

Lattice Reduction and Factorization for Equalization

Robert F.H. Fischer Sebastian Stern

Institut für Nachrichtentechnik, Universität Ulm

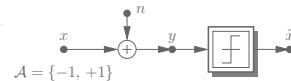


ulm university universität
uulm

Introduction

Digital Communications:

- abstract high-level view of digital communications
 - a *point* x drawn from some *signal constellation* \mathcal{A} is transmitted (a point can represent $\log_2 |\mathcal{A}|$ bits of information)
 - the channel adds (interference and) noise n
 - the received symbols is $y = x + n$
 - at the receiver, *decisions* have to be taken
- since we can use *quadrature modulation* (modulation of amplitude and phase), all signals are *complex-valued*



Channel Coding:

- for reducing the error rate, channel coding is employed
- in block codes (codelength η) not all \mathcal{A}^η combinations are used but only those which can be distinguished reliably
- a trade-off between transmission rate (bit rate) and error rate is possible

Outline

- Introduction
- Equalization
 - Structure of the Signals | Maximum-Likelihood Detection | Linear Equalization
- Lattice-Reduction-Aided Equalization
 - LRA Scheme | IF Scheme
- Factorization Task
 - Criteria | Constraints
- Lattices and Lattice Problems
 - Shortest Independent Vector Problem | Lattice Basis Reduction
- Numerical Results
- LRA Decision-Feedback Equalization
 - Structure | Sorting | Algorithm
- Numerical Results
- Summary

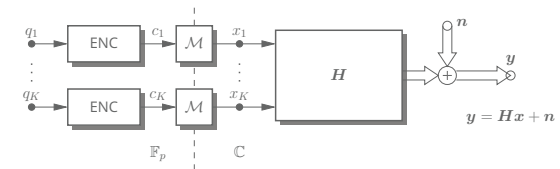
Fischer: Lattice Reduction and Factorization for Equalization

1

Introduction (II)

Situation: multipoint-to-point transmission, *MIMO multiple-access channel*

- K non-cooperating single-antenna users
- central base station with N_R receive antennas
 - \Rightarrow *joint processing/decoding at the receiver side possible*

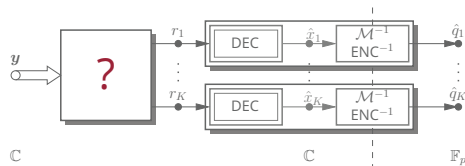


Channel Encoding / Mapping:

- channel coding done over the finite field \mathbb{F}_p (q_k and c_k taken from \mathbb{F}_p)
- mapping \mathcal{M} of finite-field symbols c_k to complex-valued points x_k taken from some signal constellation \mathcal{A}

Introduction (III)

Question: *How to perform equalization / decoding?*



Usual Approach:

- joint equalization / decoding typically much to complex
⇒ *separate equalization / decoding*
- channel decoding
 - individual (per user)
 - over a temporal block (code word)
- low-complexity equalization strategy (as for the uncoded case)
 - over the users
 - per time step

Signal Constellations and Codes

Signal Constellation: Construction

- signal point lattice

$$\Lambda_a$$

typically: $\Lambda_a = \mathbb{Z}$ or $\Lambda_a = \mathbb{G} = \mathbb{Z} + j\mathbb{Z}$

- „shaping“ lattice

$$\Lambda_s$$

and its Voronoi region $\mathcal{R}_V(\Lambda_s)$
(typically a sublattice of Λ_a : $\Lambda_s \subset \Lambda_a$)

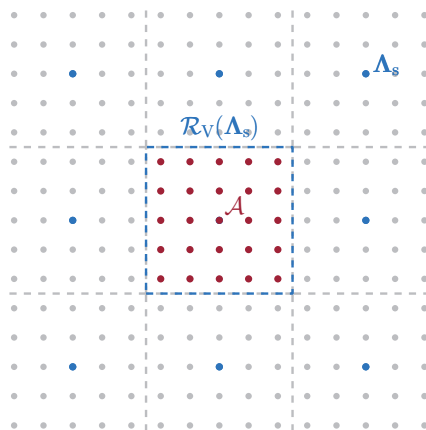
- *signal constellation*

$$\mathcal{A} = \Lambda_a \cap \mathcal{R}_V(\Lambda_s)$$

- *lattice code*

do everything in N dimensions

$$\mathcal{C} = \Lambda_a \cap \mathcal{R}_V(\Lambda_s)$$



Introduction (IV)

Equalization of MIMO Channel:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}$$

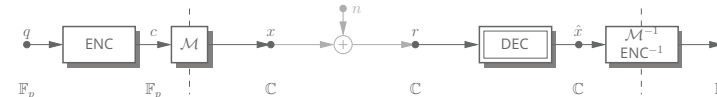
done symbol-by-symbol (independently over the time steps) in the uncoded case

Equalization Schemes:

- linear equalization
according to zero-forcing (ZF) or minimum mean-squared error (MMSE) criterion
- decision-feedback equalization (DFE)
aka successive interference cancellation, (V-)BLAST
- lattice-reduction-aided (LRA) / integer-forcing (IF) schemes
low-complexity, high-performance schemes
- maximum-likelihood detection (MLD) / lattice decoding
optimum procedure, highest complexity

Decoding and Demapping

Channel Encoding and Decoding:



Encoding:

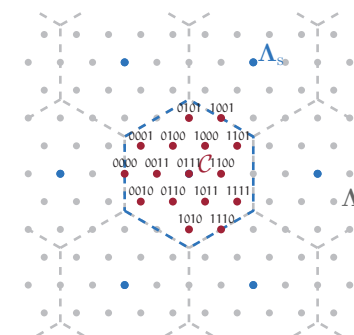
- encoding ENC over \mathbb{F}_p
- mapping \mathcal{M} to signal point in \mathbb{C}

Decoding:

- lattice decoding (in signal space)
w.r.t. to Λ_c
- demapping \mathcal{M}^{-1} to $\hat{c} \in \mathbb{F}_p$
- encoder inverse ENC^{-1}

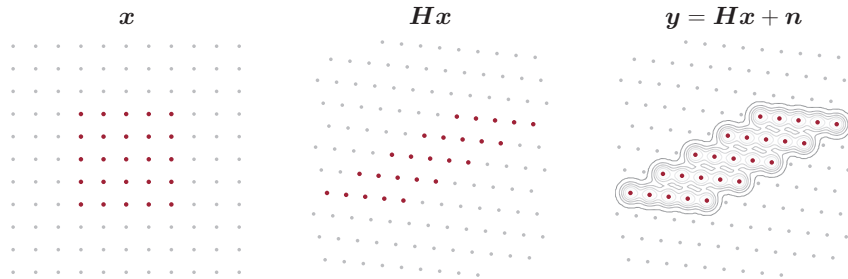
Variant:

- demapping modulo Λ_s , i.e., $\text{mod } \mathcal{M}^{-1}$



Structure of the Signals

Visualization: (real-valued example $K = 2$, $\Lambda_c = \mathbb{Z}$, $|\mathcal{A}| = 5$)



Structure of the Signals (II)

Lattice:

- K -dim. lattice spanned by basis vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_K$ — basis matrix

$$\mathbf{B} = [\mathbf{b}_1 \mathbf{b}_2 \dots \mathbf{b}_K]$$

- real-valued lattice

$$\Lambda = \left\{ \mathbf{\lambda} = \sum_{k=1}^K z_k \mathbf{b}_k = \mathbf{B} \begin{bmatrix} z_1 \\ \vdots \\ z_K \end{bmatrix} \mid z_k \in \mathbb{Z} \right\} \stackrel{\text{def}}{=} \mathbf{B}\mathbb{Z}^K$$

Lattice Structure of the Signal:

- for $\mathbf{x} \in \mathbb{G}^K = (\mathbb{Z} + j\mathbb{Z})^K$ the noise-free receive vectors

$$\mathbf{z} = \mathbf{H}\mathbf{x}$$

are taken from the complex-valued lattice $\Lambda = \mathbf{H}\mathbb{G}^K$ spanned by the columns \mathbf{h}_k of the channel matrix

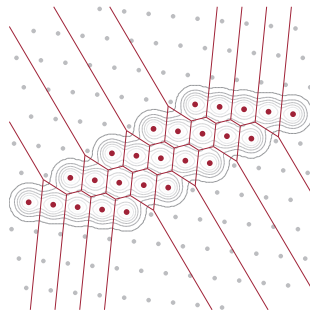
$$\mathbf{H} = [\mathbf{h}_1 \mathbf{h}_2 \dots \mathbf{h}_K]$$

Maximum-Likelihood Detection

Optimum Detection Rule: ML criterion

$f_X(x)$: probability density function

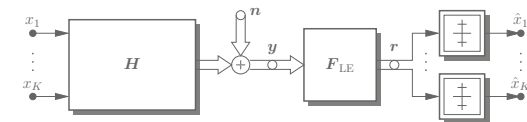
$$\hat{\mathbf{x}} = \underset{\mathbf{x} \in \mathcal{A}^K}{\operatorname{argmax}} f_Y(\mathbf{y} \mid \mathbf{x}) = \underset{\mathbf{x} \in \mathcal{A}^K}{\operatorname{argmin}} \|\mathbf{y} - \mathbf{H}\mathbf{x}\|^2$$



- **lattice decoding** — high complexity per time step
efficient implementation via the *Sphere Decoder* [AEVZ'02]
- for combination with channel decoding generation of soft output required

Linear Equalization

Linear Equalization: simple strategy — filtering followed by individual decision/decoding



- this equalization *strategy / scheme* can be optimized either according to the *zero-forcing (ZF)* or *minimum mean-squared error (MMSE) criterion*

- zero-forcing criterion: (\mathbf{I} : identity matrix; $(\cdot)^+$: (left) pseudoinverse)

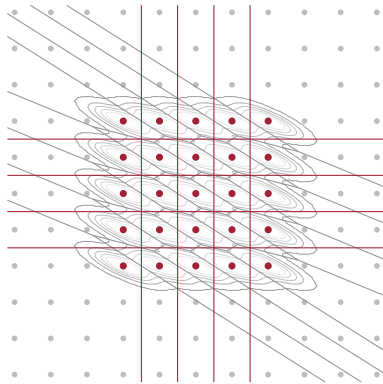
$$\mathbf{F}_{\text{LE}} \cdot \mathbf{H} \stackrel{!}{=} \mathbf{I} \quad \Rightarrow \quad \mathbf{F}_{\text{LE,ZF}} = (\mathbf{H}^H \mathbf{H})^{-1} \mathbf{H}^H \stackrel{\text{def}}{=} \mathbf{H}^+$$

- minimum mean-squared error criterion: ($\zeta \stackrel{\text{def}}{=} \sigma_n^2 / \sigma_x^2$)
error signal $\mathbf{e} = \mathbf{F}_{\text{LE}} \mathbf{y} - \mathbf{x}$; error covariance matrix $\Phi_{ee} = \mathbb{E}\{\mathbf{e}\mathbf{e}^H\}$

$$\operatorname{trace}(\Phi_{ee}) \stackrel{!}{\rightarrow} \min \quad \Rightarrow \quad \mathbf{F}_{\text{LE,MMSE}} = (\mathbf{H}^H \mathbf{H} + \zeta \mathbf{I})^{-1} \mathbf{H}^H$$

Linear Equalization (II)

Visualization:

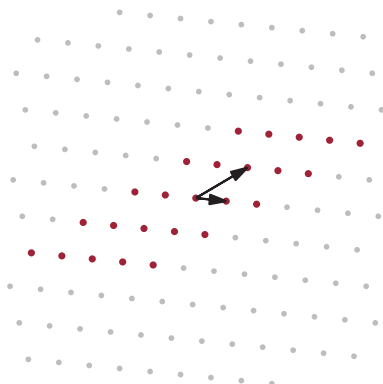


Problem of equalizing the signal

- the noise is filtered, too \Rightarrow **noise enhancement**
- individual threshold decision per dimension not optimum

Lattice-Reduction-Aided Equalization

Visualization:



$$H = [h_1 \ h_2]$$

Linear Equalization (III)

Noise Enhancement:

$$\blacksquare \text{ ZF solution — } F_{\text{LE,ZF}} = (H^H H)^{-1} H^H = \begin{bmatrix} f_1 \\ \vdots \\ f_K \end{bmatrix}; \quad r = F_{\text{LE,ZF}} y = x + F_{\text{LE,ZF}} n$$

- noise variance (n i.i.d. components with variance σ_n^2)

$$\sigma_{n_k}^2 = \sigma_n^2 \cdot \|f_k\|^2$$

- noise enhancement

$$E_k = \sigma_{n_k}^2 / \sigma_n^2 = \|f_k\|^2$$

$$\blacksquare \text{ (biased) MMSE solution — } F_{\text{LE,MMSE}} = (H^H H + \zeta I)^{-1} H^H$$

or with $\mathcal{H} = \begin{bmatrix} H \\ \sqrt{\zeta} I \end{bmatrix}$ we have $\mathcal{F}_{\text{LE,MMSE}} = (\mathcal{H}^H \mathcal{H})^{-1} \mathcal{H}^H = \begin{bmatrix} f_1 \\ \vdots \\ f_K \end{bmatrix}$

- error covariance matrix

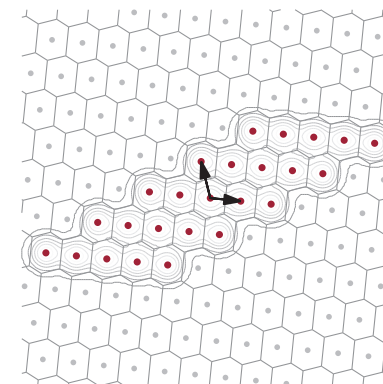
$$\Phi_{ee} / \sigma_n^2 = (H^H H + \zeta I)^{-1} = (\mathcal{H}^H \mathcal{H})^{-1}$$

- noise enhancement ($\mathcal{F}_{\text{LE,MMSE}} \mathcal{F}_{\text{LE,MMSE}}^H = (\mathcal{H}^H \mathcal{H})^{-1} \mathcal{H}^H \mathcal{H} (\mathcal{H}^H \mathcal{H})^{-1} = (\mathcal{H}^H \mathcal{H})^{-1}$)

$$E_k = [\Phi_{ee} / \sigma_n^2]_{k,k} = \|f_k\|^2$$

Lattice-Reduction-Aided Equalization

Visualization:



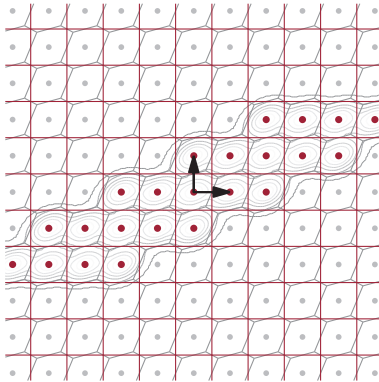
$$H = [h_1 \ h_2]$$

$$C = [c_1 \ c_2]$$

$$= HZ, \quad \begin{matrix} Z \in \mathbb{Z}^{2 \times 2} \\ |\det(Z)| = 1 \end{matrix}$$

Lattice-Reduction-Aided Equalization

Visualization:

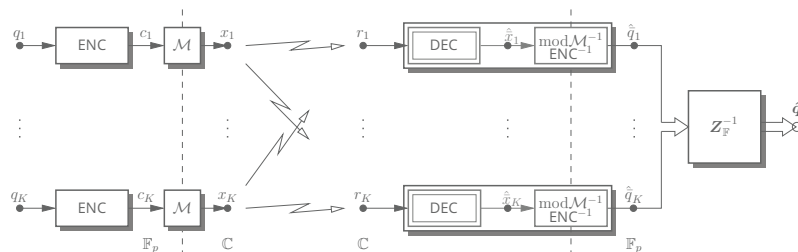


$$\begin{aligned} \mathbf{H} &= [\mathbf{h}_1 \ \mathbf{h}_2] \\ \mathbf{C} &= [\mathbf{c}_1 \ \mathbf{c}_2] \\ &= \mathbf{H}\mathbf{Z}, \quad \mathbf{Z} \in \mathbb{Z}^{2 \times 2} \\ &\quad |\det(\mathbf{Z})| = 1 \end{aligned}$$

Integer-Forcing Schemes

Compute-And-Forward Strategy in Relaying:

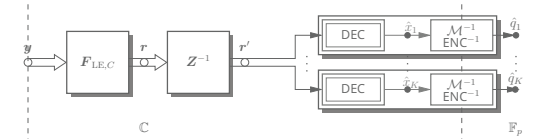
[NG'11]



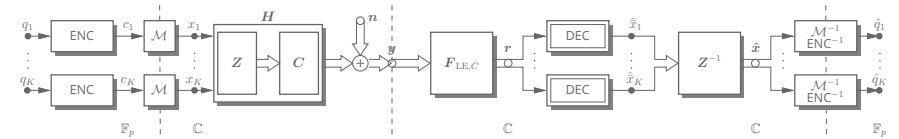
- the receiver decodes an *integer linear combination* of the codewords
- resolution of linear combinations at some central unit
only finite-field symbols are communicated — processing over \mathbb{F}_p

Equalization Schemes

Linear Equalization:



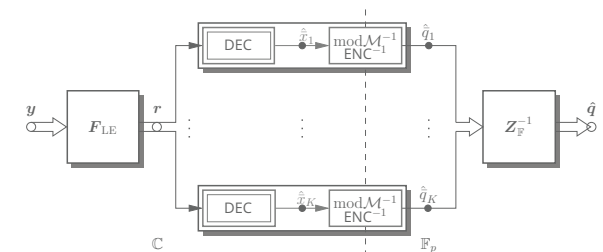
Lattice-Reduction-Aided Equalization: [YW'02], [WF'03]



Integer-Forcing Schemes

Compute-And-Forward Strategy in Relaying:

[NG'11]

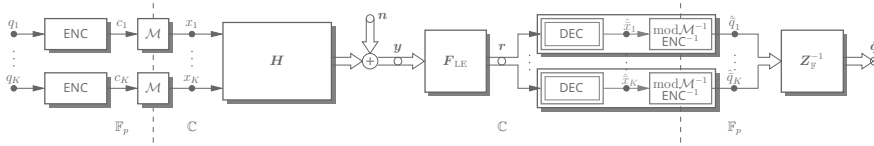


- the receiver decodes an *integer linear combination* of the codewords
- resolution of linear combinations at some central unit
only finite-field symbols are communicated — processing over \mathbb{F}_p
- if a joint/central receiver is present, some preprocessing can be done prior to channel decoding — *integer-forcing receiver* [ZNEG'14]

Integer-Forcing Schemes (II)

Integer-Forcing Equalization:

[ZNEG'14]

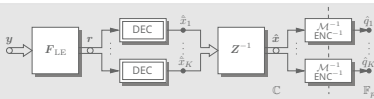


- the users have to use the same **linear code** (or subcodes thereof) any integer linear combination of valid codewords is a valid codeword over \mathbb{F}_p
- a **linear mapping** has to be applied the arithmetics over \mathbb{F}_p has to match that over \mathbb{R} (or \mathbb{C}) modulo p
- this only works if the cardinality of the signal constellation is a **prime number** and equal to the field size p
- the integer matrix has only to be invertible over \mathbb{F}_p
 $\Rightarrow \mathbf{Z}_{\mathbb{F}}$ **only has to have full rank**

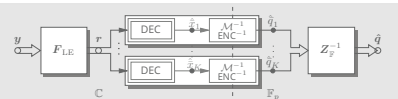
[FSK'13]

Structure

Lattice-Reduction-Aided Equalization



Integer-Forcing Equalization



denomination

channel-oriented

signal-oriented

suited for

joint receiver

distributed antenna systems

treat integer interference over

$$\mathbb{G} = \mathbb{Z} + j\mathbb{Z}$$

$$\mathbb{F}_p$$

constraint on signal constellation and mapping

usually treated uncoded
signal points drawn from a lattice
linear codes over \mathbb{R} (or \mathbb{C})

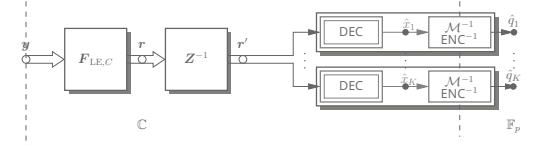
incorporation of coding
match arithmetic in \mathbb{R} (or \mathbb{C}) and \mathbb{F}_p
one-dim. p -ary constellation, p a prime

Equalization Schemes

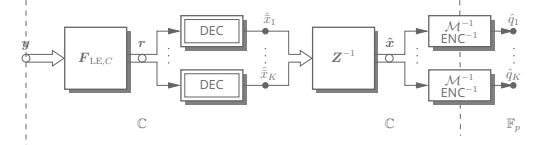
Points to discuss:

- structure
 - LRA vs. IF
 - respective constraints on signal constellations and codes
- factorization task $\mathbf{H} = \mathbf{CZ}$
 - optimization criterion
 - performance measure
 - suited algorithm
- constraints on \mathbf{Z}
 - unimodular matrix — $|\det(\mathbf{Z})| = 1$
shortest basis problem
 - full-rank matrix — $\text{rank}(\mathbf{Z}) = K$
shortest independent vector problem

Linear Equalization:

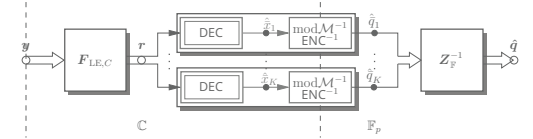


Lattice-Reduction-Aided Equalization: [YW'02], [WF'03]



Integer-Forcing Equalization:

[ZNEG'14]



Factorization Task

Basic Idea of LRA Schemes:

[YW'02], [WF'03]

- choose a "more suited" representation of the lattice, a **reduced basis**
- perform equalization with respect to this new basis; integer linear combinations of the data symbols are detected

Procedure:

- input/output relation

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} = \mathbf{CZ}\mathbf{x} + \mathbf{n}$$

- ZF linear equalization of \mathbf{C} — equalization matrix $\mathbf{F}_{\text{LE},\mathbf{C}} = \begin{bmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_K \end{bmatrix} = \mathbf{C}^+$

$$\begin{aligned} \mathbf{r} &= \mathbf{F}_{\text{LE},\mathbf{C}}\mathbf{y} = \mathbf{F}_{\text{LE},\mathbf{C}}(\mathbf{CZ}\mathbf{x} + \mathbf{n}) \\ &= \mathbf{Z}\mathbf{x} + \mathbf{F}_{\text{LE},\mathbf{C}}\mathbf{n} \end{aligned}$$

- the noise power in branch k is given by (\mathbf{n} : i.i.d. components with variance σ_n^2)

$$\sigma_{n_k}^2 = \sigma_n^2 \cdot \|\mathbf{f}_k\|^2 = \sigma_n^2 \cdot E_k$$

with noise enhancement $E_k = \|\mathbf{f}_k\|^2$

Factorization Task (II)

Problem: given \mathbf{H} , find \mathbf{C} and \mathbf{Z} such that

- factorization of \mathbf{H}

$$\mathbf{H} = \mathbf{C}\mathbf{Z}$$

- \mathbf{Z} is an *integer matrix*

$$\mathbf{Z} \in \mathbb{G}^{K \times K}, \quad \text{rank}(\mathbf{Z}) = K$$

if applicable: $|\det(\mathbf{Z})| = 1$ (unimodular)

- \mathbf{C} , the “*reduced channel*”, or $\mathbf{F}_{\text{LE},\mathbf{C}}$, the “*equalization matrix*”, have desired properties

Required: to solve this factorization problem, we need

- a meaningful criterion
- a practical algorithm

Factorization Criteria (II)

Criterion II:

[TMK'07]

- for square channel matrices, the ZF equalization matrix reads

$$\mathbf{F}_{\text{LE}} = \mathbf{C}^{-1} = (\mathbf{H}\mathbf{Z}^{-1})^{-1} = \mathbf{Z}\mathbf{H}^{-1}$$

- the squared *row norms* of \mathbf{F}_{LE} give the noise enhancement

- factorization task $(\mathbf{X}^{-\text{H}} = (\mathbf{X}^{\text{H}})^{-1} = (\mathbf{X}^{-1})^{\text{H}})$

$$\mathbf{H}^{-\text{H}} = \mathbf{F}_{\text{II}}^{\text{H}} \mathbf{Z}_{\text{II}}^{-\text{H}}$$

- the *column vectors* of $\mathbf{F}_{\text{II}}^{\text{H}}$ should be as short as possible
- if \mathbf{Z}_{II} is an unimodular integer matrix, $\mathbf{Z}_{\text{II}}^{-\text{H}}$ has also this property
- for non-square channel matrices the left pseudoinverse is used

$$(\mathbf{H}^+)^{\text{H}} = \mathbf{F}_{\text{II}}^{\text{H}} \mathbf{Z}_{\text{II}}^{-\text{H}}$$

$$(\mathbf{H} \in \mathbb{C}^{N \times K}, N \geq K)$$

Factorization Criteria

Criterion I:

[YW'02], [WF'03]

- lattice reduction may directly applied to the channel matrix \mathbf{H}

$$\mathbf{H} = \mathbf{C}_I \mathbf{Z}_I$$

- typically, the *orthogonality defect* of $\mathbf{C}_I = [\mathbf{c}_1 \cdots \mathbf{c}_K]$ is minimized

$$\delta(\mathbf{C}_I) = \frac{\prod_{k=1}^K \|\mathbf{c}_k\|}{|\det(\mathbf{C}_I)|}$$

- this means that the basis vectors \mathbf{c}_k , the *column vectors* of \mathbf{C}_I should be as short as possible (have small Euclidean norm)

\Rightarrow *shortest basis/independent vector problem*

- a substitute criterion is optimized, instead of system performance

Factorization Criteria (III)

Criterion III:

[WBKK'04]

- the MMSE solution can be calculated as ZF solution for the *augmented* channel matrix

[Has'00]

- factorization task ($\zeta = \sigma_n^2 / \sigma_x^2$)

$$\begin{bmatrix} \mathbf{H} \\ \sqrt{\zeta} \mathbf{I} \end{bmatrix} \stackrel{\text{def}}{=} \mathcal{H} = \mathbf{C}_{\text{III}} \mathbf{Z}_{\text{III}} = \begin{bmatrix} \mathbf{C}_{\text{III}} \\ \sqrt{\zeta} \mathbf{Z}_{\text{III}}^{-1} \end{bmatrix} \mathbf{Z}_{\text{III}}$$

- optimum MMSE equalization matrix

$$\begin{aligned} \mathbf{F}_{\text{LE,MMSE},\mathbf{C}} &= \left[(\mathbf{C}_{\text{III}}^{\text{H}} \mathbf{C}_{\text{III}})^{-1} \mathbf{C}_{\text{III}}^{\text{H}} \right]_{\text{left } K \text{ columns}} \\ &= (\mathbf{C}_{\text{III}}^{\text{H}} \mathbf{C}_{\text{III}} + \zeta \mathbf{Z}_{\text{III}}^{-\text{H}} \mathbf{Z}_{\text{III}}^{-1})^{-1} \mathbf{C}_{\text{III}}^{\text{H}} \\ &= \mathbf{Z}_{\text{III}} (\mathbf{H}^{\text{H}} \mathbf{H} + \zeta \mathbf{I})^{-1} \mathbf{H}^{\text{H}} = \mathbf{Z}_{\text{III}} \mathbf{F}_{\text{LE,MMSE},\mathbf{H}} \end{aligned}$$

- the *column vectors* of \mathbf{C}_{III} should be as short as possible
- as in Criterion I, a substitute measure is optimized
- in almost all cases $\mathbf{Z}_I = \mathbf{Z}_{\text{III}}$

[Fis'11]

Factorization Criteria (IV)

Criterion IV:

[FWSSSA'12], [ZNEG'14], [FCS'16]

- applying MMSE linear equalization, the noise enhancement is given by

$$\begin{aligned} E_k &= [\Phi_{ee}]_{k,k} / \sigma_n^2 = [(C^H C + \zeta Z^{-H} Z^{-1})^{-1}]_{k,k} \\ &= [Z(H^H H + \zeta I)^{-1} Z^H]_{k,k} = z_k^H (H^H H + \zeta I)^{-1} z_k \\ &= z_k^H L L^H z_k = \|L^H z_k\|^2 \end{aligned}$$

with $Z^H = [z_1, \dots, z_K]$

- L is any *square root* of $(H^H H + \zeta I)^{-1} = (\mathcal{H}^H \mathcal{H})^{-1}$; we may choose

$$L = \mathcal{H}^+$$

- factorization task (using $L^H Z^H = (\mathcal{H}^+)^H Z^H \stackrel{\text{def}}{=} \mathcal{F}^H$)

$$(\mathcal{H}^+)^H = \mathcal{F}_{IV}^H Z_{IV}^{-H}$$

- the *column vectors* of \mathcal{F}_{IV}^H should be as short as possible

Constraint on Z

Constraint on the Integer Matrix $Z \in \mathbb{G}^{K \times K}$:

- typically, in LRA equalization it has been forced

$$|\det(Z)| = 1 \quad \text{unimodular matrix}$$

hence a *change of basis* is performed

⇒ *Lattice Basis Reduction*

- in IF equalization, the constraint is relaxed to

$$\text{rank}(Z) = K \quad \text{full-rank matrix}$$

(to be precise: $\text{rank}(Z_{\mathbb{F}}) = K$)

⇒ *Shortest Independent Vector Problem*

Observation:

[FCS'16]

using the LRA equalization structure, unimodularity of Z is not required

⇒ *both, LRA and IF, can use the same factorization criterion and the same constraint on Z !*

Factorization Criteria (V)

Summary: (in each case $Z \in \mathbb{G}^{K \times K}$)

- the criteria available in the literature can be classified as follows

based on	channel matrix H ("ZF solution")	augmented matrix \mathcal{H} ("MMSE solution")
H	$H = C Z$ [YW'02], [WF'03]	$\mathcal{H} = C Z$ [WBKK'04], [Fis'11]
$(H^+)^H$	$(H^+)^H = F^H Z^{-H}$ [TMK'07]	$(\mathcal{H}^+)^H = \mathcal{F}^H Z^{-H}$ [ZNEG'14], [FCS'16]

Involved lattices:

H : lattice spanned by channel matrix

$(H^+)^H$: dual lattice

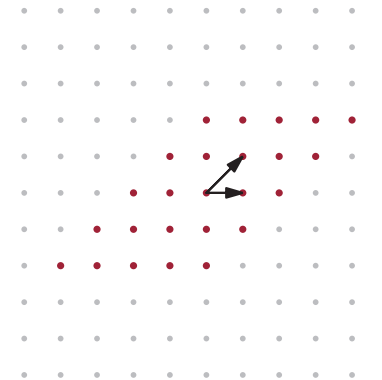
[LMG'09]

Constraint on Z

Visualization: (real-valued example $K = 2, |\mathcal{A}| = 5$)

- vectors $\bar{x} = Zx$, with $x \in \mathcal{A}^K$

- example $Z = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\det(Z) = 1$

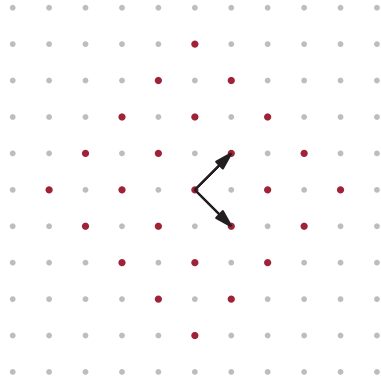


Constraint on \mathbf{Z}

Visualization: (real-valued example $K = 2, |\mathcal{A}| = 5$)

■ vectors $\tilde{\mathbf{x}} = \mathbf{Z}\mathbf{x}$, with $\mathbf{x} \in \mathcal{A}^K$

■ example $\mathbf{Z} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$, $\det(\mathbf{Z}) = 2$



Lattices and Lattice Problems (II)

Gram-Schmidt (GS) Orthogonalization:

[Fis'10]

■ any matrix $\mathbf{G} \in \mathbb{C}^{N \times K}$ can be decomposed into the form

$$\mathbf{G} = \mathbf{G}^\circ \mathbf{R}$$

with - $\mathbf{G}^\circ = [\mathbf{g}_1^\circ, \dots, \mathbf{g}_K^\circ]$: Gram-Schmidt orthogonalization of \mathbf{G}

with orthogonal columns $\mathbf{g}_1^\circ, \dots, \mathbf{g}_K^\circ$

- $\mathbf{R} = [r_{l,k}] \in \mathbb{C}^{K \times K}$: upper triangular with unit main diagonal

■ successive procedure

for $k = 1, \dots, K$

$$\mathbf{g}_k^\circ = \mathbf{g}_k - \sum_{l=1}^{k-1} r_{l,k} \mathbf{g}_l^\circ$$

$$\text{with } r_{l,k} = \frac{(\mathbf{g}_l^\circ)^H \mathbf{g}_k^\circ}{\|\mathbf{g}_l^\circ\|_2^2}, \quad l = 1, \dots, k$$

Lattices and Lattice Problems

Lattice:

■ we deal with complex-valued lattices

$$\Lambda(\mathbf{G}) = \left\{ \lambda = \sum_{k=1}^K z_k \mathbf{g}_k = \mathbf{G} \begin{bmatrix} z_1 \\ \vdots \\ z_K \end{bmatrix} \mid z_k \in \mathbb{G} \right\} \stackrel{\text{def}}{=} \mathbf{G}\mathbb{G}^K$$

where

$$\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_K] \in \mathbb{C}^{N \times K}$$

is its generator matrix (basis) consisting of

$K \in \mathbb{N}$ linearly independent basis vectors $\mathbf{g}_k \in \mathbb{C}^N$, $N \geq K$, $N \in \mathbb{N}$
(N -dimensional lattice of rank K)

Alternative Description:

■ instead of dealing with the complex-valued generator matrix \mathbf{G} ,
one can use the real-valued equivalent

[Win'04]

$$\mathbf{G}_{\text{real}} \stackrel{\text{def}}{=} \begin{bmatrix} \text{Re}\{\mathbf{G}\} & -\text{Im}\{\mathbf{G}\} \\ \text{Im}\{\mathbf{G}\} & \text{Re}\{\mathbf{G}\} \end{bmatrix}$$

of doubled dimension

Lattices and Lattice Problems (III)

Minkowski's Successive Minima:

■ k^{th} , $k = 1, \dots, K$, *successive minimum* of $\Lambda(\mathbf{G})$ [Cas'97], [LLS'90], [DKWZ'15]

$$\rho_k(\Lambda(\mathbf{G})) = \inf \{ r_k \mid \dim(\text{span}(\Lambda(\mathbf{G}) \cap \mathbf{B}_N(r_k))) = k \}$$

with - $\mathbf{B}_N(r)$: N -dimensional ball (over \mathbb{C}) with radius r centered at the origin

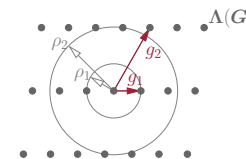
- $\text{span}(\cdot)$: linear span

■ $\rho_1(\Lambda(\mathbf{G}))$ is the norm of the shortest vector of the lattice $\Lambda(\mathbf{G})$

■ interpretation:

r_k has to be chosen as the smallest radius such that $\mathbf{B}_N(r_k)$ contains
 k linearly independent lattice vectors

■ Visualization:



Lattices and Lattice Problems (IV)

Given: a complex-valued lattice $\Lambda(\mathbf{G})$ of rank K

Shortest Independent Vector Problem (SIVP):

- find set $\mathcal{G} = \{\lambda_1, \dots, \lambda_K\}$ of K linearly independent vectors $\lambda_k \in \Lambda(\mathbf{G})$, such that

$$\max_{k=1, \dots, K} \|\lambda_k\| = \rho_K(\Lambda(\mathbf{G}))$$

- the largest vector has to be as short as possible; the norms of all shorter vectors do not matter

Successive Minima Problem (SMP):

- find set $\mathcal{G} = \{\lambda_1, \dots, \lambda_K\}$ of K linearly independent vectors $\lambda_k \in \Lambda(\mathbf{G})$, such that

$$\|\lambda_k\| = \rho_k(\Lambda(\mathbf{G})), \quad k = 1, \dots, K$$

- all lattice vectors in the set \mathcal{G} have to be as short as possible; naturally, SMP is also a solution to SIVP
- efficient strategies for solving the (C)SMP are available [DKWZ'15], [FCS'16]

Lattices and Lattice Problems (VI)

Lattice Basis Reduction:

- find set $\mathcal{G} = \{\lambda_1, \dots, \lambda_K\}$ of K linearly independent vectors $\lambda_k \in \Lambda(\mathbf{G})$, such that

$$\Lambda(\mathbf{G}) = \Lambda(\mathbf{G}_r)$$

with

$$\mathbf{G}_r = [\mathbf{g}_{r,1}, \dots, \mathbf{g}_{r,K}] = [\lambda_1, \dots, \lambda_K]$$

i.e., \mathbf{G}_r is a “reduced” basis of the lattice Λ

(the meaning of “reduced” depends on the criterion/algorithm)

- the generator matrices are related by

$$\mathbf{G}_r = \mathbf{G}\mathbf{U}$$

or

$$\mathbf{G} = \mathbf{G}_r \mathbf{U}^{-1}$$

where $\mathbf{U} \in \mathbb{G}^{K \times K}$ is unimodular, i.e., $|\det(\mathbf{U})| = 1$;
hence $\mathbf{U}^{-1} \in \mathbb{G}^{K \times K}$

(cf. factorization task $\mathbf{H} = \mathbf{C}\mathbf{Z}$)

Lattices and Lattice Problems (V)

Set of Linearly Independent Vectors:

- the obtained vectors are lattice points $\lambda_k \in \Lambda(\mathbf{G})$, hence

$$\lambda_k = \mathbf{G}\mathbf{u}_k, \quad \text{with } \mathbf{u}_k \in \mathbb{G}^K, \quad \forall k$$

- the matrix $\mathbf{V} \stackrel{\text{def}}{=} [\lambda_1, \dots, \lambda_K]$ is related to \mathbf{G} via

$$\mathbf{V} = \mathbf{G}\mathbf{U}$$

or

$$\mathbf{G} = \mathbf{V}\mathbf{U}^{-1}$$

with $\mathbf{U} \in \mathbb{G}^{K \times K}$ and $|\det(\mathbf{U})| \in \mathbb{G} \setminus \{0\}$

(cf. factorization task $(\mathbf{H}^+)^H = \mathbf{F}^H \mathbf{Z}^{-H}$)

Lattices and Lattice Problems (VII)

Lenstra-Lenstra-Lovász (LLL) Reduction:

[LLL'82]

- a generator matrix $\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_K] \in \mathbb{C}^{N \times K}$ with Gram-Schmidt orthogonal basis $\mathbf{G}^\circ = [\mathbf{g}_1^\circ, \dots, \mathbf{g}_K^\circ]$ and upper triangular matrix \mathbf{R} is called (C)LLL-reduced, if [GLM'09]

- for $1 \leq l < k \leq K$, it is *size-reduced* according to

$$|\operatorname{Re}\{r_{l,k}\}| \leq 0.5 \quad \text{and} \quad |\operatorname{Im}\{r_{l,k}\}| \leq 0.5$$

- for $k = 2, \dots, K$ and a parameter $0.5 < \delta \leq 1$

$$\|\mathbf{g}_k^\circ\|^2 \geq (\delta - |r_{k-1,k}|^2) \|\mathbf{g}_{k-1}^\circ\|^2$$

- the parameter δ controls the trade-off between “strength” of the LLL reduction and computational complexity — usually $\delta = 0.75$; the case $\delta = 1$ is denoted as *optimal LLL reduction* [A'03]
- for $\delta < 1$ the algorithm has polynomial complexity [A'03]

Lattices and Lattice Problems (VIII)

Hermite-Korkine-Zolotareff (HKZ) Reduction:

- a generator matrix $\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_K] \in \mathbb{C}^{N \times K}$ with Gram-Schmidt orthogonal basis $\mathbf{G}^\circ = [\mathbf{g}_1^\circ, \dots, \mathbf{g}_K^\circ]$ and upper triangular matrix \mathbf{R} is called (C)HKZ-reduced, if [LLS'90], [JD'13]

1. for $1 \leq l < k \leq K$, it is *size-reduced* according to

$$|\operatorname{Re}\{r_{l,k}\}| \leq 0.5 \quad \text{and} \quad |\operatorname{Im}\{r_{l,k}\}| \leq 0.5$$

2. for $k = 1, \dots, K$, the columns of \mathbf{G}° fulfill

$$\|\mathbf{g}_k^\circ\| = \rho_1(\Lambda(\mathbf{G}^{(k)}))$$

(shortest (non-zero) vector in $\Lambda(\mathbf{G}^{(k)})$)

- $\Lambda(\mathbf{G}^{(k)})$: sublattice of rank $K - k + 1$ and dimension N with generator matrix $\mathbf{G}^{(k)} = [0, \dots, 0, \mathbf{g}_k^\circ, \dots, \mathbf{g}_K^\circ] \mathbf{R}$
($\Lambda(\mathbf{G}^{(k)})$ is the orth. projection of $\Lambda(\mathbf{G})$ onto the orth. complement of $\{\mathbf{g}_1, \dots, \mathbf{g}_{k-1}\}$)
- since shortest vectors have to be found, the problem is NP-hard;
efficient (complex-valued) algorithms available [JD'13], [ZQW'12]

Application to Equalization

Recall: Criterion IV

- MMSE linear equalization via $\mathcal{F}^H = \mathbf{Z} \mathcal{H}^+ = \begin{bmatrix} f_1 \\ \vdots \\ f_K \end{bmatrix}$

- noise enhancement

$$E_k = \|\mathbf{f}_k\|^2 = \|(\mathcal{H}^+)^H \mathbf{z}_k\|^2 \rightarrow \min$$

with $\mathbf{Z}^H = [\mathbf{z}_1, \dots, \mathbf{z}_K]$

- factorization task

$$(\mathcal{H}^+)^H = \mathcal{F}^H \mathbf{Z}^{-H}$$

- the *column vectors* of \mathcal{F}^H should be as short as possible
- usually the maximum of the noise enhancement dominates

Lattices and Lattice Problems (IX)

Minkowski (MK) Reduction:

- a generator matrix $\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_K] \in \mathbb{C}^{N \times K}$ is called (C)MK-reduced, if [Min'1891], [ZQW'12]

$$\|\mathbf{g}_k\| \leq \|\mathbf{g}'_k\|, \quad k = 1, \dots, K$$

$$\forall \mathbf{G}' = [\mathbf{g}_1, \dots, \mathbf{g}_{k-1}, \mathbf{g}'_k, \dots, \mathbf{g}'_K]$$

with

$$\Lambda(\mathbf{G}') = \Lambda(\mathbf{G})$$

\mathbf{G} is Minkowski-reduced if for $k = 1, \dots, K$ the basis vector \mathbf{g}_k has minimum norm among all possible lattice points \mathbf{g}'_k for which the set $\{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{k-1}, \mathbf{g}'_k\}$ can be extended to a basis of $\Lambda(\mathbf{G})$

- in contrast to the SMP where only the K shortest *independent* lattice vectors have to be found, here the K shortest vectors have to be obtained that *form a basis of the lattice*
- efficient (real-valued) algorithm available [ZQW'12]
in the real-valued case, the calculation of a greatest common divisor (gcd) is required;
in the complex-valued case the gcd for Gaussian integers has to be used
(calculated via the Euclidean Algorithm)

Application to Equalization (II)

Factorization Problem: $\mathbf{Z}^H = [\mathbf{z}_1, \dots, \mathbf{z}_K]$

- $|\det(\mathbf{Z}^H)| = 1$ required

$$\mathbf{Z}^H = \underset{\substack{\mathbf{Z}^H \in \mathbb{C}^{K \times K} \\ |\det(\mathbf{Z}^H)|=1}}{\operatorname{argmin}} \max_{k=1, \dots, K} \|(\mathcal{H}^+)^H \mathbf{z}_k\|^2$$

\Rightarrow *shortest basis problem (SBP)*

- the MK-reduced basis is directly defined by the length of its basis vectors
— it consists of the K shortest lattice vectors that form a basis of the lattice
(not only the maximum norm is minimized)

\Rightarrow *Minkowski reduction gives the optimum integer matrix \mathbf{Z}*

- full-rank matrix \mathbf{Z} sufficient

$$\mathbf{Z}^H = \underset{\substack{\mathbf{Z}^H \in \mathbb{C}^{K \times K} \\ \operatorname{rank}(\mathbf{Z}^H)=K}}{\operatorname{argmin}} \max_{k=1, \dots, K} \|(\mathcal{H}^+)^H \mathbf{z}_k\|^2$$

\Rightarrow *shortest independent vector problem (SIVP)*

- this problem is optimally solved—in a stricter sense—if the K successive minima of $\Lambda((\mathcal{H}^+)^H)$ are obtained

\Rightarrow *Minkowski's successive minima give the optimum integer matrix \mathbf{Z}*

Numerical Results

Obtained Vectors \mathbf{z}_i :

■ factorization of $\mathbf{G} = \begin{bmatrix} 0.8 + 0.5j & -0.8 + 0.1j & -0.1 - 0.6j & 0.7 - 1.0j \\ -0.5 + 0.4j & -0.1 - 0.2j & -1.1 + 0.8j & -0.3 - 1.0j \\ 0.3 - 0.5j & 1.1 + 2.1j & 0.8 - 0.3j & 0.4 + 1.4j \\ -0.3 - 0.2j & -1.0 + 0.0j & 0.6 - 0.4j & 0.2 + 1.1j \end{bmatrix}$

\mathbf{u}_i	$\begin{bmatrix} 3+0j \\ 0+1j \\ -2-1j \\ 1-2j \end{bmatrix}$	$\begin{bmatrix} 2+0j \\ 0+1j \\ -2-1j \\ 1-2j \end{bmatrix}$	$\begin{bmatrix} 1+0j \\ 0+0j \\ -1-1j \\ 1-1j \end{bmatrix}$	$\begin{bmatrix} 1+1j \\ 0+0j \\ 0-1j \\ 1+0j \end{bmatrix}$	$\begin{bmatrix} 1+0j \\ 0+0j \\ -1+0j \\ 0-1j \end{bmatrix}$	$\begin{bmatrix} 3+0j \\ 0+1j \\ -3-1j \\ 1-3j \end{bmatrix}$	$\begin{bmatrix} 4-1j \\ 0+1j \\ -5-1j \\ 1-4j \end{bmatrix}$	$\begin{bmatrix} 4+0j \\ 0+1j \\ -4-1j \\ 1-3j \end{bmatrix}$	$\begin{bmatrix} 3+0j \\ 0+1j \\ -4-1j \\ 1-3j \end{bmatrix}$	$\begin{bmatrix} 1+0j \\ 0+0j \\ 0-1j \\ 1+0j \end{bmatrix}$	$\begin{bmatrix} 0+0j \\ 0+0j \\ 0-1j \\ 0+0j \end{bmatrix}$	$\begin{bmatrix} 1+0j \\ 0+0j \\ 0+0j \\ 0+0j \end{bmatrix}$
λ_i	$\begin{bmatrix} 0.6-0.4j \\ -0.6+0.2j \\ 0.1-0.0j \\ -0.1-0.7j \end{bmatrix}$	$\begin{bmatrix} -0.2-0.9j \\ -0.1-0.2j \\ -0.2+0.5j \\ 0.2-0.5j \end{bmatrix}$	$\begin{bmatrix} 0.0-0.5j \\ 0.1+0.0j \\ 1.0-0.0j \\ 0.0+0.5j \end{bmatrix}$	$\begin{bmatrix} 0.4+0.4j \\ -0.4+0.0j \\ 0.9+0.4j \\ -0.3+0.0j \end{bmatrix}$	$\begin{bmatrix} -0.1+0.4j \\ -0.4-0.1j \\ 0.9-0.6j \\ 0.2+0.0j \end{bmatrix}$	$\begin{bmatrix} -0.3-0.5j \\ -0.5-0.3j \\ 0.7-0.1j \\ 0.4-0.5j \end{bmatrix}$	$\begin{bmatrix} 0.2-0.3j \\ 0.6-0.7j \\ 0.3-0.7j \\ -0.2+0.2j \end{bmatrix}$	$\begin{bmatrix} 0.6+0.6j \\ 0.1-0.7j \\ 0.2-0.3j \\ -0.5-0.3j \end{bmatrix}$	$\begin{bmatrix} -0.2+0.1j \\ 0.6-1.1j \\ -0.1+0.2j \\ -0.2-0.1j \end{bmatrix}$	$\begin{bmatrix} 0.9-0.4j \\ 0.0+0.5j \\ 0.4+0.1j \\ -0.5+0.3j \end{bmatrix}$	$\begin{bmatrix} 0.1-0.9j \\ 0.5+0.1j \\ 0.1+0.6j \\ -0.2+0.5j \end{bmatrix}$	$\begin{bmatrix} 0.8+0.5j \\ -0.5+0.4j \\ 0.3-0.5j \\ -0.3-0.2j \end{bmatrix}$
$\ \lambda_i\ ^2$	1.43	1.48	1.51	1.54	1.55	1.59	1.64	1.69	1.72	1.73	1.74	1.77
rank	1	2	3	3	3	3	4	4	4	4	4	4
LLL $\delta = .75$	X			X				X				X
LLL $\delta = 1$			X	X		X	X					
HKZ	X	X						X		X		
MK	X	X		X			X					
SMP	X	X	X				X					

■ here: $\det(\mathbf{Z}_{\text{SMP}}) = 1 + j$

Numerical Results (III)

Distribution of $|\det(\mathbf{Z})|$:

- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian
- $K = N = 6$
- criterion IV — SMP

[DKWZ'15], [FCS'16]

$ \det(\mathbf{Z}) =$	1	$\sqrt{2}$	2	$\sqrt{5}$
$\sigma_x^2/\sigma_n^2 \cong 0$ dB	99.6 %	0.45 %	0.0002 %	—
$\sigma_x^2/\sigma_n^2 \cong 10$ dB	96.2 %	3.83 %	0.02 %	0.002 %
$\sigma_x^2/\sigma_n^2 \cong 20$ dB	95.4 %	4.45 %	0.03 %	0.003 %
$\sigma_x^2/\sigma_n^2 \cong 30$ dB	95.5 %	4.48 %	0.03 %	0.003 %

Numerical Results (II)

Distribution of $|\det(\mathbf{Z})|$:

- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- $\sigma_x^2/\sigma_n^2 \cong 20$ dB
- criterion IV — SMP

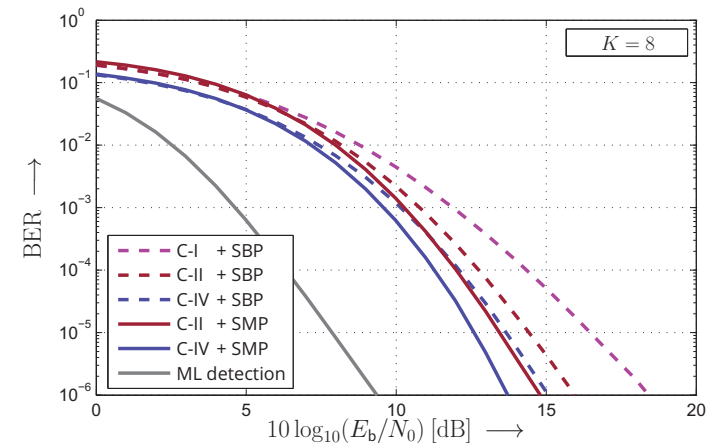
[DKWZ'15], [FCS'16]

$ \det(\mathbf{Z}) =$	1	$\sqrt{2}$	2	$\sqrt{5}$
$K = 2$	100 %	—	—	—
$K = 3$	99.8 %	0.2 %	—	—
$K = 4$	99.0 %	1.0 %	—	—
$K = 5$	97.5 %	2.4 %	0.005 %	—
$K = 6$	95.6 %	4.5 %	0.03 %	0.003 %
$K = 7$	92.7 %	7.1 %	0.15 %	0.02 %
$K = 8$	89.3 %	10.2 %	0.39 %	0.06 %

Numerical Results (IV)

Bit Error Rate: LRA structure; linear MMSE equalization — different criteria and constraints

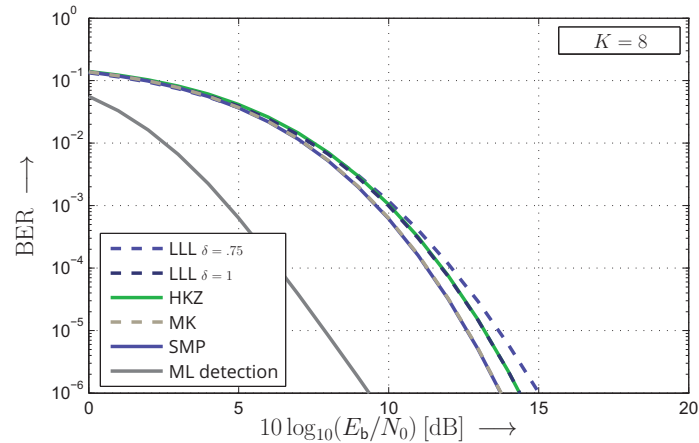
- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- uncoded transmission; 16QAM signaling; $E_b/N_0 = \sigma_x^2/(\sigma_n^2 \log_2(16))$



Numerical Results (V)

Bit Error Rate: LRA structure; linear MMSE equalization; criterion C-IV — different algorithms

- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- uncoded transmission; 16QAM signaling; $E_b/N_0 = \sigma_x^2/(\sigma_n^2 \log_2(16))$



Numerical Results (VII)

Percentages “MK = SMP” and “MK = SIVP”:

- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian
- $K = N$; criterion IV [DKWZ'15], [FCS'16]

SMP $K = N =$	2	4	6	8	10
$\sigma_x^2/\sigma_n^2 \cong 15$ dB	100 %	99.0 %	95.7 %	90.3 %	83.8 %
$\sigma_x^2/\sigma_n^2 \cong 20$ dB	100 %	99.0 %	95.6 %	89.8 %	82.3 %
$\sigma_x^2/\sigma_n^2 \rightarrow \infty$	100 %	99.0 %	95.5 %	89.4 %	81.5 %

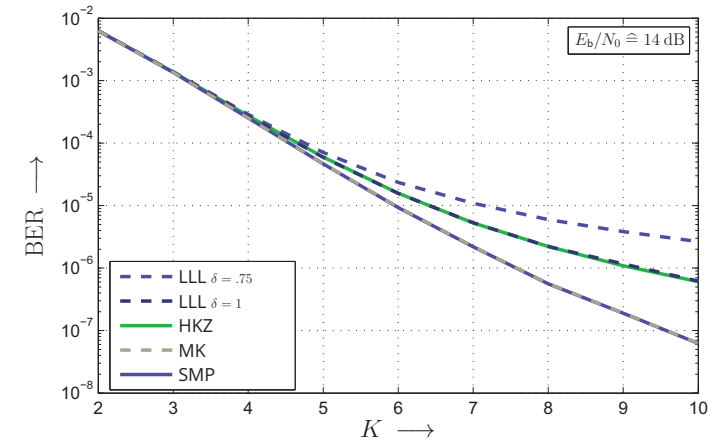
SIVP $K = N =$	2	4	6	8	10
$\sigma_x^2/\sigma_n^2 \cong 15$ dB	100 %	99.2 %	97.0 %	94.0 %	90.6 %
$\sigma_x^2/\sigma_n^2 \cong 20$ dB	100 %	99.2 %	97.0 %	93.5 %	89.3 %
$\sigma_x^2/\sigma_n^2 \rightarrow \infty$	100 %	99.2 %	96.9 %	93.2 %	88.5 %

for the complex case and $K = N = 2$, an MK-reduced basis is always a solution to the SMP

Numerical Results (VI)

Bit Error Rate: LRA structure; linear MMSE equalization; criterion C-IV — different algorithms

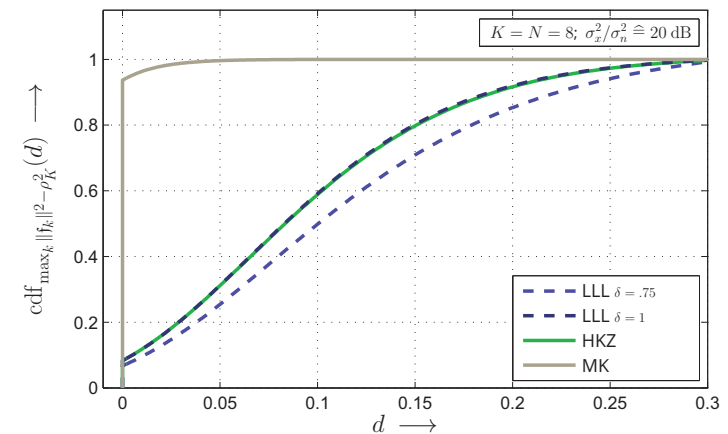
- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- uncoded transmission; 16QAM signaling



Numerical Results (VIII)

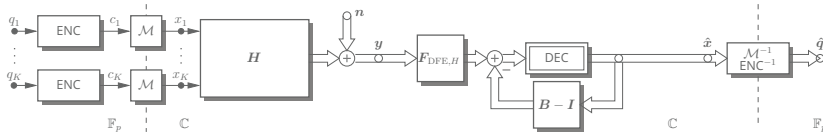
Distribution of Deviation from Optimum:

- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian
- $K = N = 8$; $\sigma_x^2/\sigma_n^2 \cong 20$ dB
- criterion IV [DKWZ'15], [FCS'16]



Decision-Feedback Equalization

Decision-Feedback Equalization: aka successive interference cancellation, V-BLAST



- QR decomposition of the channel matrix:
 Q : orthogonal matrix; B : upper triangular, unit main diagonal

$$H = QB$$

- signal after feedforward processing with $F_{DFE,H} \stackrel{\text{def}}{=} (Q^H Q)^{-1} Q^H$

$$r = F_{DFE,H} y = Bx + \tilde{n}$$

- spatially causal signal transmission matrix B
- Gaussian noise vector \tilde{n} with correlation matrix $\sigma_{\tilde{n}}^2 (Q^H Q)^{-1}$
i.e., with $Q = [q_1 \dots q_K]$ noise variances $\sigma_{\tilde{n}_k}^2 = \sigma_{\tilde{n}}^2 / \|q_k\|^2$
- decisions are taken successively (order $K, \dots, 1$)

Decision-Feedback Equalization (II)

Optimum Detection Order: V-BLAST ordering [WFGV'98]

- signal-to-noise ratio in component k is proportional to $\|q_k\|^2$
 \Rightarrow for $k = K, \dots, 1$: the norm of the vector q_k should be the largest among the remaining components $1, \dots, k$
- BLAST ordering requires great effort

Simpler Strategy: [WBKK'03], [Fis'10]

- instead of *maximizing* $\|q_k\|^2$ in sequence $k = K, K-1, \dots, 1$ it is *minimized* in sequence $k = 1, 2, \dots, K$
 \Rightarrow for $k = 1, \dots, K$: the norm of the vector q_k should be the smallest among the remaining components k, \dots, K
- **Gram-Schmidt procedure with pivoting**

Simple but Optimum Strategy: [LMG'09]

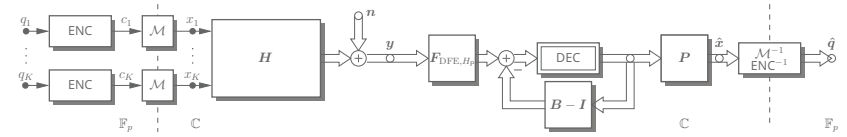
- do not apply Gram-Schmidt procedure with pivoting to \mathcal{H} , but to $(\mathcal{H}^+)^H$
 \Rightarrow use factorization

$$(\mathcal{H}^+)^H P^{-H} = \mathcal{F}^H B^{-H}$$

order within GS proc.: $k = K, \dots, 1$; i.e., B^{-H} should be lower triangular

Decision-Feedback Equalization

Decision-Feedback Equalization: aka successive interference cancellation, V-BLAST



- **sorted** QR decomposition of the channel matrix:
 Q : orthogonal matrix; B : upper triangular, unit main diagonal; P : permutation matrix

$$HP \stackrel{\text{def}}{=} H_P = QB$$

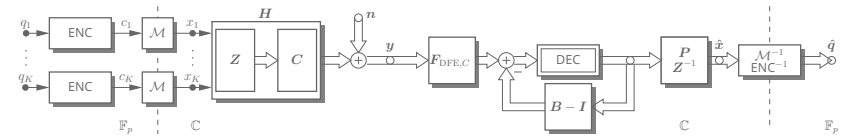
\Rightarrow criterion for sorting required

MMSE version of DFE:

- ZF version for $K = N$: $HP = F^{-1}B$
- MMSE version of DFE: $\mathcal{H}P = \mathcal{F}^+B$
with $\mathcal{H} = \begin{bmatrix} H \\ \sqrt{C}I \end{bmatrix}$

LRA Decision-Feedback Equalization

LRA Decision-Feedback Equalization: [YW'02], [WF'03]



Strategies:

- obvious [YW'02], [WF'03]
perform i) factorization $H = CZ$;
ii) sorted QR decomposition $CP = QB$
- more efficient [WBKK'04], [Fis'11]
reuse Q and R anyway calculated within LLL or HKZ
- optimum [LMG'09], [Fis'10], [SF'17]
do sorting, Gram-Schmidt procedure, and size reduction jointly

LRA Decision-Feedback Equalization (II)

Pseudocode of Factorization Approach:

[SF'17]

```

[Q, R, T] = GramSchmidtSort_LRA(G)
1  Q = G, R = I, T = I
2  k = 1
3  while k ≤ K {
4      q_s = shortest vector in Λ([q_k, ..., q_K])
5      if ||q_s||² ≠ ||q_k||² {
6          q_k = q_s
7          update Q, R, T such that Λ(QR) = Λ(G)
8      }
9      for i = k + 1, ..., K {
10         r_ki = q_k^H q_i / ||q_k||²
11         q_i = q_i - r_ki q_k
12     }
13     k = k + 1
14 }
    
```

LRA Decision-Feedback Equalization (IV)

Discussion:

- the size-reduction step of HKZ is not present;
as it changes only \mathbf{R} it is of no relevance for performance of LRA DFE
⇒ *effective HKZ reduction*
 - for $\mathbf{G} = (\mathcal{H}^+)^H$ the algorithm returns $\mathbf{Z}^H = \mathbf{T}$ and $\mathcal{F}^H = \mathbf{Q}$ with
 - V-BLAST sorting
 - the columns of \mathcal{F}^H have minimum norm
(optimal worst-link performance as in classical V-BLAST but for LRA equalization)
 - this optimum is achieved with an unimodular \mathbf{Z} ;
a relaxation to $\text{rank}(\mathbf{Z}) = K$ is not required [OEN'13]
- ⇒ *successive IF and LRA DFE both can be restricted to unimodular \mathbf{Z}*

LRA Decision-Feedback Equalization (III)

Recall: Hermite-Korkine-Zolotareff (HKZ) Reduction

- a generator matrix $\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_K] \in \mathbb{C}^{N \times K}$ with Gram-Schmidt orthogonal basis $\mathbf{G}^\circ = [\mathbf{g}_1^\circ, \dots, \mathbf{g}_K^\circ]$ and upper triangular matrix \mathbf{R} is called (C)HKZ-reduced, if [LLS'90], [D'13]

1. for $1 \leq l < k \leq K$, it is *size-reduced* according to

$$|\text{Re}\{r_{l,k}\}| \leq 0.5 \quad \text{and} \quad |\text{Im}\{r_{l,k}\}| \leq 0.5$$

2. for $k = 1, \dots, K$, the columns of \mathbf{G}° fulfill

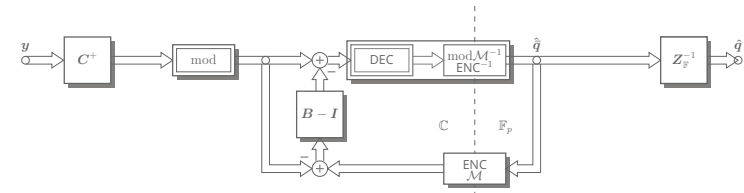
$$\|\mathbf{g}_k^\circ\| = \rho_1(\Lambda(\mathbf{G}^{(k)}))$$

(shortest (non-zero) vector in $\Lambda(\mathbf{G}^{(k)})$)

- $\Lambda(\mathbf{G}^{(k)})$: sublattice with generator matrix $\mathbf{G}^{(k)} = [0, \dots, 0, \mathbf{g}_k^\circ, \dots, \mathbf{g}_K^\circ] \mathbf{R}$

LRA Decision-Feedback Equalization (V)

LRA Decision-Feedback Equalization:



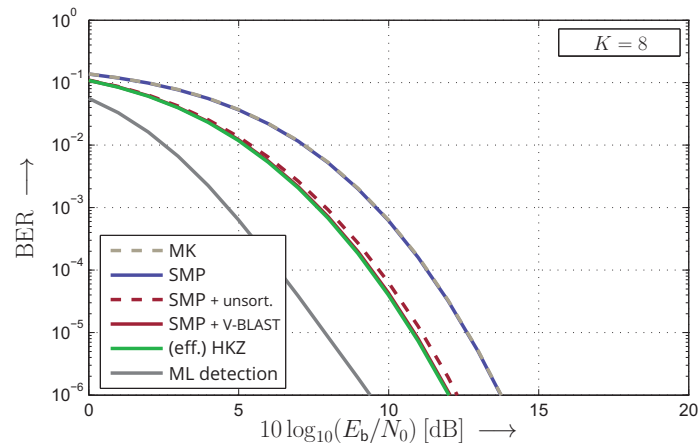
- redraw to noise-prediction structure [Fis'02]
- apply modulo reduction w.r.t. Λ_s
- exchange \mathbf{Z}^{-1} and demapping/encoder inverse
- combine to demapping modulo Λ_s

⇒ *successive IF only works in noise-prediction structure*

Numerical Results

Bit Error Rate: LRA structure; linear MMSE equalization; criterion C-IV — different algorithms

- \mathbf{H} : i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- uncoded transmission; 16QAM signaling; $E_b/N_0 = \sigma_x^2 / (\sigma_n^2 \log_2(16))$



References

References

- [AEVZ'02] E. Agrell, T. Eriksson, A. Vardy, K. Zeger. Closest Point Search in Lattices. *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.
- [A'03] A. Akhavi. The Optimal LLL Algorithm is Still Polynomial in Fixed Dimension. *Theoretical Computer Science*, vol. 297, pp. 3–23, Mar. 2003.
- [Cas'97] J.W.S. Cassels. *An Introduction to the Geometry of Numbers*. Springer Berlin/Heidelberg, Reprint of the 1971 Edition, 1997.
- [DKWZ'15] L. Ding, K. Kansanen, Y. Wang, J. Zhang. Exact SMP Algorithms for Integer Forcing Linear MIMO Receivers. *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6955–6966, Dec. 2015.
- [FSK'13] C. Feng, D. Silva, F.R. Kschischang. An Algebraic Approach to Physical-Layer Network Coding. *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7576–7596, Nov. 2013.
- [Fis'02] R.F.H. Fischer. *Precoding and Signal Shaping for Digital Transmission*. John Wiley & Sons, Inc., New York, 2002.
- [Fis'10] R.F.H. Fischer. From Gram–Schmidt Orthogonalization via Sorting and Quantization to Lattice Reduction. In *Joint Workshop on Coding and Communications*, Santo Stefano Belbo, Italy, Oct. 2010.
- [Fis'11] R.F.H. Fischer. Efficient Lattice-Reduction-Aided MMSE Decision-Feedback Equalization. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Prag, Czech Republic, May 2011.
- [FWSSA'12] R.F.H. Fischer, C. Windpassinger, C. Stierstorfer, C. Siegl, A. Schenk, Ü. Abay. Lattice-Reduction-Aided MMSE Equalization and the Successive Estimation of Correlated Data. *AEÜ—Int. Journal of Electronics and Communications*, vol. 65, no. 8, pp. 688–693, Aug. 2011.
- [FCS'16] R.F.H. Fischer, M. Cyran, S. Stern. Factorization Approaches in Lattice-Reduction-Aided and Integer-Forcing Equalization. In *International Zurich Seminar on Communications*, Zurich, Switzerland, March 2016.
- [GLM'09] Y.H. Gan, C. Ling, W.H. Mow. Complex Lattice Reduction Algorithm for Low-Complexity Full-Diversity MIMO Detection. *IEEE Transactions on Signal Processing*, vol. 57, no. 7, pp. 2701–2710, July 2009.

Summary

Low-Complexity Equalization Schemes:

- tight relation between LRA and IF equalization
⇒ *structure how equalization and decoding are combined*
- performance measure for defining the factorization task
⇒ *optimization criterion*
- constraints on the integer matrix — SBP vs. SIVP
⇒ *algorithms for performing the factorization*

Optimum Integer Matrix \mathbf{Z} :

- linear equalization
 - $|\det(\mathbf{Z})| = 1$ *Minkowski reduction gives the optimum*
 - $\text{rank}(\mathbf{Z}) = K$ *Minkowski's successive minima give the optimum*
- decision-feedback equalization
(effective) HKZ reduction gives the optimum
(relaxation to $|\det(\mathbf{Z})| > 1$ not required)

Dualization:

- transmitter-side precoding for broadcast channel
(LRA / IF precoding)

[HC'13], [HNS'14], [SF'15]

References

- [Has'00] B. Hassibi. An Efficient Square-Root Algorithm for BLAST. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 11737–11740, 2000.
- [HNS'14] W. He, B. Nazer, S. Shamai. Uplink-Downlink Duality for Integer-Forcing. In *IEEE International Symposium on Information Theory*, pp. 2544–2548, 2014.
- [HC'13] S.-N. Hong, G. Caire. Compute-and-Forward Strategies for Cooperative Distributed Antenna Systems. *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5227–5243, Sept. 2013.
- [JD'13] H. Jiang, S. Du. Complex Korkine-Zolotareff Reduction Algorithm for Full-Diversity MIMO Detection. *IEEE Communications Letters*, vol. 17, no. 2, pp. 381–384, Feb. 2013.
- [LLS'90] J.C. Lagarias, H.W. Lenstra, C.P. Schnorr. Korkin-Zolotarev Bases and Successive Minima of a Lattice and its Reciprocal Lattice. *Combinatorica*, vol. 10, no. 4, pp. 333–348, 1990.
- [LL'82] A.K. Lenstra, H.W. Lenstra, L. Lovász. Factoring Polynomials with Rational Coefficients, *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 1982.
- [LMG'09] C. Ling, W.H. Mow, L. Gan. Dual-Lattice Ordering and Partial Lattice Reduction for SIC-Based MIMO Detection. *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 6, pp. 975–985, Dec. 2009.
- [Min'1891] H. Minkowski. Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen. *Journal für die reine und angewandte Mathematik*, vol. 107, pp. 278–297, 1891.
- [NG'11] B. Nazer, M. Gastpar. Compute-and-Forward: Harnessing Interference Through Structured Codes. *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.
- [OEN'13] O. Ordentlich, U. Erez, B. Nazer. Successive Integer-Forcing and its Sum-Rate Optimality. In *Annual Allerton Conference*, pp. 282–292, Oct. 2013.
- [SF'15] S. Stern, R. Fischer. Lattice-Reduction-Aided Preequalization over Algebraic Signal Constellations. In *9th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Cairns, Australia, Dec. 2015.
- [SF'17] S. Stern, R.F.H. Fischer. V-BLAST in Lattice Reduction and Integer Forcing. In *International Symposium on Information Theory*, Aachen, Germany, June 2017.

References

- [TMK'07] M. Taherzadeh, A. Mobasher, A.K. Khandani. LLL Reduction Achieves the Receive Diversity in MIMO Decoding. *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4801–4805, Dec. 2007.
- [WF'03] C. Windpassinger, R.F.H. Fischer. Low-Complexity Near-Maximum-Likelihood Detection and Precoding for MIMO Systems using Lattice Reduction. In *Proceedings of IEEE Information Theory Workshop*, pp. 345–348, Paris, France, March/April 2003.
- [Win'04] C. Windpassinger. *Detection and Precoding for Multiple Input Multiple Output Channels*. Dissertation, Erlangen, June 2004.
- [WFGV'98] P.W. Wolniansky, G.J. Foschini, G.D. Golden, R.A. Valenzuela. V-BLAST: An Architecture for Realizing Very High Data Rates over the Rich-Scattering Wireless Channel. In *International Symposium on Signals, Systems, and Electronics*, pp. 295–300, Sep. 1998.
- [WBKK'03] D. Wübben, R. Böhnke, V. Kühn, K.D. Kammeyer. MMSE Extension of V-BLAST Based on Sorted QR Decomposition. In *IEEE Vehicular Technology Conference*, pp. 508–512, Orlando, Florida, USA, Oct. 2003.
- [WBKK'04] D. Wübben, R. Böhnke, V. Kühn, K.D. Kammeyer. Near-Maximum-Likelihood Detection of MIMO Systems using MMSE-Based Lattice Reduction. *IEEE International Conference on Communications*, pp. 798–802, Paris, France, June 2004.
- [YW'02] H. Yao, G. Wornell. Lattice-Reduction-Aided Detectors for MIMO Communication Systems. In *Proceedings of IEEE Global Telecommunications Conference*, pp. 424–428, Taipei, Taiwan, Nov. 2002.
- [ZNEG'14] J. Zhan, B. Nazer, U. Erez, M. Gastpar. Integer-Forcing Linear Receivers. *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7661–7685, Dec. 2014.
- [ZQW'12] W. Zhang, S. Qiao, Y. Wei. HKZ and Minkowski Reduction Algorithms for Lattice-Reduction-Aided MIMO Detection. *IEEE Transactions on Signal Processing*, vol. 60, no. 11, pp. 5963–5976, Nov. 2012.