25-ary square-QAM and Eisenstein prime constellation.

Via $\boldsymbol{Z}_\mathrm{p}$, linear combinations of data symbols or lattice points, respectively, are calculated. Performing LRA preequalization, the encoded symbols $\tilde{\boldsymbol{a}}$ are then simply modulo-reduced via $\tilde{\boldsymbol{x}} = \mathrm{mod}_{\boldsymbol{\Lambda}_\mathrm{p}}(\tilde{\boldsymbol{a}})$, resulting in symbols identical to the ones from the original signal constellation $\mathcal{A}$ (Fig. 3 left). For algebraic constellations $\mathcal{A}_\Theta^{(\cdot)}$ this has the consequence that still elements of the finite field are present, i.e., the cascade of integer equalization and modulo can be interpreted as one operation over $\mathcal{A}_\Theta^{(\cdot)} \simeq \mathbb{F}_q$. The residual non-integer interference is equalized by the (pseudo-)inverse of the reduced augmented channel matrix.

In LRA precoding, the feedforward matrix shapes the reduced channel to have a lower triangular structure; consequently the remaining causal interference can perfectly be eliminated by successive interference cancellation. As in conventional THP—due to the modulo operation—this results in

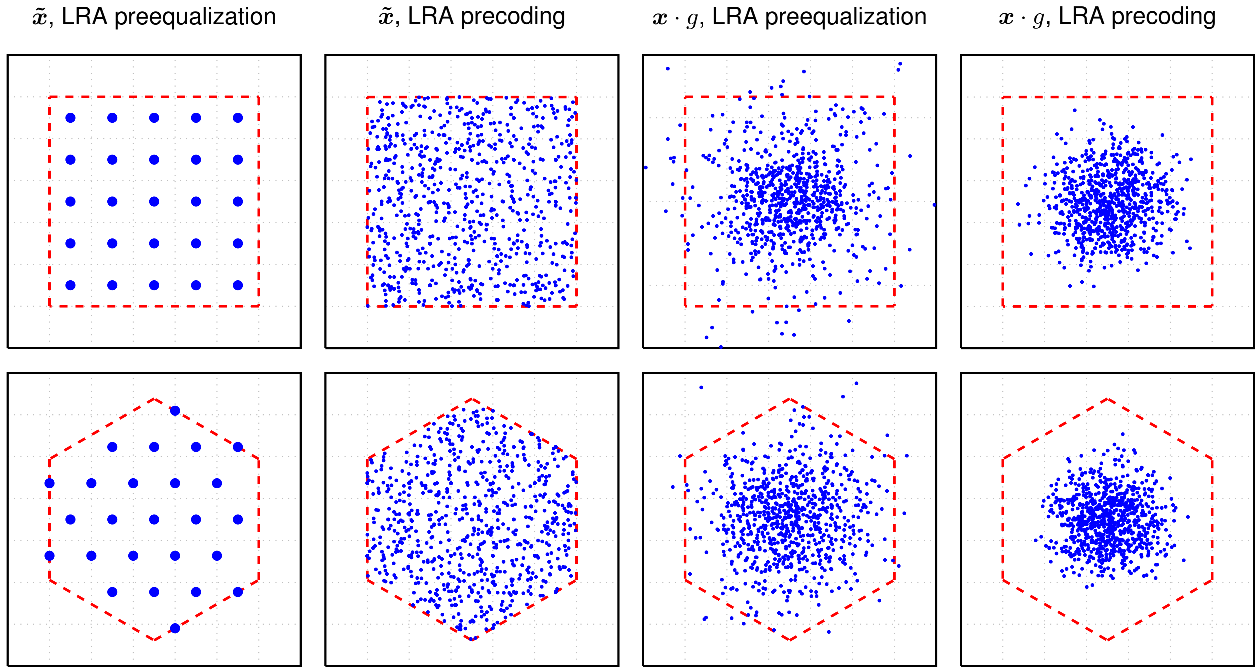

Fig. 3. Comparison of signal processing for LRA preequalization and precoding (cf. Fig. 2). Channel factorization via complex LLL [13] and Eisenstein LLL [25]; additional QR decomposition for precoding. 25-ary square-QAM (top) and Eisenstein prime (bottom) constellations. $E_{\mathrm{b,TX}}/N_0 = 10$ dB, $N_{\mathrm{T}} = N_{\mathrm{R}} = 8$, $N_{\mathrm{R}} \cdot 100 = 800$ samples per illustration.

approximately uniformly distributed encoded symbols $\tilde{\boldsymbol{x}}$ over $\mathcal{R}_{\mathrm{V}}(\boldsymbol{\Lambda}_{\mathrm{p}})$ (cf. Fig 3). A finite-field property of $\tilde{\boldsymbol{x}}$ is no longer present as a part of the non-integer interference is already incorporated.

In Fig. 3 (right side), the transmit symbols $\boldsymbol{x}$ (after feedforward processing) are illustrated for both cases neglecting the scaling factor g which enables a fair comparison. Apparently, on average precoding results in lower signal amplitudes. This is accompanied by a lower scaling factor g for a constant transmit power (dual to the noise enhancement for receiver-side equalization) which finally results in an increase in the receiver-side SNR and hence an improved performance. The gain is induced by a lower row norm [11] of the feedforward matrix when performing precoding instead of simple inversion of the reduced channel matrix. Moreover, as can be seen from Fig. 3 (both preequalization and precoding), the mean amplitude is even more decreased when applying the Eisenstein constellation. This not only results from the packing and shaping gain, but also from a factorization gain due to the higher packing density [25].

IV. Preliminary Numerical Results

In this section, we present numerical results for the approach of coded modulation over algebraic signal constellations. Noteworthy, a factorization according to the shortest basis problem via the complex LLL or its Eisenstein variant has been applied. In the final paper, this will be extended to results on the basis of a recently proposed algorithm [6] solving the shortest independent vector problem. Below, always the average over all users and a sufficiently large number of channel realizations is shown.

TABLE I
Simulation Parameters.

$\mathcal{A}$	$\boldsymbol{\Lambda}_{\mathrm{a}}$	Field	μ	ν	n_{c}	k_{c}	Info-Bits
$\mathcal{A}_{\Theta}^{(\mathbb{G})}$	$\mathbb{G}$	$\mathbb{F}_{13}$	37	10	16200	8760	32412
$\mathcal{A}_{\Theta}^{(\mathbb{G})}$	$\mathbb{G}$	$\mathbb{F}_{17}$	94	23	16200	7935	32430
$\mathcal{A}_{\Theta}^{(\mathbb{E})}$	$\mathbb{E}$	$\mathbb{F}_{13}$	37	10	16200	8760	32412
$\mathcal{A}_{\Theta}^{(\mathbb{E})}$	$\mathbb{E}$	$\mathbb{F}_{19}$	497	117	16200	7722	32802
16QAM	$\mathbb{G}$	$\mathbb{F}_{16}$	4	1	16200	8100	32400
16QAM	$\mathbb{G}$	$\mathbb{F}_2$	–	–	64800	32400	32400

A. Uncoded Transmission

For a reasonable assessment of the coded modulation approach and its impact on the transmission performance of LRA transmission, we first restrict to the uncoded case. Binary end-to-end transmission is considered, i.e., a modulus conversion is performed for the use of q-ary signal constellations. The simulation parameters are listed in Table I; for the moment the last three columns and last two rows can be omitted.

The simulation results for $N_{\mathrm{T}} = N_{\mathrm{R}} = 8$ are shown in Fig. 4. Considering the symbol-error rate (SER), we are able to observe the convergence to diversity order eight independently from the constellation, and a precoding gain of about 3–4 dB. The superiority of the Eisenstein constellations is clearly visible. However, their packing, shaping, and factorization gain [25] has a minor impact on LRA precoding (compared to preequalization): as the overall performance is increased, the potential gain by changing the signal grid is not that high. The Gaussian prime constellations show—at least when factorizing according to the shortest basis problem—an

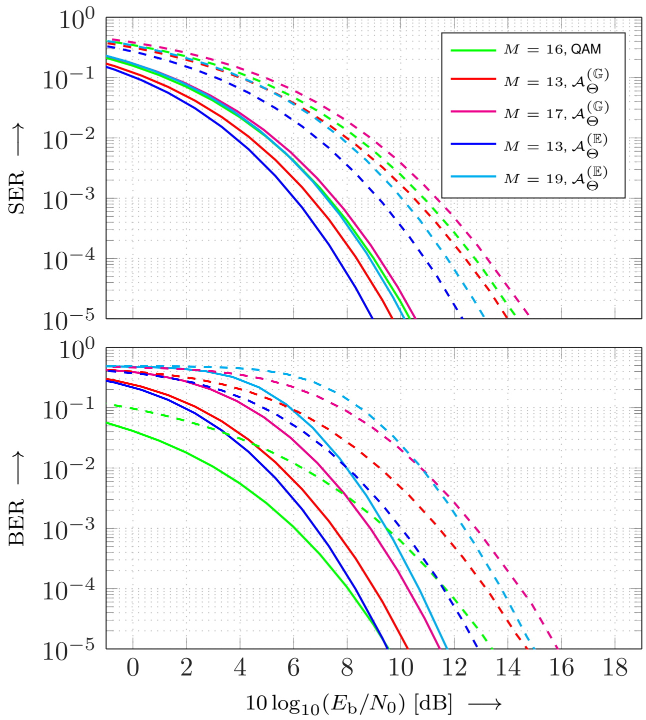

Fig. 4. SER (top) and BER (bottom) over $E_{\mathrm{b,TX}}/N_0$ for LRA preequalization (dashed) and precoding (solid) assuming uncoded binary transmission. Parameter: M; variation of the signal constellation $\mathcal{A}$ and the related signal point and precoding lattice. $N_\mathrm{T} = N_\mathrm{R} = 8$.

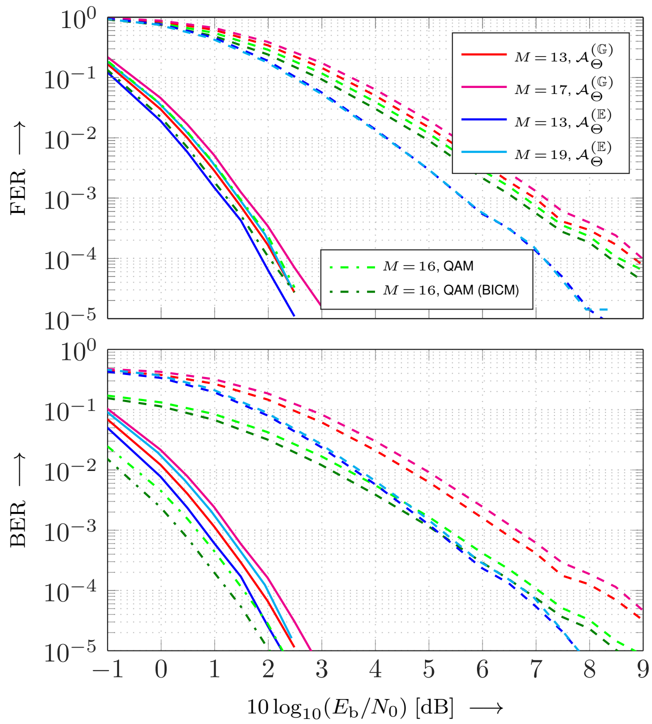

Fig. 5. FER (top) and BER (bottom) over $E_{\mathrm{b,TX}}/N_0$ for LRA preequalization (dashed) and precoding (solid, dashed dotted) assuming coded binary transmission. Parameter: M; variation of the signal constellation $\mathcal{A}$ and the related signal point and precoding lattice. $N_\mathrm{T} = N_\mathrm{R} = 8$.

equivalent performance as the 16-ary QAM one.

The related bit-error rate (BER) is depicted in Fig. 4. The precoding gain expectable from the SER curves is visible, but all non-QAM constellations suffer from an error propagation in the inverse modulus conversion [25]. Additionally, a direct mapping from bits allows *Gray labeling*, still more increasing the advantage of conventional QAM constellations. Even the 13-ary Eisenstein constellation only achieves the same performance as the 16-ary QAM one in the high-SNR regime, but naturally with an decrease in modulation rate. Consequently, an uncoded binary transmission in combination with modulus conversion is not advisable even in the case of LRA precoding.

B. Coded Transmission

Finally, we apply the presented coded modulation scheme based on LRA preequalization/precoding. For this purpose, near-ultra-sparse [4] semi-random-based irregular repeat-accumulate parity-check matrices of the form $\boldsymbol{H}_\mathrm{c} = [\boldsymbol{H}_\mathrm{c}^{(\mathrm{A})} \,|\, \boldsymbol{H}_\mathrm{c}^{(\mathrm{S})}] = [\boldsymbol{H}_\mathrm{c}^{(\mathrm{A1})} \, \boldsymbol{H}_\mathrm{c}^{(\mathrm{A2})} \,|\, \boldsymbol{H}_\mathrm{c}^{(\mathrm{S})}]$ have been employed. Thereby, the submatrix $\boldsymbol{H}_\mathrm{c}^{(\mathrm{S})}$ denotes the fixed systematic part [20] and the submatrices $\boldsymbol{H}_\mathrm{c}^{(\mathrm{A1})}$ and $\boldsymbol{H}_\mathrm{c}^{(\mathrm{A2})}$ form the random part, which is chosen according to a given rate distribution. To achieve a irregular code structure, we set the column weight of $\boldsymbol{H}_\mathrm{c}^{(\mathrm{A1})}$ to $d_\mathrm{c} = 3$, and the one of $\boldsymbol{H}_\mathrm{c}^{(\mathrm{A1})}$ to $d_\mathrm{c} = 2$; the row weight d_r is chosen in accordance and may only differ by one. Thereby, about 10 % of the $n_\mathrm{c} - k_\mathrm{c}$ columns of $\boldsymbol{H}_c^{(\mathrm{A})}$ are assigned to $\boldsymbol{H}_\mathrm{c}^{(\mathrm{A1})}$, the other 90 % to $\boldsymbol{H}_\mathrm{c}^{(\mathrm{A2})}$.

Fig. 5 illustrates the results for a end-to-end binary coded transmission; the parameters are listed again in Table I (code parameters are given in the last three columns). To have a fair comparison among the different settings, by adapting the code rate R_c the number of information bits per code block is fixed to achieve the same amount of transmission data. For comparison, a 16-ary square-QAM transmission is studied performing the channel coding in the extension field $\mathbb{F}_{16}$ with the above code construction. Besides, the conventional bit-interleaved coded modulation (BICM) [2] approach is applied, where a respective bit-log-likelihood metric and a well-optimized binary repeat-accumulate parity-check matrix from the DVB-S2 standard [8] are employed.

Considering the frame-error rate (FER; frame is the decoded message word), all transmissions based on the Gaussian integers as signal point lattice nearly perform the same. Among them, the BICM approach slightly shows an advantage due to the optimized code. In contrast, the Eisenstein-based ones allow a gain in $E_{\mathrm{b,TX}}/N_0$ of more than 1 dB (packing, shaping, and factorization gain). Applying LRA precoding, the transmission performance can enormously be increased (gain of about 5–6 dB). The choice of the constellation has a lower influence on the performance; a minor gain of the Eisenstein lattice is present. Apparently, the combination of constellations with lower cardinality but in compensation a higher code rate seems to be advantageous.

Concerning the BER (Fig. 5 bottom), the negative impact of the error propagation in the inverse modulus conversion (if the block/frame cannot be decoded correctly) is visible, degrading the performance of the non-QAM constellations. Nevertheless, in the low-BER regime of LRA preequalization, the Eisenstein transmissions even perform better than the BICM one with optimized code. For LRA precoding, only a small loss is present in comparison to BICM.

V. Summary and Contributions of the Final Paper

In this paper, we have presented an LRA MIMO broadcast channel transmission strategy, where the integer-interference is eliminated over finite-field constellations enabling a non-unimodular integer equalization matrix. These constellations have also enabled a coded modulation scheme, where the channel coding and the integer channel equalization are performed over the same q-ary arithmetic. For the cancellation of the non-integer interference, both LRA linear preequalization and precoding have been considered, including a discussion on the advantages of precoding.

Numerical results employing LLL-based algorithms (resulting in unimodular integer equalization matrices) have been shown. In the final paper, a comparison with the non-unimodular case will be given, where a factorization according to the shortest independent vector problem [6] will be applied. In combination with the application of optimized non-binary (q-ary) codes, as recently presented in [18], further gains in transmission performance are expected.

References

[1] M. Bossert. *Channel Coding for Telecommunications*. John Wiley & Sons Ltd, 1999.

[2] G. Caire, G. Taricco, E. Biglieri. Bit-Interleaved Coded Modulation *IEEE Transactions on Information Theory*, pp. 927–946, May 1998.

[3] J. Conway, N.J.A. Sloane. *Sphere Packings, Lattices and Groups*. Third Edition, Springer, 1999.

[4] L. Costantini, B. Matuz, G. Liva, E. Paolini, M. Chiani. Non-Binary Protograph Low-Density Parity-Check Codes for Space Communications. *International Journal of Satellite Communications and Networking*, pp. 43–51, Mar./Apr. 2012.

[5] D. Declercq, M. Fossorier. Decoding Algorithms for Nonbinary LDPC Codes Over $\mathrm{GF}(q)$. *IEEE Transactions on Communications*, pp. 633–643, Apr. 2007.

[6] L. Ding, K. Kansanen, Y. Wang, J. Zhang. Exact SMP Algorithms for Integer Forcing Linear MIMO Receivers. To be published in *IEEE Transactions on Wireless Communications*, preprint available, July 2015.

[7] U. Erez, S. Shamai, R. Zamir. Capacity and Lattice Strategies for Canceling Known Interference. *IEEE Transactions on Information Theory*, pp. 3820–3833, Nov. 2005.

[8] European Telecommunications Standards Institute. DVB-S2. *ETSI Standard EN 302 307 V1.1.1: Digital Video Broadcasting (DVB)*, 2005.

[9] C. Feng. D. Silva, F.R. Kschischang. An Algebraic Approach to Physical-Layer Network Coding. *IEEE Transactions on Information Theory*, pp. 7576–7596, Nov. 2013.

[10] R.F.H. Fischer. *Precoding and Signal Shaping for Digital Transmission*. Wiley-IEEE Press, 2002.

[11] R.F.H. Fischer. Complexity-Performance Trade-Off of Algorithms for Combined Lattice Reduction and QR Decomposition. *International Journal of Electronics and Communications (AEÜ)*, pp. 871–879, Nov. 2012.

[12] G.D. Forney, G. Ungerböck. Modulation and Coding for Linear Gaussian Channels. *IEEE Transactions on Information Theory*, pp. 2384–2415, Oct. 1998.

[13] Y.H. Gan, C. Ling, W.H. Mow. Complex Lattice Reduction Algorithm for Low-Complexity Full-Diversity MIMO Detection. *IEEE Transactions on Signal Processing*, pp. 2701–2710, July 2009.

[14] G.D. Golden, G.J. Foschini, R.A. Valenzuela, P.W. Wolniansky. Detection Algorithm and Initial Laboratory Results Using V-BLAST Space-Time Communication Architecture. *Electronics Letters*, pp. 14–15, Jan. 1999.

[15] H. Harashima, H. Miyakawa. Matched-Transmission Technique for Channels with Intersymbol Interference. *IEEE Transactions on Communications*, pp. 774–780, Aug. 1972.

[16] W. He, B. Nazer, S. Shamai. Uplink-Downlink Duality for Integer-Forcing. Proc. *IEEE International Symposium on Information Theory*, pp. 2544–2548, June/July 2014.

[17] S.N. Hong, G. Caire. Compute-and-Forward Strategies for Cooperative Distributed Antenna Systems. *IEEE Transactions on Information Theory*, pp. 5227–5243, May 2013.

[18] J. Yuan, L. Yang, T. Yang, J. An. Design of Non-Binary Irregular Repeat-Accumulate Codes for Reliable Physical-Layer Network Coding. Proc. *International Conference on Communications*, pp. 265–271, London, United Kingdom, June 2015

[19] K. Huber. Codes over Gaussian Integers. *IEEE Transactions on Information Theory*, pp. 207–216, Jan. 1994.

[20] H. Jin, A. Khandekar, R. McEliece. Irregular Repeat Accumulate Codes. Proc. *International Symposium on Turbo Codes*, pp. 1–8, Brest, France, Sep. 2000.

[21] A.K. Lenstra, H.W. Lenstra, L. Lovasz. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, pp. 515–534, 1982.

[22] W. Lin, B. Bai, Y. Li, X. Ma. Design of q-ary Irregular Repeat-Accumulate Codes. Proc. *International Conference on Advanced Information Networking and Applications*, pp. 201–206, Bradford, United Kingdom, May 2009.

[23] B. Nazer, M. Gastpar. Compute-and-Forward: Harnessing Interference Through Structured Codes. *IEEE Transactions on Information Theory*, pp. 6463–6486, Oct. 2011.

[24] A. Sakzad, J. Harshan, E. Viterbo. On Complex LLL Algorithm for Integer Forcing Linear Receivers. Proc. *Australian Communications Theory Workshop*, pp. 13–17, Jan./Feb. 2013.

[25] S. Stern, R.F.H. Fischer. Lattice-Reduction-Aided Preequalization over Algebraic Signal Constellations. Proc. *International Conference on Signal Processing and Communication Systems*, Cairns, Australia, Dec. 2015. Available online: http://nt.uni-ulm.de/lrapasc.

[26] C. Stierstorfer, R.F.H. Fischer. Lattice-Reduction-Aided Tomlinson-Harashima Precoding for Point-to-Multipoint Transmission. *International Journal of Electronics and Communications (AEÜ)*, pp. 328–330, 2006.

[27] Q.T. Sun, J. Yuan, T. Huang, K.W. Shum. Lattice Network Codes Based on Eisenstein Integers. *IEEE Transactions on Communications*, pp. 2713–2725, July 2013.

[28] M. Taherzadeh, A. Mobasher, A.K. Khandani. LLL Reduction Achieves the Receive Diversity in MIMO Decoding. *IEEE Transactions on Information Theory*, pp. 4801–4805, Dec. 2007.

[29] M. Tomlinson. New Automatic Equalizer Employing Modulo Arithmetic. *Electronics Letters*, pp. 138–139, Mar. 1971.

[30] N.E. Tunali, Y.C. Huang, J.J. Boutros, K.R. Narayanan. Lattices over Eisenstein Integers for Compute-and-Forward. *IEEE Transaction on Information Theory*, pp. 5306–5321, Oct. 2015.

[31] P. Viswanath, D.N.C. Tse. Sum Capacity of the Vector Gaussian Broadcast Channel and Uplink-Downlink Duality. *IEEE Transactions on Information Theory*, pp. 1912–1921, Aug. 2003.

[32] S. Vishwanath, N. Jindal, A. Goldsmith. Duality, Achievable Rates, and Sum-Rate Capacity of Gaussian MIMO Broadcast Channels. *IEEE Transactions on Information Theory*, pp. 2658–2668, Oct. 2003.

[33] C. Windpassinger, R.F.H. Fischer. Low-Complexity Near-Maximum-Likelihood Detection and Precoding for MIMO Systems Using Lattice Reduction. Proc. *IEEE Information Theory Workshop*, pp. 345–348, Mar. 2003.

[34] C. Windpassinger, R.F.H. Fischer, J.B. Huber. Lattice-Reduction-Aided Broadcast Precoding. *IEEE Transactions on Communications*, pp. 2057–2060, Dec. 2004.

[35] H. Yao, G.W. Wornell. Lattice-Reduction-Aided Detectors for MIMO Communication Systems. Proc. *IEEE Global Telecommunications Conference*, Taipei, Taiwan, Nov. 2002.

[36] J. Zhan, B. Nazer, U. Erez, M. Gastpar. Integer-Forcing Linear Receivers. *IEEE Transactions on Information Theory*, pp. 7661–7685, Oct. 2014.