The Principle of Universal Lattice Decoding

presented by

Wai Ho Mow

Hong Kong University of Science & Technology

Outline

- Preliminaries on lattices
- Closest Vector Problem (CVP)
- CVP in communications
- Lattice basis reduction
- Sphere decoding (SD)
- Lattice-reduced sub-optimal detectors
- Low-complexity MLD via packing radius test
- Simulation results for MIMO fading channels
- Concluding remarks

Preliminary (1)

- For $n \leq m$, let $\mathbf{b}_1$, $\mathbf{b}_2$, …, $\mathbf{b}_n$ be a set of independent vectors in $\mathbf{R}^m$
- $\mathbf{b}_i$ are called the *basis vectors*
- A *lattice* is defined as the set of points:

  $$\{ \mathbf{x} \mid \mathbf{x} = a_1\mathbf{b}_1 + \ldots + a_n\mathbf{b}_n \}$$

  where a_i are integers
- Equivalently, in matrix form:

  $$\{ \mathbf{x} \mid \mathbf{x} = \mathbf{B}\mathbf{a} \}$$

  where $\mathbf{B} = [\mathbf{b}_1 \ \ldots \ \mathbf{b}_n]$ and $\mathbf{a}$ is an integer (column) vector
- The same lattice (i.e. the same set of points) can be generated by *different* basis:

  $$L = L(\mathbf{B}_1) = L(\mathbf{B}_2) \text{ iff } \mathbf{B}_1 = \mathbf{U}\mathbf{B}_2$$

  where $\mathbf{U}$ is an *unimodular* matrix (i.e. $\det(\mathbf{U}) = \pm 1$)
- The *determinant* of lattice L is defined as the volume of the *fundamental parallelotope* of L:

  $$\det(L) = \det(L(\mathbf{B})) = |\det(\mathbf{B})|$$

Preliminary (2)

- Gram-Schmidt Orthogonalization (GSO):
  - for any basis $\mathbf{B} = [\mathbf{b}_1 \ldots \mathbf{b}_n]$ we can find a set of orthogonal vectors $\{\mathbf{b}_i^*\}$ that span the space of $L(\mathbf{B})$:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=i+1}^{n} \mu_{ij} \mathbf{b}_j^* \qquad \mu_{ij} = \frac{<\mathbf{b}_i, \mathbf{b}_j^*>}{\left\|\mathbf{b}_j^*\right\|}$$

    for $i = n, n\text{-}1, \ldots, 1$

- Note that:
  - different permutations of $[\mathbf{b}_1 \ldots \mathbf{b}_n]$ give you different set of $\{\mathbf{b}^*_1 \ldots \mathbf{b}^*_n\}$
  - $$\prod_{i=1}^{n} \left\|\mathbf{b}_i^*\right\| = \left|\det(\mathbf{B})\right| = \det(L(\mathbf{B}))$$

Closest Vector Problem (CVP)

- Definition of the CVP:
  - Given a lattice $L(\mathbf{B})$ and an arbitrary query point $\mathbf{q}$ in $\mathbf{R}^m$, to find, among all lattice points, the one that is closest to $\mathbf{q}$ w.r.t. Euclidean distance
  - More precisely, to solve:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in L(\mathbf{B})} \left\| \mathbf{x} - \mathbf{q} \right\|^2$$

CVP in Communications (1)

- Many detection problems in communications can be re-formulated as CVP.
- Detection for MIMO fading channels (Viterbo'93, Viterbo-Boutros'99, Damen et al.'2000):
  - assuming independent flat-fading channels, the received symbol vector **y** is given by:

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

    where **x** := transmitted vector; **H** := channel matrix; **w** := AWGN
  - **Sphere detector** finds:

    $$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathbf{Z}^n} \left\|\mathbf{H}\mathbf{x} - \mathbf{y}\right\|^2$$

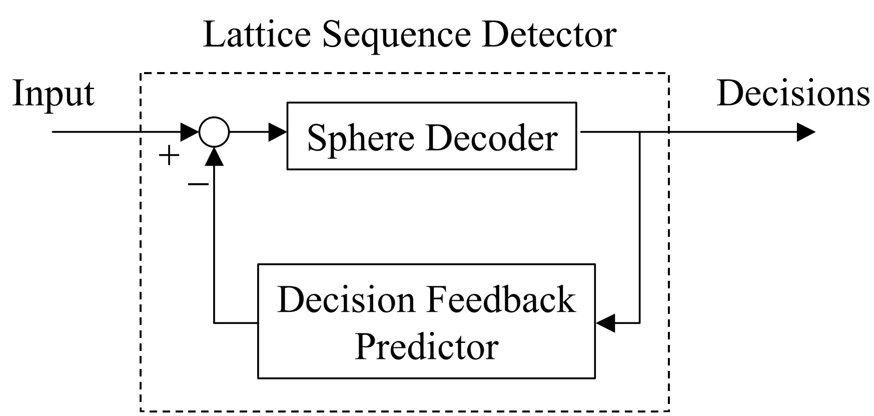
  - thus **H** is the lattice basis, **y** is the query point.
- Block-based space-time decoding (Damen'2000 & many others) can be formulated in a similar way.

CVP in Communications (2)

- Sequence detection for ISI channels (Mow'91 & '94):
  - Sequence detector for ISI channels minimizes the metric:

$$\left\| \mathbf{H}\tilde{\mathbf{u}} - (\mathbf{y} - \mathbf{G}\hat{\mathbf{u}}) \right\|^2$$

    where **y** := received seq.; **G, H** := Toeplitz channel matrices; **ũ** := integer-valued seq. to be detected; **û** := previously detected seq.
  - Let **q** = **y** - **Gû** be the query point, **H** be the lattice basis



- CDMA multiuser detection (Brunel et al.'98 &'2003) and MIMO sequence detection (Vikalo-Hassibi'2002) can be formulated similarly.

Solving CVP approximately

- Very efficient algorithms exist for some special types of lattices, e.g. cubic lattices
- But in general, solving CVP is hard
- Solving CVP *approximately* is less difficult:
  - Nulling & rounding/quantization (***zero-forcing***)
  - Babai's nearest plane algorithm (***DFE***: ***successive nulling*** & ***cancellation***)
  - Nearest plane algorithm with optimal ordering (***VBLAST***)
- These sub-optimal detectors have much lower complexity than the optimal MLD.

Solving CVP exactly

- How to solve CVP exactly for optimal performance?
- Solving CVP in 2 steps:
  1. (***lattice reduction***) for a given lattice, find a “short” and fairly “orthogonal” basis
  2. (***sphere decoding***) enumerate all lattice points inside a sphere centered at the query point
- Lattice reduction can also enhance the performance of suboptimal schemes mentioned before

Lattice Reduction

- The definition of basis reduction is not unique:
  - for 2-D lattices: *Gauss reduction*
  - *Minkowski reduction*: the shortest possible basis
  - *Lenstra, Lenstra & Lovász (LLL or L^3) reduction*
- LLL reduction is very important and useful in practical applications (such as cryptanalysis) as its complexity is only polynomial time

Lattice Reduction Algorithm (1)

- The first step of the reduction algorithm is called *size-reduction*:

$$\mathbf{b}_i \leftarrow \mathbf{b}_i - \sum_{j=i+1}^{m} \mu_{ij} \mathbf{b}_j \qquad \mu_{ij} = \left\lceil \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \right\rfloor$$

- This operation shortens the lengths of the basis vectors (hence its name)
- After size reduction, $|\mu_{i+1,i}| \leq 0.5$

Lattice Reduction Algorithm (2)

- Can we do better?
- We can re-order (how?) the basis vectors to obtain a new set of $\{\mathbf{b}_i^*\}$
- After this re-ordering, $|\mu_{i+1,i}| > 0.5$, so perform the size-reduction again
- Repeat until no further improvement is achievable

Lattice Reduction Algorithm (3)

- For LLL, swap $\mathbf{b}_i$ and $\mathbf{b}_{i+1}$ if:

$$\delta\left\|\mathbf{b}_i^*\right\|^2 > \left\|\mathbf{b}_{i+1}^*\right\|^2 + \mu_{i+1,i}^2\left\|\mathbf{b}_i^*\right\|^2 \qquad \frac{2}{3} < \delta < 1$$

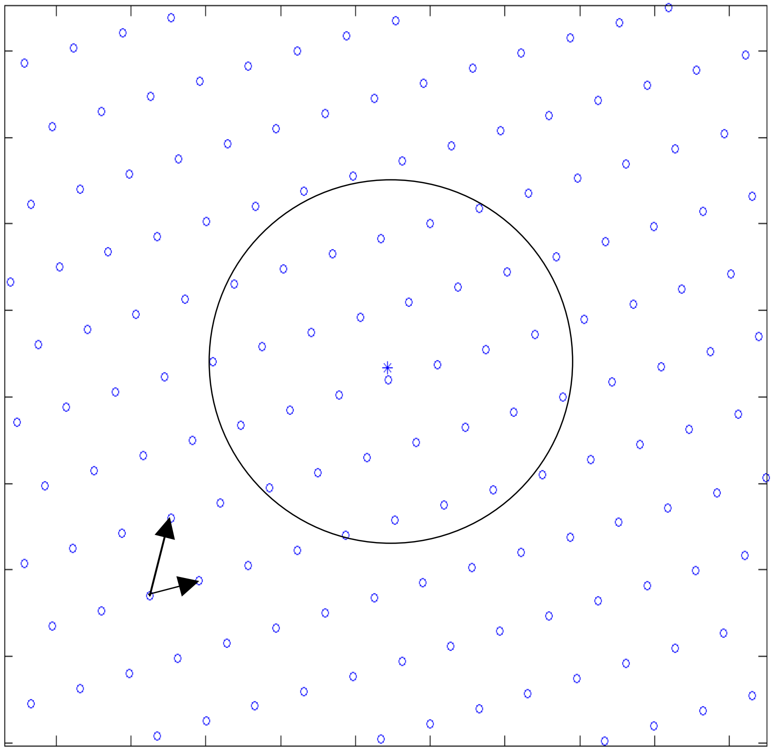
- δ is a parameter:
  - choose small δ for faster convergence
  - choose large δ for better reduced basis
  - the basis might not be reduced and the algorithmic complexity is not polynomial time, if δ is chosen outside the specified range.

Properties of LLL-reduced basis

- Denote $\lambda(L)$ as the length of the shortest vector in L, then (when $\delta = ¾$):
  1. $||\mathbf{b}_1|| \leq 2^{(n-1)/2} \lambda(L)$
  2. $||\mathbf{b}_1|| \leq 2^{(n-1)/4} \det(L)^{1/n}$
  3. $||\mathbf{b}_1||\ldots||\mathbf{b}_n|| \leq 2^{n(n-1)/4} \det(L)$
- (1) & (2) ensure that the reduced-basis contains short vectors.
- (3) ensures a “near-orthogonal” basis.
- From experience these bounds are quite loose, i.e., the algorithm does better in practice.

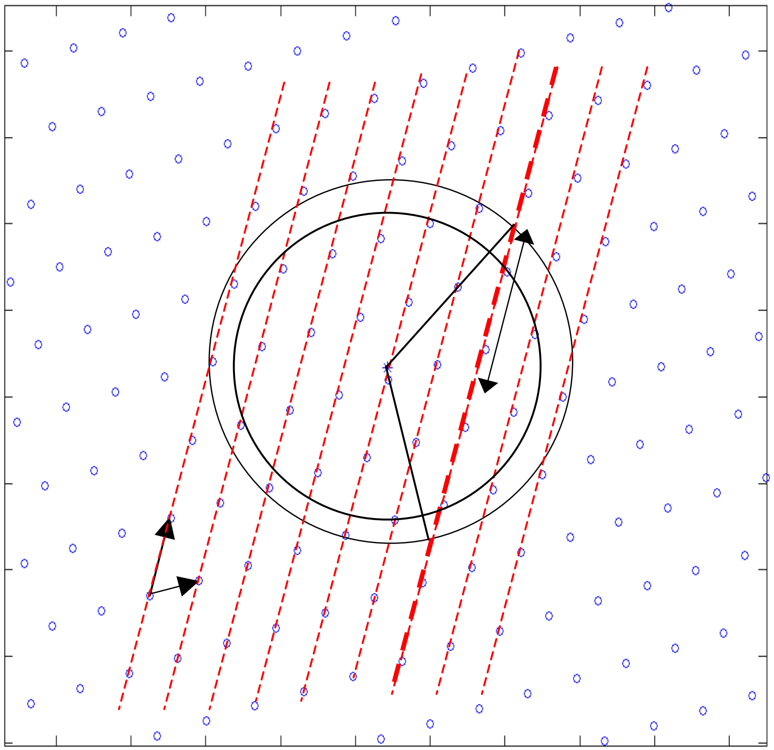
Sphere Decoding (1)

- Originally developed by Pohst in 1981
- To enumerate the lattice points inside a sphere centered at the query point
- A lattice point is identified *coordinate by coordinate.*



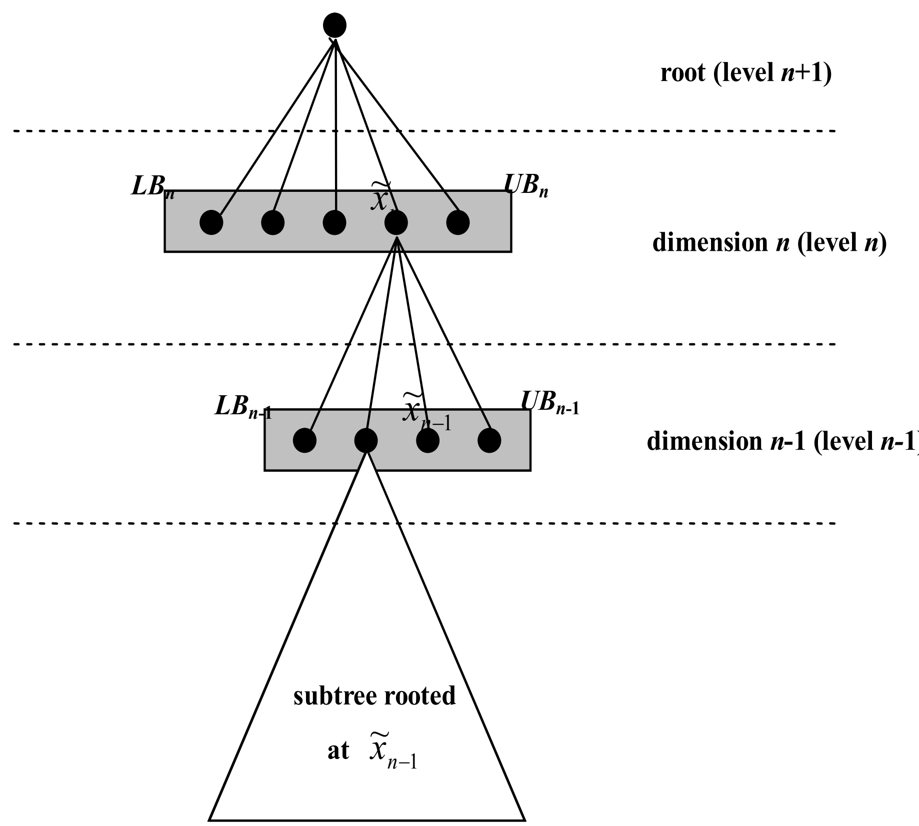
Sphere Decoding (2)

1. Identify the range of m-D “planes” (i.e. lines here) bounded by the sphere
2. Choose one of the plane within this range, then project the sphere onto this plane
3. Identify the range of (m-1)-D “planes” (i.e. points) bounded by this new lower-dimensional “sphere”, and choose one within the range
4. Perform the above recursively until eventually a lattice point is found, its distance to the query point can be calculated conveniently.
5. The radius of the sphere and the search ranges could be shrunk
6. Repeat until no more point can be found inside the sphere.



Sphere Decoding (3)

- Sphere decoding can also be viewed as a ***tree search***
- The radius defines a lower upper bounds for each dimension (level)
- Once a leaf node (i.e. lattice point) is reached, the bounds are updated
- The tree becomes smaller and smaller until no leaf can be found with the most current bounds.



Sphere Decoding Complexity

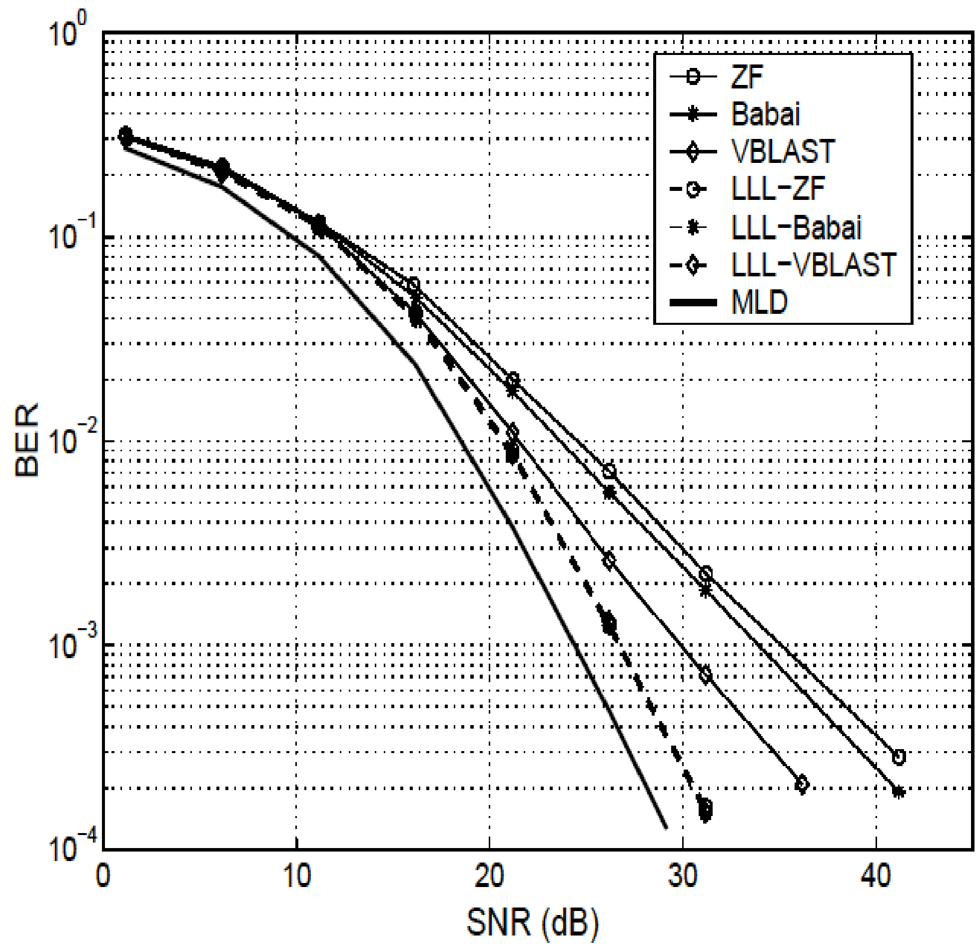
- The SD complexity is sensitive to :
  - the initial radius of the sphere
  - the enumeration order
- Reduced basis may also lower the SD complexity

Packing Radius Test

- A simplification of the sphere decoder is to make use of the *packing radius* in a *sufficiency test.*
- Already used in Mow’91 & ‘94.
- A lattice point found inside the packing sphere of the query point must be the closest one, so the enumeration can be terminated immediately
- The packing radius which is a property of the lattice, can be found in the preprocessing stage and it needs to be updated only when the channel matrix requires so.

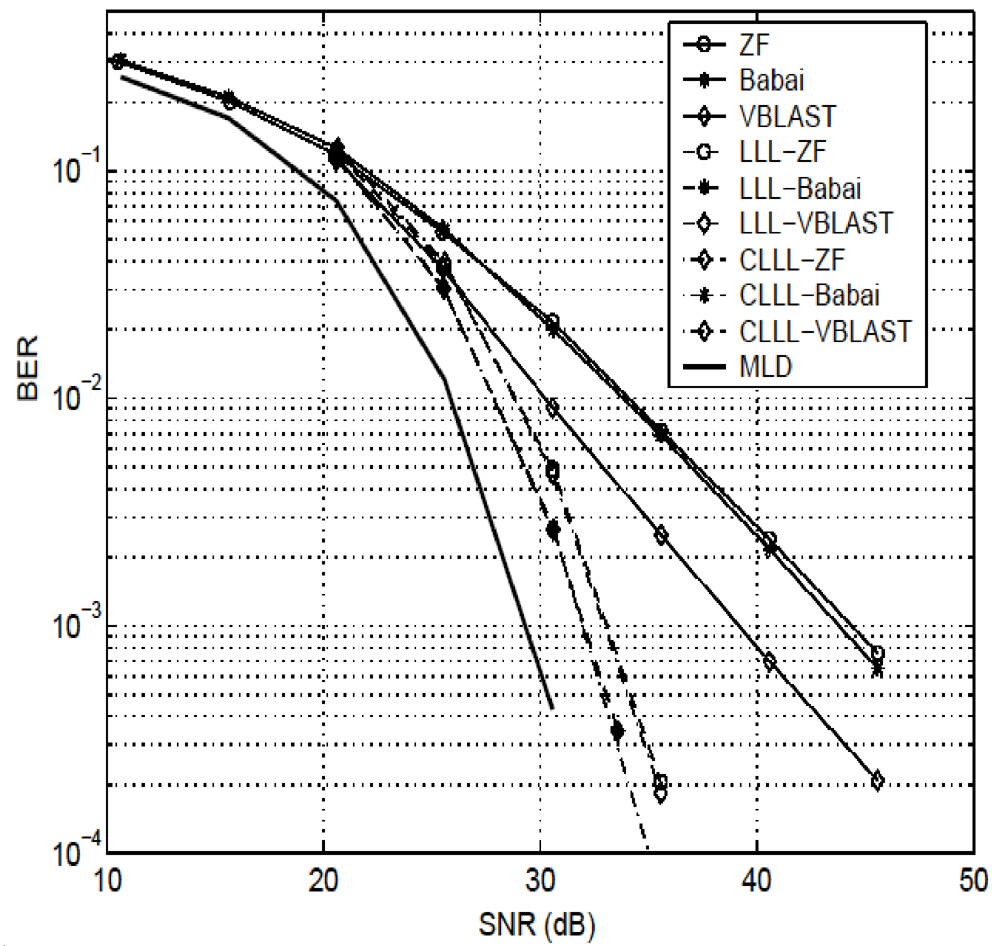
BER Performance

- Simulation of a 2-transmitter 3-receiver MIMO system using 4-PAM
- Equivalent to solving CVP of 2D lattice in 6D space
- LLL reduction enhances the performance of various suboptimal schemes
- MLD performance was achieved by sphere decoding



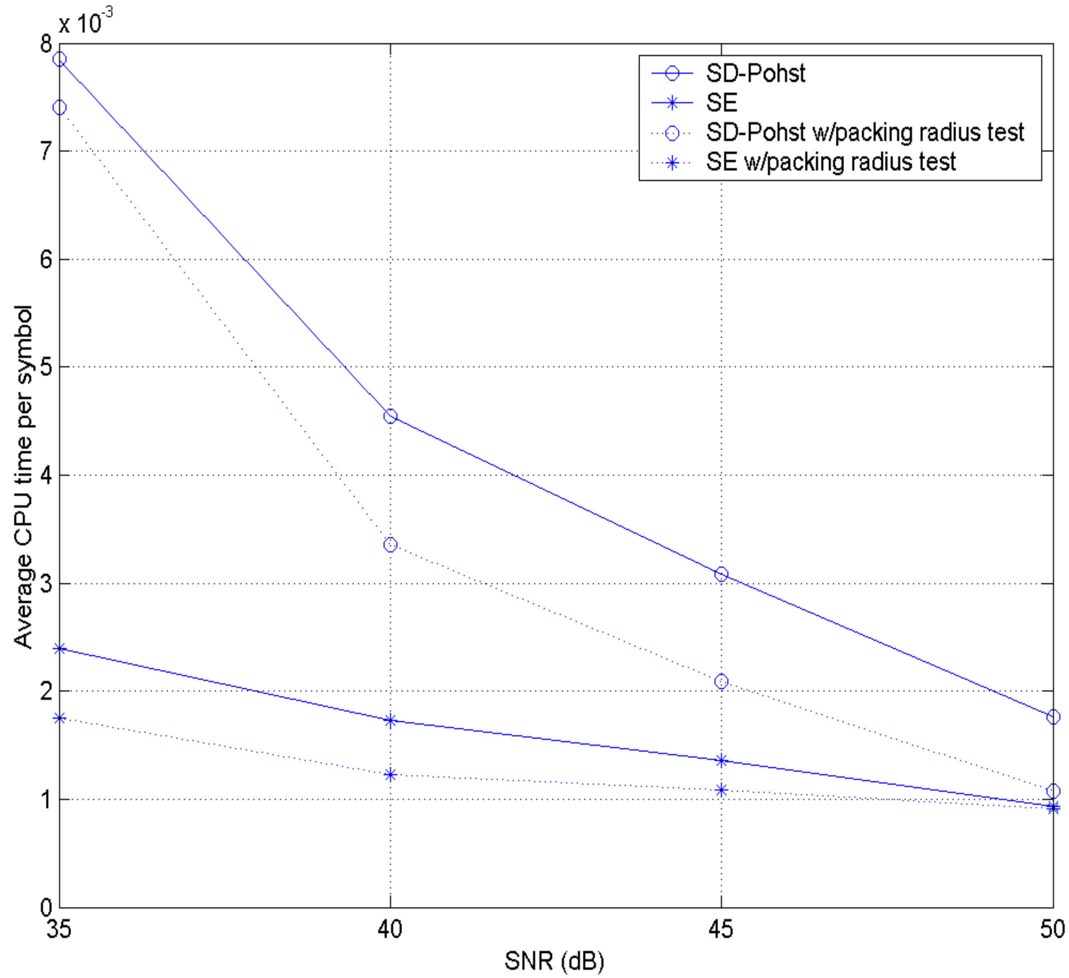
BER Performance

- Simulation of a 4-transmitter-4-receiver MIMO system using 64-QAM
- Again LLL reduction enhances the performance of various suboptimal schemes
- Complex lattice based detectors (CLLL-ZF etc.) can provide the same performance



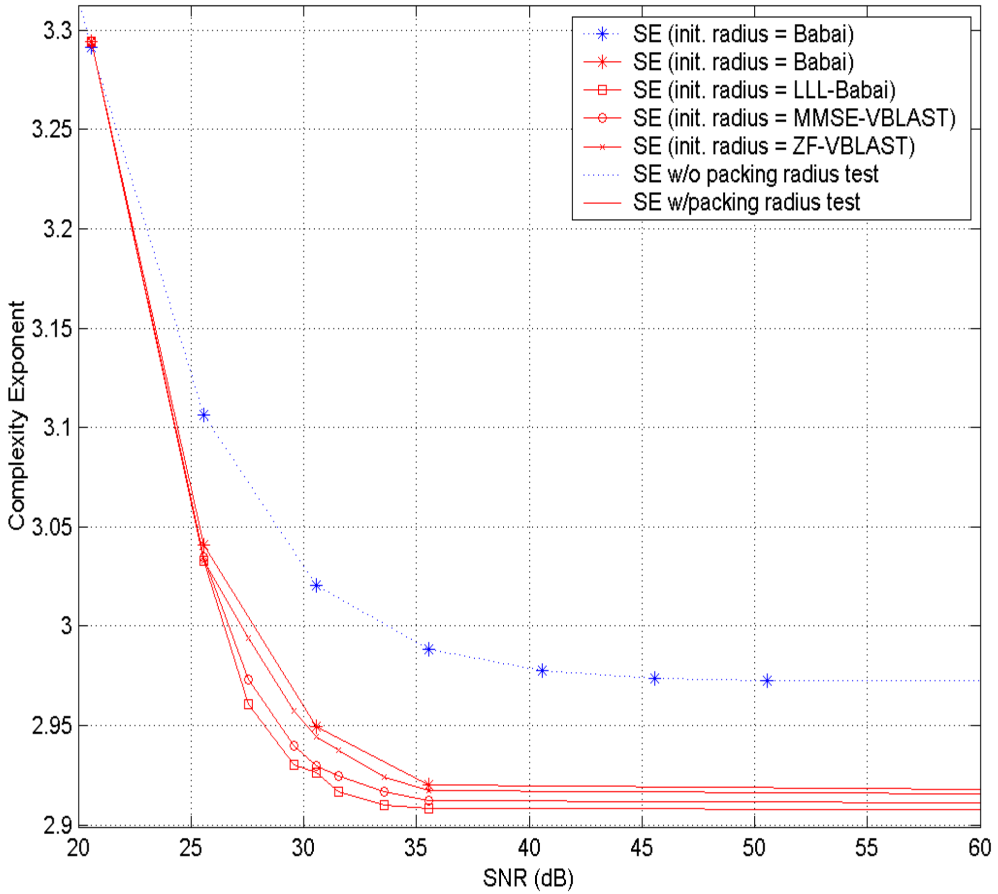
MLD Complexity Comparison

- Simulation of a 4-tx 4-rx MIMO flat fading channel with 64-QAM
- Time complexity is measured in ***average CPU time per symbol***
- SD-Pohst: sphere decoder with the original Pohst ordering
- SE: sphere decoder with Schnorr-Euchner ordering



MLD Complexity Comparison

- Simulation of a 4-transmitter-4-receiver MIMO system using 64-QAM
- Time complexity is measured by the ***complexity exponent*: $\log_m$(average #flops)**
- Dotted line: sphere decoder without packing radius test
- Solid lines: sphere decoder with packing radius test



Concluding Remarks

- Many communications detection problems can be re-formulated as a CVP, so that the SD is applicable.
- The first of such communications detection problems solved is probably the MLSD problem for ISI channels.
- Lattice basis reduction is a powerful technique for improving the performance of various known algorithms (e.g. ZF, DFE, VBLAST) at the expense of higher preprocessing complexity.
- The packing radius test is an effective technique for reducing the average complexity (or power consumption) of MLD at the expense of higher preprocessing complexity.

Concluding Remarks (2)

- The rich lattice/communications theory guarantees that many lattice related ideas are still waiting for us to explored!
- We have plenty of rooms for collaborations!!!
- To probe further:
  - W.H. Mow, "Universal Lattice Decoding: Principle and Recent Advances", ***Wireless Communications and Mobile Computing***, *Special Issue on Coding and Its Applications in Wireless CDMA Systems*, Vol.3, Issue 5, August 2003, pp. 553-569.
  - **http://www.ee.ust.hk/~eewhmow**
- Finally, you might not know the impact of your present work until 10 years later!!!

Thank You