**Lattice Reduction and Factorization for Equalization**

Robert F.H. Fischer  Sebastian Stern

Institut für Nachrichtentechnik, Universität Ulm

---

**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 $\eta$) not all $\mathcal{A}^\eta$ 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

---

**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
- 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 too 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 Voronoï region \( \mathcal{R}_V(\Lambda_s) \)
  (typically a sublattice of \( \Lambda_a \))
- **signal constellation**
  \[ \mathcal{A} = \Lambda_a \cap \mathcal{R}_V(\Lambda_s) \]
- **lattice code**
  do everything in \( N \) dimensions
  \[ \mathcal{C} = \Lambda_a \cap \mathcal{R}_V(\Lambda_s) \]

**Intuition (IV)**

**Equalization of MIMO Channel:**

\[ y = Hx + n \]

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 \( F_p \)
- mapping \( \mathcal{M} \) to signal point in \( \mathcal{C} \)

**Decoding:**
- lattice decoding (in signal space) w.r.t. to \( \Lambda_s \)
- demapping \( \mathcal{M}^{-1} \) to \( \hat{c} \in F_p \)
- encoder inverse ENC\(^{-1} \)

**Variant:**
- demapping modulo \( \Lambda_a \), i.e., \( \text{mod} \mathcal{M}^{-1} \)
**Structure of the Signals**

Visualization: (real-valued example $K = 2$, $A = \mathbb{Z}$, $|A| = 3$)

\[ x, Hx, y = Hx + n \]

Maximum-Likelihood Detection

Optimum Detection Rule: ML criterion $f_X(x)$: probability density function

\[ \hat{x} = \arg\max_{x \in A^K} f_Y(y | x) = \arg\min_{x \in A^K} \|y - Hx\|^2 \]

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

Lattice:
- $K$-dim. lattice spanned by basis vectors $b_1, b_2, \ldots, b_K$ — basis matrix
  \[ B = [b_1 \ b_2 \ \cdots \ b_K] \]
- real-valued lattice
  \[ \Lambda = \{ \lambda = \sum_{k=1}^{K} z_k b_k = B [z_1 \ z_2 \ \cdots \ z_K] \mid z_k \in \mathbb{Z} \} \]

Lattice Structure of the Signal:
- for $x \subset G^K = (\mathbb{Z} + j\mathbb{Z})^K$ the noise-free receive vectors
  \[ z = Hx \]
  are taken from the complex-valued lattice $\Lambda = HG^K$ spanned by the columns $h_k$ of the channel matrix
  \[ H = [h_1 \ h_2 \ \cdots \ h_K] \]

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: \( I: \) identity matrix; \( (\cdot)^{\dagger}: \) (left) pseudoinverse
  \[ F_{LE} \cdot H = I \quad \Rightarrow \quad F_{LE,ZF} = (H^H H)^{-1} H^H \]
- minimum mean-squared error criterion: \( \varsigma \approx 1/\sigma_e^2 \)
  \[ \text{error signal } e = F_{LE} y - x; \text{ error covariance matrix } \Phi_e = E\{ee^H\} \]
  \[ \text{trace } (\Phi_e) \rightarrow \min \quad \Rightarrow \quad F_{LE,MMSE} = (H^H H + \varsigma I)^{-1} H^H \]
Linear Equalization (II)

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:

\[
H = \begin{bmatrix} h_1 & h_2 \end{bmatrix}
\]

Linear Equalization (III)

Noise Enhancement:
- ZF solution \( F_{ZF} = (H^H H)^{-1} H^H \)

\[
r = F_{ZF} y = x + F_{ZF} n
\]
- noise variance (n i.i.d. components with variance \( \sigma_n^2 \))

\[
\sigma_{n_k}^2 = \sigma_n^2 \cdot \|f_k\|^2
\]
- noise enhancement

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

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

or with \( H = \begin{bmatrix} \mathbf{H} \end{bmatrix} \) we have \( F_{LE, MMSE} = (H^H H + \zeta I)^{-1} H^H \)
- error covariance matrix

\[
\Phi_{ee} / \sigma_n^2 = (H^H H + \zeta I)^{-1} = (H^H H)^{-1}
\]
- noise enhancement

\[
E_k = \left[ \frac{\Phi_{ee}}{\sigma_n^2} \right]_{k,k} = \|f_k\|^2
\]

Visualization:

\[
H = \begin{bmatrix} h_1 & h_2 \end{bmatrix}
\]

\[
C = \begin{bmatrix} c_1 & c_2 \end{bmatrix}
\]

\[
= HZ, \quad Z \in \mathbb{Z}^{2 \times 2} / \{ \text{det}(Z) = 1 \}
\]
Lattice-Reduction-Aided Equalization

Visualization:

\[
H = \begin{bmatrix} h_1 & h_2 \end{bmatrix}
\]
\[
C = \begin{bmatrix} c_1 & c_2 \end{bmatrix}
= HZ , \quad Z \in \mathbb{Z}_{2 \times 2} | \det(Z) = 1
\]

Integer-Forcing Schemes

Compute-And-Forward Strategy in Relaying:

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

Equalization Schemes

Linear Equalization:

Lattice-Reduction-Aided Equalization: \([YW02],[WF03]\)

Compute-And-Forward Strategy in Relaying:

- the receiver decodes an integer linear combination of the codewords
- resolution of linear combinations at some central unit on 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 \([ZNEG14]\)
Integer-Forcing Equalization:

- 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 \( \mathbb{F}_p \)
  \( \Rightarrow \) \( \mathbb{Z}_p \) only has to have full rank

Fischer: Lattice Reduction and Factorization for Equalization

Structure

<table>
<thead>
<tr>
<th>Lattice-Reduction-Aided Equalization</th>
<th>Integer-Forcing Equalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-oriented</td>
<td>signal-oriented</td>
</tr>
<tr>
<td>joint receiver</td>
<td>distributed antenna systems</td>
</tr>
<tr>
<td>treat integer interference over</td>
<td></td>
</tr>
<tr>
<td>( \mathbb{G} = \mathbb{Z} + \mathbb{J} \mathbb{Z} )</td>
<td>( \mathbb{F}_p )</td>
</tr>
<tr>
<td>constraint on signal constellation and mapping</td>
<td>Incorporation of coding match arithmetic in ( \mathbb{R} ) (or ( \mathbb{C} )) and ( \mathbb{F}_p ) one-dim. ( p )-ary constellation, ( p ) a prime</td>
</tr>
</tbody>
</table>

Equalization Schemes

Points to discuss:

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

Factorization Task

Basic Idea of LRA Schemes:

- 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
  \( \mathbb{y} = \mathbb{Hx} + \mathbb{n} = \mathbb{CZx} + \mathbb{n} \)
- ZF linear equalization of \( \mathbb{C} \) — equalization matrix \( \mathbb{F}_\text{LE},\mathbb{C} = \begin{bmatrix} \mathbf{f}_1 & \mathbf{f}_2 \end{bmatrix} = \mathbb{C}^+ \)
  \( \mathbb{r} = \mathbb{F}_\text{LE},\mathbb{C} \mathbb{y} = \mathbb{F}_\text{LE},\mathbb{C} (\mathbb{CZx} + \mathbb{n}) = \mathbb{Zx} + \mathbb{F}_\text{LE},\mathbb{C} \mathbb{n} \)
- the noise power in branch \( k \) is given by (\( \mathbb{m} \): i.i.d. components with variance \( \sigma_m^2 \))
  \[ \sigma_{n_k}^2 = \sigma_m^2 \cdot \| \mathbf{f}_k \|_2^2 = \sigma_m^2 \cdot E_k \]
  with noise enhancement \( E_k = \| f_k \|_2^2 \)
**Factorization Task (II)**

Problem: given \( H \), find \( C \) and \( Z \) such that

- factorization of \( H \)
  \[ H = CZ \]
- \( Z \) is an integer matrix
  \[ Z \in \mathbb{Z}^{K \times K}, \quad \text{rank}(Z) = K \]
- if applicable: \( |\det(Z)| = 1 \) (unimodular)
- \( C \), the "reduced channel", or
  \( F_{LE} \), the "equalization matrix", have desired properties

Required: to solve this factorization problem, we need
- a meaningful criterion
- a practical algorithm

---

**Factorization Criteria**

Criterion I:

- lattice reduction may directly applied to the channel matrix \( H \)
  \[ H = C_I Z_I \]

- typically, the orthogonality defect of \( C_I = [c_1 \ldots c_K] \) is minimized
  \[ \delta(C_I) = \prod_{k=1}^{K} \|c_k\| \]

- this means that the basis vectors \( c_k \), the column vectors of \( C_I \)
  should be as short as possible (have small Euclidean norm)
- shortest basis/independent vector problem

- a substitute criterion is optimized, instead of system performance

---

**Factorization Criteria (II)**

Criterion II:

- for square channel matrices, the ZF equalization matrix reads
  \[ F_{LE} = C^{-1} = (HZ^{-1})^{-1} = ZH^{-1} \]
- the squared row norms of \( F_{LE} \) give the noise enhancement
- factorization task
  \[ (X^{-H})^{-1} = (X^{-1})^H \]
  \[ H^{-H} = F_{II}^H Z_{II}^{-H} \]

- the column vectors of \( F_{II}^H \) should be as short as possible
- if \( Z_{II}^{-1} \) is an unimodular integer matrix, \( Z_{II}^{-H} \) has also this property
- for non-square channel matrices the left pseudoinverse is used
  \[ (H^{-H})^H = F_{II}^H Z_{II}^{-H} \]

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

---

**Factorization Criteria (III)**

Criterion III:

- the MMSE solution can be calculated as ZF solution for the augmented channel matrix
  \[ H = C_{III} Z_{III} \]

- factorization task (\( \zeta = \sigma_n^2/\sigma_x^2 \))
  \[ \begin{bmatrix} H & \sqrt{\zeta} I \end{bmatrix} \hat{C}_{III} = Z_{III} \]

- optimum MMSE equalization matrix
  \[ F_{LE,MMSE,C} = \left( \begin{bmatrix} C_{III}^H \end{bmatrix}^{-1} C_{III} \right)^{-1} C_{III}^H \]
  \[ = \left( C_{III}^H C_{III} + \zeta Z_{III}^H Z_{III} \right)^{-1} C_{III}^H \]
  \[ = Z_{III} (H^H H + \zeta I)^{-1} H^H = Z_{III} F_{LE,MMSE,H} \]

- the column vectors of \( C_{III} \) should be as short as possible
- as in Criterion I, a substitute measure is optimized
- in almost all cases \( Z_I = Z_{III} \)

---
**Factorization Criteria (IV)**

Criterion IV: [FWSSSU12], [ZNEG14], [FCS16]

- applying MMSE linear equalization, the noise enhancement is given by
  \[ E_k = \left( \Phi_{kk} \right)_{kk} / \sigma_n^2 = \left( C^H C + \zeta Z^H Z^{-1} \right)_{kk} \]
  \[ = \left[ Z (H^H H + \zeta I)^{-1} Z^H \right]_{kk} = z_k^H (H^H H + \zeta I)^{-1} z_k \]
  with \( Z^H = [z_1, \ldots, z_K] \)

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

- factorization task (using \( L^H Z = (H^+)^H Z \), \( H^+ \) is the dual lattice)
  \[ (H^+)^H = F^H Z^{-1} \]

- the column vectors of \( F^H \) should be as short as possible

---

**Factorization Criteria (V)**

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

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

<table>
<thead>
<tr>
<th>Based on channel matrix ( H ) (&quot;ZF solution&quot;)</th>
<th>Augmented matrix ( \mathcal{H} ) (&quot;MMSE solution&quot;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H )</td>
<td>( H = CZ )</td>
</tr>
<tr>
<td>( (H^+)^H )</td>
<td>( (H^+)^H = F^H Z^{-1} )</td>
</tr>
</tbody>
</table>

Involved lattices:
- \( H \): lattice spanned by channel matrix
- \( (H^+)^H \): dual lattice

---

**Constraint on \( Z \)**

Constraint on the Integer Matrix \( Z \in \mathbb{Z}^{K \times K} \):

- typically, in LRA equalization it has been forced
  \[ \det(Z) = 1 \] unimodular matrix

  hence a change of basis is performed
  \( \Rightarrow \) Lattice Basis Reduction

- in IF equalization, the constraint is relaxed to
  \[ \text{rank}(Z) = K \] full-rank matrix

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

  \( \Rightarrow \) Shortest Independent Vector Problem

Observation: [FCS16]

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

\( \Rightarrow \) both, LRA and IF, can use the same factorization criterion and the same constraint on \( Z \)!

---

**Visualization** (real-valued example \( K = 2, |A| = 5 \))

- vectors \( \bar{x} = Zx \), with \( x \in A^K \)

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

---
**Lattices and Lattice Problems**

**Lattice:**
- We deal with complex-valued lattices

\[ \Lambda(G) = \{ \lambda = \sum_{k=1}^{K} z_k g_k | z_k \in \mathbb{C} \} \]

where

\[ G = [g_1, \ldots, g_K] \in \mathbb{C}^{N \times K} \]

is its generator matrix (basis) consisting of \( K \in \mathbb{N} \) linearly independent basis vectors \( g_k \in \mathbb{C}^N, N \geq K, N \in \mathbb{N} \)

\( (N \)-dimensional lattice of rank \( K \))

**Alternative Description:**
- Instead of dealing with the complex-valued generator matrix \( G \), one can use the real-valued equivalent \([\text{Win'04}]\)

\[ G_{\text{real}} = \begin{bmatrix} \text{Re}(G) & -\text{Im}(G) \\ \text{Im}(G) & \text{Re}(G) \end{bmatrix} \]

of doubled dimension

**Minkowski's Successive Minima:**
- \( k^{th}, k = 1, \ldots, K \), successive minimum of \( \Lambda(G) \) \([\text{Cas'97}, \text{LLS'90}, \text{DKWZ'15}]\)

\[ \rho_k(\Lambda(G)) = \inf \{ r_k | \dim (\text{span} (\Lambda(G) \cap B_N(r_k))) = k \} \]

with
- \( B_N(r) \): \( N \)-dimensional ball (over \( \mathbb{C} \)) with radius \( r \) centered at the origin
- \( \text{span}(\cdot) \): linear span

\( \rho_k(\Lambda(G)) \) is the norm of the shortest vector of the lattice \( \Lambda(G) \)

**Visualization:**
- For any matrix \( G \in \mathbb{C}^{N \times K} \) can be decomposed into the form

\[ G = G^* R \]

with
- \( G^* = [g_1^*, \ldots, g_K^*] \): Gram-Schmidt orthogonalization of \( G \) with orthogonal columns \( g_1^*, \ldots, g_K^* \)
- \( R = [r_{l,k}] \in \mathbb{C}^{K \times K} \): upper triangular with unit main diagonal

**Gram-Schmidt (GS) Orthogonalization:**
- Successive procedure

\[ g_k^* = g_k - \sum_{l=1}^{k-1} r_{l,k} g_l^* \]

\[ r_{l,k} = \frac{(g_l^*)^H g_k^*}{\|g_l^*\|^2}, \quad l = 1, \ldots, k \]

**Visualization:**
Lattices and Lattice Problems (IV)

Given: a complex-valued lattice \( \Lambda(G) \) of rank \( K \)

Shortest Independent Vector Problem (SIVP):
- find set \( \mathcal{G} = \{ \lambda_1, \ldots, \lambda_K \} \) of \( K \) linearly independent vectors \( \lambda_k \in \Lambda(G) \), such that
  \[
  \max_{k=1,\ldots,K} \| \lambda_k \| = \rho_K(\Lambda(G))
  \]
- 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 \( \mathcal{G} = \{ \lambda_1, \ldots, \lambda_K \} \) of \( K \) linearly independent vectors \( \lambda_k \in \Lambda(G) \), such that
  \[
  \| \lambda_k \| = \rho_k(\Lambda(G)), \quad k = 1, \ldots, K
  \]
- 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 \([\text{DKWZ}'15],[\text{FCS}'16]\)

Lattices and Lattice Problems (V)

Set of Linearly Independent Vectors:
- the obtained vectors are lattice points \( \lambda_k \in \Lambda(G) \), hence
  \[
  \lambda_k = Gu_k, \quad \text{with} \quad u_k \in \mathbb{C}^K, \quad \forall k
  \]
- the matrix \( V \equiv [\lambda_1, \ldots, \lambda_K] \) is related to \( G \) via
  \[
  V = GU
  \]
  or
  \[
  G = VU^{-1}
  \]
  with \( U \in \mathbb{C}^{K \times K} \) and \( |\det(U)| \in \overline{G} \setminus \{0\} \)

Lattices and Lattice Problems (VI)

Lattice Basis Reduction:
- find set \( \mathcal{G} = \{ \lambda_1, \ldots, \lambda_K \} \) of \( K \) linearly independent vectors \( \lambda_k \in \Lambda(G) \), such that
  \[
  \Lambda(G) = \Lambda(G_i)
  \]
  with
  \[
  G_i = [g_{i,1}, \ldots, g_{i,K}] = [\lambda_1, \ldots, \lambda_K]
  \]
- the generator matrices are related by
  \[
  G_i = GU
  \]
  or
  \[
  G = G_iU^{-1}
  \]
  where \( U \in \mathbb{C}^{K \times K} \) is unimodular, i.e., \( |\det(U)| = 1 \); hence \( U^{-1} \in \mathbb{C}^{K \times K} \)

Lattices and Lattice Problems (VII)

Lenstra-Lenstra-Lovász (LLL) Reduction:
- a generator matrix \( G = [g_1, \ldots, g_K] \in \mathbb{C}^{N \times K} \) with Gram–Schmidt orthogonal basis \( G' = [g'_1, \ldots, g'_K] \) and upper triangular matrix \( R \) is called (C)LLL-reduced, if
  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 \( k = 2, \ldots, K \) and a parameter \( 0.5 < \delta \leq 1 \)
    \[
    \| g_k \|^2 \geq (\delta - |r_{k-1,k}|^2)\| g_{k-1} \|^2
    \]
- the parameter \( \delta \) 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 \([\text{A03}]\)
- for \( \delta < 1 \) the algorithm has polynomial complexity \([\text{A03}]\)
Lattices and Lattice Problems (VIII)

Hermite-Korkine-Zolotareff (HKZ) Reduction:
- a generator matrix \( G = [g_1, \ldots, g_K] \in \mathbb{C}^{N \times K} \) with Gram-Schmidt orthogonal basis \( G^\perp = [g_1^\perp, \ldots, g_K^\perp] \) and upper triangular matrix \( R \) is called (C)HKZ-reduced, if

1. for \( 1 \leq l < k \leq K \), it is size-reduced according to
   \[ \text{Re}\{r_{lk}\} \leq 0.5 \quad \text{and} \quad \text{Im}\{r_{lk}\} \leq 0.5 \]
2. for \( k = 1, \ldots, K \), the columns of \( G^\perp \) fulfill
   \[ \|g_k^\perp\| = \rho_1(\Lambda(G^{(k)})) \]
   (shortest (non-zero) vector in \( \Lambda(G^{(k)}) \))

- \( \Lambda(G^{(k)}) \): sublattice of rank \( K - k + 1 \) and dimension \( N \) with generator matrix \( G^{(k)} = [0, \ldots, 0, g_k^\perp, \ldots, g_K^\perp] R \)
- \( \Lambda(G^{(k)}) \) is the orth. projection of \( \Lambda(G) \) onto the orth. complement of \( \{g_1, \ldots, g_{k-1}\} \)

since shortest vectors have to be found, the problem is NP-hard;
- efficient (complex-valued) algorithms available

Application to Equalization

Recall: Criterion IV
- MMSE linear equalization via \( F^H = ZH^+ = \begin{bmatrix} h_1 \\ \vdots \\ h_N \end{bmatrix} \)
- noise enhancement
  \[ E_k = \| \tilde{f}_k \|^2 = \| (H^+)^k z_k \|^2 \rightarrow \min \]
  with \( Z^H = [z_1, \ldots, z_K] \)
- factorization task
  \[ (H^+)^k = F^H Z^{-1} \]
- the column vectors of \( F^H \) should be as short as possible

Lattices and Lattice Problems (IX)

Minkowski (MK) Reduction:
- a generator matrix \( G = [g_1, \ldots, g_K] \in \mathbb{C}^{N \times K} \) is called (CMK-reduced, if

\[ \|g_k\| \leq \|g_k^\prime\|, \quad k = 1, \ldots, K \]
\[ \forall G^\prime = [g_1^\prime, \ldots, g_{K-1}^\prime, g_K^\prime, \ldots, g_K^\prime] \]

with
\[ \Lambda(G^\prime) = \Lambda(G) \]

\( G \) is Minkowski-reduced if for \( k = 1, \ldots, K \) the basis vector \( g_i \) has minimum norm among all possible lattice points \( g_i^\prime \) for which the set \( \{g_1, g_2, \ldots, g_{i-1}, g_i^\prime, g_i^\prime, \ldots, g_K^\prime\} \) can be extended to a basis of \( \Lambda(G) \)

- 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

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: \( Z^H = [z_1, \ldots, z_K] \)
- \( |\det(Z^H)| = 1 \) required

\[ Z^H = \arg\min_{g_k \in \mathbb{C}^{K \times K}} \max_{k=1,\ldots,K} \| (H^+)^k z_k \|^2 \] \( \Rightarrow \) 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 norm is minimized)

\( \Rightarrow \) Minkowski reduction gives the optimum integer matrix \( Z \)

- full-rank matrix \( Z \) sufficient

\[ Z^H = \arg\min_{g_k \in \mathbb{C}^{K \times K}} \max_{k=1,\ldots,K} \| (H^+)^k z_k \|^2 \] \( \Rightarrow \) shortest independent vector problem (SIVP)

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

\( \Rightarrow \) Minkowski’s successive minima give the optimum integer matrix \( Z \)
**Numerical Results**

Obtained Vectors $z_k$:  
- factorization of $G$
  
\[
G = \begin{bmatrix}
 0.8 + 0j & -0.5 + 0j & -0.1 - 0j & 0.7 - 1j \\
 0.3 - 0j & 0.1 + 0j & 0.2 - 0j & 0.2 + 1j \\
 0.1 - 0j & -0.2 + 0j & 0.1 + 0j & 0.3 - 1j \\
 0.8 - 0j & 0.1 - 0j & 0.2 + 0j & 0.2 - 1j \\
\end{bmatrix}
\]

$u_k$:  
- LatticeReductionandFactorizationforEqualization
  
\[
\begin{array}{c|cccccccc}
\lambda_k & |\lambda_k|^2 & 1.43 & 1.48 & 1.51 & 1.54 & 1.55 & 1.59 & 1.64 & 1.69 & 1.72 & 1.73 & 1.74 & 1.77 \\
\hline
\text{rank} & 1 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 4 \\
LLL = 25 & X & X & X & X & X & X & X & X & X & X & X & X & X \\
LLL = 1 & X & X & X & X & X & X & X & X & X & X & X & X & X \\
HKZ & X & X & X & X & X & X & X & X & X & X & X & X & X \\
MK & X & X & X & X & X & X & X & X & X & X & X & X & X \\
SMP & X & X & X & X & X & X & X & X & X & X & X & X & X \\
\end{array}
\]

- det($Z_{SMP}$) = 1 + j

**Numerical Results (II)**

Distribution of $|\det(Z)|$:  
- $H$: i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- $\sigma_i^2/\sigma_n^2 \in [20\text{ dB}]$
- criterion IV — SMP

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

**Numerical Results (III)**

Distribution of $|\det(Z)|$:  
- $H$: i.i.d. random zero-mean unit-variance complex Gaussian
- $K = N = 6$
- criterion IV — SMP

**Numerical Results (IV)**

Bit Error Rate:  
- LRA structure; linear MMSE equalization — different criteria and constraints
- $H$: i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- uncoded transmission; 16QAM signaling:  

\[
E_b/N_0 = \sigma_i^2/(\sigma_n^2 \log_2(16))
\]

\[
\begin{array}{c}
\text{BER} \\
\hline
\text{C-I + SBP} & \text{C-II + SBP} & \text{C-IV + SBP} & \text{C-I + V} & \text{C-II + V} & \text{C-IV + V} \\
\end{array}
\]

$K = 8$
Numerical Results (V)

Bit Error Rate: LRA structure; linear MMSE equalization; criterion C-IV — different algorithms
- $H$: i.i.d. random zero-mean unit-variance complex Gaussian; $K = N$
- uncoded transmission; 16QAM signaling; $E_b/N_0 = \sigma_x^2 / (\sigma_n^2 \text{log}_2(16))$

<table>
<thead>
<tr>
<th>SMP</th>
<th>$K = N =$</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_x^2 / \sigma_n^2 \leq 15$ dB</td>
<td>100 %</td>
<td>99.0 %</td>
<td>95.7 %</td>
<td>90.3 %</td>
<td>83.8 %</td>
<td></td>
</tr>
<tr>
<td>$\sigma_x^2 / \sigma_n^2 \leq 20$ dB</td>
<td>100 %</td>
<td>99.0 %</td>
<td>95.6 %</td>
<td>89.8 %</td>
<td>82.3 %</td>
<td></td>
</tr>
<tr>
<td>$\sigma_x^2 / \sigma_n^2 \rightarrow \infty$</td>
<td>100 %</td>
<td>99.0 %</td>
<td>95.5 %</td>
<td>89.4 %</td>
<td>81.5 %</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIVP</th>
<th>$K = N =$</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_x^2 / \sigma_n^2 \leq 15$ dB</td>
<td>100 %</td>
<td>99.2 %</td>
<td>97.0 %</td>
<td>94.0 %</td>
<td>90.6 %</td>
<td></td>
</tr>
<tr>
<td>$\sigma_x^2 / \sigma_n^2 \leq 20$ dB</td>
<td>100 %</td>
<td>99.2 %</td>
<td>97.0 %</td>
<td>93.5 %</td>
<td>89.3 %</td>
<td></td>
</tr>
<tr>
<td>$\sigma_x^2 / \sigma_n^2 \rightarrow \infty$</td>
<td>100 %</td>
<td>99.2 %</td>
<td>96.9 %</td>
<td>93.2 %</td>
<td>88.5 %</td>
<td></td>
</tr>
</tbody>
</table>

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

Numerical Results (VII)

Percentages “MK = SMP” and “MK = SIVP”:
- $H$: i.i.d. random zero-mean unit-variance complex Gaussian
- $K = N$; criterion IV

Numerical Results (VIII)

Distribution of Deviation from Optimum:
- $H$: i.i.d. random zero-mean unit-variance complex Gaussian
- $K = N = 8$; $\sigma_x^2 / \sigma_n^2 \geq 20$ dB
- criterion IV
Lattice Reduction and Factorization for 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 $F_{\text{DFE},H} \equiv (Q^H Q)^{-1} Q^H$ $r = F_{\text{DFE},H} y = B x + \tilde{n}$
  - spatially causal signal transmission matrix $B$
  - Gaussian noise vector $\tilde{n}$ with correlation matrix $\sigma^2_{\tilde{n}} Q^H Q$^{-1}
  - i.e., with $Q = \begin{bmatrix} q_1 & \cdots & q_K \end{bmatrix}$ noise variances $\sigma^2 = \sigma^2_{\tilde{n}} |q_k|^2$
  - decisions are taken successively (order $K, \ldots, 1$)

**Optimum Detection Order:** V-BLAST ordering

- for $k = K, \ldots, 1$: the norm of the vector $q_k$ should be the largest among the remaining components $1, \ldots, k$
- BLAST ordering requires great effort

**Simpler Strategy:**

- instead of maximizing $\|q_k\|^2$ in sequence $k = K, K-1, \ldots, 1$
  - it is minimized in sequence $k = 1, 2, \ldots, K$
- for $k = 1, \ldots, K$: the norm of the vector $q_k$ should be the smallest among the remaining components $k, \ldots, K$

**Gram–Schmidt procedure with pivoting**

**Simple but Optimum Strategy:**

- do not apply Gram–Schmidt procedure with pivoting to $H$, but to $(H^H)^H$
- use factorization $(H^H)^H P^{-H} = F^H B^{-H}$
- order within GS proc.: $k = K, \ldots, 1$; i.e., $B^{-H}$ should be lower triangular

**MMSE version of DFE:**

- ZF version for $K = N$:
  - $HP = F^{-1} B$
- MMSE version of DFE:
  - with $H = \begin{bmatrix} q_1 \\ \vdots \\ q_K \end{bmatrix}$

**LRA Decision-Feedback Equalization:**

**Strategies:**

- obvious
  - perform i) factorization $H = CZ$;
    - ii) sorted QR decomposition $CP = QB$
- more efficient
  - reuse $Q$ and $R$ anyway calculated within LLL or HKZ
- optimum
  - do sorting, Gram–Schmidt procedure, and size reduction jointly
LRA Decision-Feedback Equalization (II)

Pseudocode of Factorization Approach: [SF17]

\[
\begin{align*}
&[Q, R, T] = \text{GramSchmidtSort}_{\text{LRA}}(G) \\
&Q = G, R = I, T = I \\
&k = 1 \\
&\text{while } k \leq K 
\{ \\
&\quad q_k = \text{shortest vector in } \Lambda([q_k, \ldots, q_K]) \\
&\quad \text{if } \|q_k\|^2 \neq \|q_i\|^2 
\{ \\
&\quad \quad q_k = q_k \\
&\quad \quad \text{update } Q, R, T \text{ such that } \Lambda(QR) = \Lambda(G) \\
&\quad \} \\
&\quad \text{for } i = k + 1, \ldots, K 
\{ \\
&\quad r_{ik} = q_i^T q_k / \|q_k\|^2 \\
&\quad q_i = q_i - r_{ik} q_k \\
&\quad \} \\
&\quad k = k + 1 \\
&\}
\end{align*}
\]

Fischer: Lattice Reduction and Factorization for Equalization

51

LRA Decision-Feedback Equalization (III)

Recall: Hermite-Korkine-Zolotareff (HKZ) Reduction

- a generator matrix \( G = [g_1, \ldots, g_K] \in \mathbb{C}^{N \times K} \) with Gram-Schmidt orthogonal basis \( G' = [g'_1, \ldots, g'_K] \) and upper triangular matrix \( R \)

is called (C)HKZ-reduced, if

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

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

2. for \( k = 1, \ldots, K \), the columns of \( G' \) fulfill

\[
\|g'_k\| = \rho_1(\Lambda(G^{(k)}))
\]

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

- \( \Lambda(G^{(k)}); \) sublattice with generator matrix \( G^{(k)} = [0, \ldots, 0, g'_k, \ldots, g'_K]R \)

Fischer: Lattice Reduction and Factorization for Equalization

52

LRA Decision-Feedback Equalization (IV)

Discussion:

- the size-reduction step of HKZ is not present; as it changes only \( R \) it is of no relevance for performance of LRA DFE
  \( \Rightarrow \) effective HKZ reduction

- for \( G = (H^*)^H \) the algorithms returns \( Z^H = T \) and \( F^H = Q \) with
  - V-CAST sorting
  - the columns of \( F^H \) have minimum norm (optimal worst-link performance as in classical V-CAST but for LRA equalization)

- this optimum is achieved with an unimodular \( Z \); a relaxation to \( \text{rank}(Z) = K \) is not required
  \( \Rightarrow \) successive IF and LRA DFE both can be restricted to unimodular \( Z \)

\[\text{[OEN13]}\]

Fischer: Lattice Reduction and Factorization for Equalization

53

LRA Decision-Feedback Equalization (V)

LRA Decision-Feedback Equalization:

- redraw to noise-prediction structure
- apply modulo reduction w.r.t. \( \Lambda_s \)
- exchange \( Z^{-1} \) and demapping/encoder inverse
- combine to demapping modulo \( \Lambda_s \)

\( \Rightarrow \) successive IF only works in noise-prediction structure

\[\text{[Fis02]}\]

Fischer: Lattice Reduction and Factorization for Equalization

54
Numerical Results

Table: BER vs. \( 10 \log_{10}\left(\frac{E_b}{N_0}\right) \) [dB]

<table>
<thead>
<tr>
<th>BER</th>
<th>( 10 \log_{10}\left(\frac{E_b}{N_0}\right) ) [dB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>10^-1</td>
<td>0</td>
</tr>
<tr>
<td>10^-2</td>
<td>1</td>
</tr>
<tr>
<td>10^-3</td>
<td>2</td>
</tr>
<tr>
<td>10^-4</td>
<td>3</td>
</tr>
</tbody>
</table>

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

Dualization:
- transmitter-side precoding for broadcast channel
  - LRA / IF precoding

References


References


