Joint Algebraic Coded Modulation and Lattice-Reduction-Aided Preequalization

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 (LRA) preequalization for the multiple-input/ multiple-output broadcast channel has most often been considered for the uncoded case so far. However, recent advantages in the closely related field of integer-forcing equalization, where the cancellation of the multiuser interference and the channel coding are combined, create doubt to this separated point of view. In this letter, the philosophy of matching both the channel code and the complex-valued signal constellation to the same finite-field arithmetic is proposed. The consequences on the factorization task present in LRA preequalization are discussed and covered by numerical performance evaluations based on non-binary low-density parity-check codes.**

I. Introduction

Over the last years, multiuser multiple-input/multiple-output (MIMO) communication has gained huge interest. For downlink transmission (MIMO broadcast channel), i.e., joint transmitter-side (TX) and non-cooperative receiver-side (RX) processing, especially lattice-reduction-aided (LRA) preequalization and precoding [16] have become popular achieving full diversity. Thereby, the main idea is to perform the preequalization in a *suited basis*. This is achieved by factorizing the channel matrix into an integer part and a reduced part which is conventionally equalized instead. As the equalization of the integer matrix is performed by an integer inverse thereof, a unimodularity constraint is set for the factorization. The related factorization task is known as *shortest basis problem* (SBP).

Recently, an approach derived from physical-layer network coding [6] named integer-forcing equalization [17] has been proposed, sharing the same philosophy of factorizing the channel matrix. The main difference is that both channel coding and equalization are performed over the same finite-field arithmetic. In turn, as an (integer) inverse always exists over a finite field if a matrix has full rank, the unimodularity constraint can be dropped leading to the *shortest independent vector problem* (SIVP).

In the following, this finite-field approach is adapted to LRA preequalization. To this end, *algebraic signal constellations* [6] over the complex plane are applied. Specifically, fields of Gaussian and Eisenstein primes [3], [14] isomorphic to (real-valued) prime fields are convenient. Given both the channel code and the signal points in the same arithmetic, a coded modulation strategy is straightforward. Numerical simulations using non-binary low-density parity check (LDPC) codes show the effectiveness of the strategy at hand compared with conventional schemes.

II. System Model

A discrete-time complex-baseband multiuser MIMO broadcast channel with joint TX-side processing (N transmit antennas; illustrated in Fig. 1) and $K \leq N$ non-cooperating users is considered. For simplicity, the user index is omitted for equivalent parallel processing.

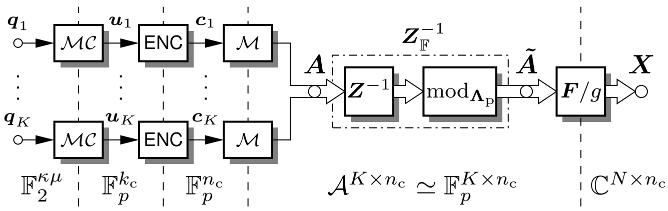

Fig. 1. Individual channel encoding and joint TX-side LRA equalization.

Independent streams of binary information/source symbols (bits) are sent to user $1, \ldots, K$. In order to be able to operate over a finite field $\mathbb{F}_p = \{\varphi_1, \ldots, \varphi_p\}$ of prime order $p > 2$, modulus conversion [10], [7], [14] is applied: each bitstream is divided into blocks of length μ that are mapped to blocks of ν message symbols with elements drawn from $\mathbb{F}_p$.

Following this, an encoding via some linear block code over $\mathbb{F}_p$ is performed. The code rate is $R_\mathrm{c} = k_\mathrm{c}/n_\mathrm{c}$, where $k_\mathrm{c} = \kappa\nu$, $\kappa \in \mathbb{N}$, denotes the code's dimension and n_c the code length. This leads to encoded symbols $\boldsymbol{c} = [c_1, \ldots, c_{n_\mathrm{c}}] \in \mathbb{F}_p^{n_\mathrm{c}}$ that are subsequently mapped ($\mathcal{M}$) to a block of complex-valued zero-mean (channel) symbols $\boldsymbol{a} = [a_1, \ldots, a_{n_\mathrm{c}}] \in \mathcal{A}^{n_\mathrm{c}}$ drawn from a p-ary constellation $\mathcal{A} = \mathcal{R}_\mathrm{V}(\boldsymbol{\Lambda}_\mathrm{p}) \cap \boldsymbol{\Lambda}_\mathrm{a}$ with variance σ_a^2. Thereby, $\boldsymbol{\Lambda}_\mathrm{a}$ is the signal point lattice and $\mathcal{R}_\mathrm{V}(\boldsymbol{\Lambda}_\mathrm{p})$ the Voronoi region of the precoding lattice $\boldsymbol{\Lambda}_\mathrm{p}$ [7], [14]. All independently encoded blocks $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K$ are finally (row-wise) combined into a data symbol matrix $\boldsymbol{A} \in \mathbb{C}^{K\times n_\mathrm{c}}$ enabling a joint LRA preequalization.

For the application of LRA preequalization, the $K \times N$ channel matrix $\boldsymbol{H}$ is factorized according to $\bar{\boldsymbol{H}} = \boldsymbol{Z}\bar{\boldsymbol{H}}_\mathrm{r}$, where $\bar{\boldsymbol{H}} = [\boldsymbol{H}, \sqrt{\zeta}\boldsymbol{I}]_{K\times(K+N)}$ denotes the augmented channel matrix and $\bar{\boldsymbol{H}}_\mathrm{r}$ the augmented reduced channel matrix of same dimension [8], [14]; $\zeta = \sigma_n^2/\sigma_a^2$ (σ_n^2 is the noise variance and $\boldsymbol{I}$ the identity matrix). The integer matrix $\boldsymbol{Z} \in \boldsymbol{\Lambda}_\mathrm{a}^{K\times K}$ is

This paper is a postprint of a paper submitted to and accepted for publication in Electronics Letters and is subject to Institution of Engineering and Technology Copyright. The copy of record is available at IET Digital Library. This work has been supported by Deutsche Forschungsgemeinschaft (DFG) within the framework COIN under grant Fi 982/4-3.

usually demanded to be unimodular ($|\det(\boldsymbol{Z})| = 1$). Dualizing the results for the multiple-access channel in [9], the optimum factorization criterion reads $(\bar{\boldsymbol{H}}^{+})^{\mathsf{H}} = \boldsymbol{Z}^{-\mathsf{H}}(\bar{\boldsymbol{H}}_{\mathrm{r}}^{+})^{\mathsf{H}}$, where $\bar{\boldsymbol{H}}^{+}$ denotes the right pseudo-inverse of $\bar{\boldsymbol{H}}$ and $(\bar{\boldsymbol{H}}^{+})^{\mathsf{H}}$ the Hermitian matrix thereof. The integer preequalization is performed via the matrix $\boldsymbol{Z}^{-1} = (\boldsymbol{Z}^{-\mathsf{H}})^{\mathsf{H}}$ and the modulo function reads $\mathrm{mod}_{\boldsymbol{\Lambda}_{\mathrm{p}}}(z) = z - \mathcal{Q}_{\boldsymbol{\Lambda}_{\mathrm{p}}}(z)$, $z \in \mathbb{C}$, where $\mathcal{Q}_{\boldsymbol{\Lambda}_{\mathrm{p}}}(z)$ is the quantization w.r.t. the precoding lattice [14]. The residual equalization via $\boldsymbol{F}$ is performed with the matrix of precoded symbols $\tilde{\boldsymbol{A}}$, resulting in the blocks of transmit symbols $\boldsymbol{X} \in \mathbb{C}^{N\times n_{\mathrm{c}}}$ to be radiated from the antennas. Here, $\boldsymbol{F}$ is the $N \times K$ upper part of $\bar{\boldsymbol{H}}_{\mathrm{r}}^{+}$. For each channel realization, the factor g is chosen to ensure the sum-power constraint $N\sigma_x^2 = K\sigma_a^2$.

The coefficients of $\boldsymbol{H}_{K\times N}$ are assumed to be i.i.d. zero-mean unit-variance complex Gaussian and constant over one block of n_{c} symbols (block-fading channel). At each receiver, i.i.d. zero-mean complex white Gaussian noise with variance σ_n^2 is present, which is combined into the matrix $\boldsymbol{N} \in \mathbb{C}^{K\times n_{\mathrm{c}}}$ (cf. Fig. 2). The MIMO system equation reads

$$\boldsymbol{Y} = \boldsymbol{H}\boldsymbol{X} + \boldsymbol{N} \,. \tag{1}$$

The signal-to-noise ratio (SNR) is expressed as transmitted energy per information bit in relation to the noise power spectral density and is given by $E_{\mathrm{b,TX}}/N_0 = \sigma_a^2/(\sigma_n^2 R_{\mathrm{c}}\mu/\nu)$.

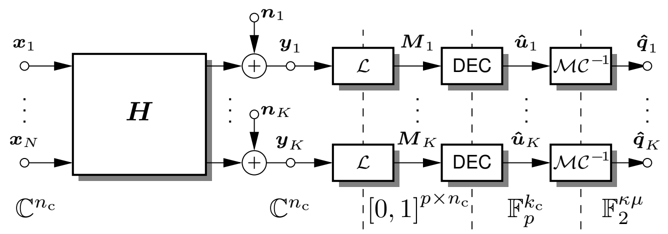

Fig. 2. Channel model and separated RX-side soft-decision decoding.

On the receiver-side (Fig. 2), each user separately starts with a metric calculation $\mathcal{L} : \mathbb{C}^{n_{\mathrm{c}}} \to [0,1]^{p\times n_{\mathrm{c}}}$ for soft-decision decoding based on its incoming signals $\boldsymbol{y} = [y_1, \ldots, y_{n_{\mathrm{c}}}] \in \mathbb{C}^{n_{\mathrm{c}}}$. The channel probabilities $m_{\rho,\gamma} = \Pr\{c_\gamma = \varphi_\rho \,|\, y_\gamma\}$, $\rho = 1,\ldots,p$, $\gamma = 1,\ldots,n_{\mathrm{c}}$, represented by $\boldsymbol{M} \in [0,1]^{p\times n_{\mathrm{c}}}$, are calculated for each user. Channel decoding w.r.t. $\boldsymbol{M}$ results in the estimated messages $\hat{\boldsymbol{u}} = [\hat{u}_1, \ldots, \hat{u}_{k_{\mathrm{c}}}] \in \mathbb{F}_p^{k_{\mathrm{c}}}$. Via inverse modulus conversion, a block of estimated bits $\hat{\boldsymbol{q}}$ is obtained.

III. Algebraic Signal Constellations

For LRA preequalization, fields of Gaussian primes [12], [3], [14] ($\boldsymbol{\Lambda}_{\mathrm{a}} = \mathbb{G}$, i.e., over the Gaussian integers) or Eisenstein primes [3], [15], [14] ($\boldsymbol{\Lambda}_{\mathrm{a}} = \mathbb{E}$, i.e., over the Eisenstein integers) are suited as they yield p-ary constellations with algebraic properties [6]: both are two-dimensional representations of $\mathbb{F}_p$ forming a field over the complex plane under modulo arithmetic. This not only means that a finite-field processing is possible—as performed in integer-forcing schemes—but also an isomorphism $\mathcal{A}_\Theta \simeq \mathbb{F}_p$ and a natural mapping $\mathbb{F}_p \to \mathcal{A}_\Theta$ can be given [14] (Θ is a Gaussian or Eisenstein prime and $\mathcal{A}_\Theta$ the respective field, where $|\Theta|^2 = p$). The precoding lattice reads $\boldsymbol{\Lambda}_{\mathrm{p}} = \Theta\mathbb{G}$ or $\boldsymbol{\Lambda}_{\mathrm{p}} = \Theta\mathbb{E}$ [14]. The integer preequalization and the modulo operation thus can equivalently be interpreted as a finite-field equalization matrix $\boldsymbol{Z}_{\mathbb{F}}^{-1} \in \mathbb{F}_p^{K\times K}$ (see Fig. 1), where $\boldsymbol{Z}_{\mathbb{F}}^{-1} \simeq (\mathrm{mod}_{\boldsymbol{\Lambda}_{\mathrm{p}}}(\boldsymbol{Z}))^{-1} \in \mathcal{A}_\Theta^{K\times K}$. Since (full-rank) matrices over $\mathbb{F}_p$ always have a finite-field inverse, the common unimodularity constraint present in LRA schemes is not necessary any more ($|\det(\boldsymbol{Z})| \geq 1$; SIVP).

IV. Coded Modulation

When demanding a joint arithmetic in channel coding and preequalization, non-binary LDPC codes [4] over $\mathbb{F}_p$ are convenient. More specifically, their subclass of repeat-accumulate codes [13] is suited as both systematic linear encoding and soft-decision decoding are possible. On the basis of the probability matrix $\boldsymbol{M}$, a non-binary (p-ary) belief-propagation (BP) decoding [2] can be performed.

Provided that the same arithmetic is present ($\mathcal{A}_\Theta \simeq \mathbb{F}_p$), the metric calculation can be performed as follows: According to Bayes' theorem, $m_{\rho,\gamma} = \Pr\{c_\gamma = \varphi_\rho \,|\, y_\gamma\} = \eta \cdot \Pr\{y_\gamma \,|\, c_\gamma = \varphi_\rho\}$, where the factor $\eta = \Pr\{c_\gamma = \varphi_\rho\}/\Pr\{y_\gamma\}$ can be assumed as constant $\forall\varphi_\rho$, $\rho = 1,\ldots,p$. Since modulo-congruent signal points are present at the receiver-side [7],

$$\Pr\{y_\gamma \,|\, c_\gamma = \varphi_\rho\} = \sum_{\boldsymbol{\lambda}\in\boldsymbol{\Lambda}_{\mathrm{p}}} f_N\left(y_\gamma - (\mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda})\right) \cdot \Pr_{\rho,\gamma}^{(\boldsymbol{\lambda})} \,. \tag{2}$$

Thereby, $\Pr_{\rho,\gamma}^{(\boldsymbol{\lambda})} = \Pr\left\{y_\gamma - n_\gamma = \mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda}\right\}\big|_{\boldsymbol{Z}^{-1}}$ is dependent on the actual integer equalization matrix. The first factor is the probability density function $f_N(n) = \exp\left(-|n|^2/(g^2\sigma_n^2)\right)/(\pi g^2\sigma_n^2)$ of the scaled noise. Via nearest-neighbor approximation [7], (2) can be simplified to

$$\tilde{m}_{\rho,\gamma} = f_N\left(\min_{\boldsymbol{\lambda}\in\boldsymbol{\Lambda}_{\mathrm{p}}} |y_\gamma - (\mathcal{M}(\varphi_\rho) + \boldsymbol{\lambda})|\right) \,, \tag{3}$$

and normalized to probability mass functions of the form $\boldsymbol{m}_\gamma = \tilde{\boldsymbol{m}}_\gamma / \sum_{\rho=1}^{p} \tilde{m}_{\rho,\gamma}$.

V. Numerical Results

The performance of the proposed approach is assessed by means of numerical simulations. Random-based irregular repeat-accumulate codes have been applied, where the vast majority of all arbitrary parity-check columns has a weight of 3 and a small number of 4 (irregular row weight that differs by one). The simulation parameters are listed in Table 1; the number of information bits per block is (almost) kept constant (2 bits/symbol; code rate is adapted). Starting from conventional 16QAM ($\boldsymbol{\Lambda}_{\mathrm{a}} = \mathbb{G}$, $\boldsymbol{\Lambda}_{\mathrm{p}} = 4\mathbb{G}$, $R_{\mathrm{c}} = 1/2$), the 13-ary Gaussian and Eisenstein prime constellation, as well as the 17-ary Gaussian and 19-ary Eisenstein one are considered. For the Gaussian ones, an efficient factorization according to the SIVP is possible [9], which can easily be adapted to the Eisenstein lattice. Following the common demand for an integer equalization matrix $\boldsymbol{Z}^{-1} \in \boldsymbol{\Lambda}_{\mathrm{a}}{}^{K\times K}$, a restriction to the SBP is necessary for the QAM constellation. Hence, the

TABLE I
SIMULATION PARAMETERS.

Field	$\mathcal{A}$	$\mathbf{\Lambda}_\mathrm{a}$	μ	ν	n_c	k_c	Info-Bits
$\mathbb{F}_{13}$	$\mathcal{A}_\ominus$	$\mathbb{G}$	37	10	16200	8760	32412
$\mathbb{F}_{13}$	$\mathcal{A}_\ominus$	$\mathbb{E}$	37	10	16200	8760	32412
$\mathbb{F}_{17}$	$\mathcal{A}_\ominus$	$\mathbb{G}$	94	23	16200	7935	32430
$\mathbb{F}_{19}$	$\mathcal{A}_\ominus$	$\mathbb{E}$	497	117	16200	7722	32802
$\mathbb{F}_{16}$	16QAM	$\mathbb{G}$	4	1	16200	8100	32400
$\mathbb{F}_{2}$	16QAM	$\mathbb{G}$	–	–	64800	32400	32400

complex-valued variant of the LLL algorithm [11] has to be used.

Fig. 3 illustrates both the frame- and the bit-error rate (FER/BER) in dependency of $E_{\mathrm{b,TX}}/N_0$ in dB if $N = K = 8$. For comparison, the results for 16QAM are given when performing a non-binary coding over $\mathbb{F}_{16}$. As state-of-the-art approach, bit-interleaved coded modulation (BICM) [1] is employed (bit log-likelihood BP decoding according to (3); Gray labeling). Thereby, the binary DVB-S2 irregular repeat-accumulate code [5] is assessed for LRA and non-LRA linear preequalization (LPE).

Regarding the FER for 16QAM transmission, the BICM approach shows a slightly better performance than the non-binary coding over $\mathbb{F}_{16}$ due to the highly-optimized binary LDPC code. Employing Gaussian prime constellations and a factorization according to the SIVP, a gain of about 0.25–0.5 dB is possible (mid-to-high SNR regime; 17-ary one has comparably low power efficiency). Furthermore, the Eisenstein ones achieve a gain of about 1 dB due to a packing, shaping, and additional factorization gain of the hexagonal lattice [14]. In the non-LRA case, the impact of diversity order one is clearly visible in spite of channel coding.

Concerning the BER, a degradation of the p-ary constellations is present, which is caused by error propagation in the inverse modulus conversion [14]. Nevertheless, the Eisenstein constellations are still advantageous (gain of about 0.5 dB in the high-SNR range). Besides, at least for the 13-ary Gaussian one the same performance as in the BICM case is achieved, where no modulus conversion has to be applied.

VI. CONCLUSION

A coded modulation and preequalization strategy for the MIMO broadcast channel has been proposed, where the channel code and the signal constellation share the same finite-field arithmetic. This strategy—following the philosophy of integer-forcing equalization—drops the unimodularity constraint in LRA schemes. Simulations on the basis of non-binary LDPC codes have revealed that a factorization gain is possible compared with state-of-the art approaches like BICM; employing the hexagonal (Eisenstein) lattice even results in further enhancement. In combination with optimized non-binary LDPC codes and non-binary source encoders the transmission performance may even be increased.

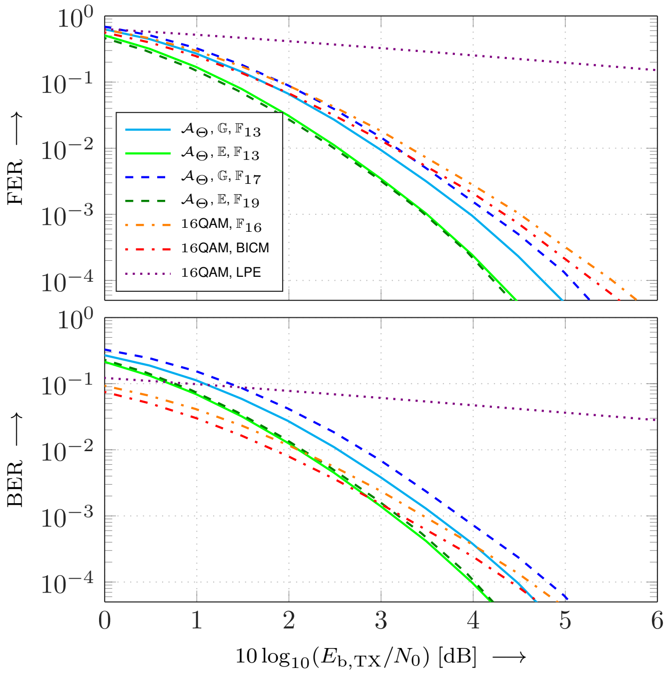

Fig. 3. Frame- and bit-error rate over $E_{\mathrm{b,TX}}/N_0$ in dB ($N = K = 8$).

REFERENCES

[1] Caire, G., Taricco, G., Biglieri, E.: 'Bit-Interleaved Coded Modulation', *IEEE Trans. Inf. Theory*, **44**, (3), pp. 927–946, May 1998.

[2] Costantini, L., Matuz, B., et al.: 'Non-Binary Protograph Low-Density Parity-Check Codes for Space Communications', *Int. Journal on Satellite Commun. and Networking*, **30**, (2), pp. 43–51, Mar./Apr. 2012.

[3] Conway, J., Sloane, N.: 'Sphere Packings, Lattices and Groups', (Third Edition, Springer, 1999).

[4] Davey, M.C., MacKay, D.: 'Low-Density Parity Check Codes over GF(q)' *IEEE Commun. Lett.*, **2**, (6), pp. 165–167, June 1998.

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

[6] Feng, C., Silva, D., Kschischang, F.R.: 'An Algebraic Approach to Physical-Layer Network Coding', *IEEE Trans. Inf. Theory*, **59**, (11), pp. 7576–7596, Nov. 2013.

[7] Fischer, R.F.H.: 'Precoding and Signal Shaping for Digital Transmission', (Wiley-IEEE Press, 2002).

[8] Fischer, R.F.H.: 'Complexity-Performance Trade-Off of Algorithms for Combined Lattice Reduction and QR Decomposition', *Int. Journal of Electronics and Commun. (AEÜ)*, **66**, (11), pp. 871–879, Nov. 2012.

[9] Fischer, R.F.H., Cyran, M., Stern, S.: 'Factorization Approaches in Lattice-Reduction-Aided and Integer-Forcing Equalization', *Int. Zurich Seminar on Communications*, Zurich, Switzerland, Mar. 2016.

[10] Forney, G.D., Ungerböck, G.: 'Modulation and Coding for Linear Gaussian Channels', *IEEE Trans. Inf. Theory*, **44**, (6), pp. 2384–2415, Oct. 1998.

[11] Gan, Y.H., Ling, C., Mow, W.H.: 'Complex Lattice Reduction Algorithm for Low-Complexity Full-Diversity MIMO Detection', *IEEE Trans. Signal Process.*, **57**, (7), pp. 2701–2710, July 2009.

[12] Huber, K.: 'Codes over Gaussian Integers', *IEEE Trans. Inf. Theory*, **40**, (1), pp. 207–216, Jan. 1994.

[13] Jin, H., Khandekar, A., McEliece, R.: 'Irregular Repeat Accumulate Codes', *Int. Symp. on Turbo Codes*, Brest, France, Sep. 2000.

[14] Stern, S., Fischer, R.F.H.: 'Lattice-Reduction-Aided Preequalization over Algebraic Signal Constellations', *Int. Conf. on Signal Processing and Communication Systems*, Cairns, Australia, Dec. 2015.

[15] Tunali, N.E., Narayanan, K.R, et al.: 'Lattices over Eisenstein Integers for Compute-and-Forward', *IEEE Trans. Inf. Theory*, **61**, (10), pp. 5306–5321, Oct. 2015.

[16] Windpassinger, C., Fischer, R.F.H., Huber, J.B.: 'Lattice-Reduction-Aided Broadcast Precoding', *IEEE Trans. Commun.*, **52**, (12), pp. 2057–2060, Dec. 2004.

[17] Zhan, J., Nazer, B., et al.: 'Integer-Forcing Linear Receivers', *IEEE Trans. Inf. Theory*, **60**, (12), pp. 7661–7685, Dec. 2014.