Applications of Lattices in Telecommunications

Amin Sakzad
Dept of Electrical and Computer Systems Engineering
Monash University
amin.sakzad@monash.edu

Oct. 2013
1 Sphere Decoder Algorithm
   - Rotated Signal Constellations
   - Sphere Decoding Algorithm

2 Lattice Reduction Algorithms
   - Definitions

3 Integer-Forcing Linear Receiver
   - Multiple-input Multiple-output Channel
   - Problem statement
   - Integer-Forcing

4 Lattice-based Cryptography
   - GGH public-key cryptosystem
We consider $n$-dimensional signal constellation $A$ carved from the lattice $\Lambda$ with generator matrix $G$, for example 4-QAM.
We consider $n$-dimensional signal constellation $\mathcal{A}$ carved from the lattice $\Lambda$ with generator matrix $G$, for example 4-QAM.

Hence, $x = uG$ represent a transmitted signal.
We consider $n$-dimensional signal constellation $\mathcal{A}$ carved from the lattice $\Lambda$ with generator matrix $G$, for example 4-QAM.

Hence, $x = uG$ represent a transmitted signal.

The received vector $y = \alpha \cdot x + z$, where $\alpha_i$, are independent real Rayleigh random variables with unit second moment and $z_i$ are real Gaussian distributed with zero mean and variance $\sigma/2$. 


Channel Model

- We consider $n$-dimensional signal constellation $A$ carved from the lattice $\Lambda$ with generator matrix $G$, for example 4-QAM.
- Hence, $x = uG$ represent a transmitted signal.
- The received vector $y = \alpha \cdot x + z$, where $\alpha_i$, are independent real Rayleigh random variables with unit second moment and $z_i$ are real Gaussian distributed with zero mean and variance $\sigma/2$.
- With perfect Channel State Information (CSI) at the receiver, the ML decoder requires to solve the following optimization problem

$$\min \sum_{i=1}^{n} |y_i - \alpha_i x_i|^2.$$
Using standard Chernoff bound technique one can estimate pairwise error probability under ML decoder as

$$\Pr(\mathbf{x} \rightarrow \mathbf{x}') \leq \frac{1}{2} \prod_{x_i \neq x'_i} \frac{4\sigma}{(x_i - x'_i)^2} = \frac{(4\sigma)^{\ell}}{2d_{\min,p}^{(\ell)}(\mathbf{x}, \mathbf{x}')^2},$$

where the \(\ell\)-product distance is

$$d_{\min,p}^{(\ell)}(\mathbf{x}, \mathbf{x'}) \triangleq \prod_{x_i \neq x'_i} |x_i - x'_i|.$$
We define the product distance as $d_{\text{min}}, p = \min d(L)_{\text{min}}, p$. To minimize the error probability, one should increase both $L$ and $d_{\text{min}}, p$. The parameter $L = \min(\ell)$ is called modulation diversity.
Rotated Signal Constellations

**Goal**

**Definition**

The parameter $L = \min(\ell)$ is called *modulation diversity*.

**Definition**

We define the *product distance* as $d_{\text{min},p} = \min d_{\text{min},p}^{(L)}$. 
Definition

The parameter \( L = \min(\ell) \) is called modulation diversity.

Definition

We define the product distance as \( d_{\min,p} = \min d_{\min,p}^{(L)} \).

To minimize the error probability, one should increase both \( L \) and \( d_{\min,p} \).
Rotated $\mathbb{Z}^n$-lattice constellations

(a) 4-QAM

(b) 4-RQAM

$\alpha = (1, 0.5)$
“Algebraic Number Theory” has been used as a strong tool to construct good lattices for signal constellations.
“Algebraic Number Theory” has been used as a strong tool to construct good lattices for signal constellations.

For these lattices, the minimum product distance will be related to the volume of the lattice and the “discriminant” of the underlying number field.
Rotated $\mathbb{Z}^n$-lattice constellations

- “Algebraic Number Theory” has been used as a strong tool to construct good lattices for signal constellations.
- For these lattices, the minimum product distance will be related to the volume of the lattice and the “discriminant” of the underlying number field.
- The “signature” of a number field determines the modulation diversity.
“Algebraic Number Theory” has been used as a strong tool to construct good lattices for signal constellations.

For these lattices, the minimum product distance will be related to the volume of the lattice and the “discriminant” of the underlying number field.

The “signature” of a number field determines the modulation diversity.

List of good algebraic rotations are available online. See Emanuele’s webpage.
The problem is to solve the following:

$$\min_{x \in \Lambda} ||y - x||^2 = \min_{w \in y - \Lambda} ||w||^2.$$
Algorithm [Viterbo’99]

- Set $x = uG$, $y = \rho G$, and $w = \zeta G$ for $u \in \mathbb{Z}^n$ and $\rho, \zeta \in \mathbb{R}^n$. 
Sphere Decoding Algorithm

Algorithm [Viterbo’99]

- Set \( x = uG, \ y = \rho G, \) and \( w = \zeta G \) for \( u \in \mathbb{Z}^n \) and \( \rho, \zeta \in \mathbb{R}^n. \)

- Let the Gram matrix \( M = GG^T \) has the following Cholesky decomposition \( M = RR^T, \) where \( R \) is an upper triangular matrix.
Algorithm [Viterbo’99]

- Set $x = uG$, $y = \rho G$, and $w = \zeta G$ for $u \in \mathbb{Z}^n$ and $\rho, \zeta \in \mathbb{R}^n$.

- Let the Gram matrix $M = GG^T$ has the following Cholesky decomposition $M = RR^T$, where $R$ is an upper triangular matrix.

- We have

$$\|w\|^2 = \zeta RR^T \zeta^T = \sum_{i=1}^{n} q_{ii} U_i^2 \leq C,$$

where $U_i, q_{ii}$ are based on $r_{ij}$ and $\zeta_i$, for $1 \leq i, j \leq n$. 
Algorithm [Viterbo’99]

- Set \( x = uG \), \( y = \rho G \), and \( w = \zeta G \) for \( u \in \mathbb{Z}^n \) and \( \rho, \zeta \in \mathbb{R}^n \).
- Let the Gram matrix \( M = GG^T \) has the following Cholesky decomposition \( M = RR^T \), where \( R \) is an upper triangular matrix.
- We have

\[
\|w\|^2 = \zeta R R^T \zeta^T = \sum_{i=1}^{n} q_{ii} U_i^2 \leq C,
\]

where \( U_i, q_{ii} \) are based on \( r_{ij} \) and \( \zeta_i \), for \( 1 \leq i, j \leq n \).

- Starting from \( U_n \) and working backward, one can find bounds on \( U_i \), these will be transformed to bounds on \( u_i \).
The sphere decoding algorithm can be adapted to work on fading channels as well.
The sphere decoding algorithm can be adapted to work on fading channels as well.

Choosing the radius $C$ is a crucial part of the algorithm. Covering radius is an excellent choice.
The sphere decoding algorithm can be adapted to work on fading channels as well.

Choosing the radius $C$ is a crucial part of the algorithm. Covering radius is an excellent choice.

The complexity is reasonable for low dimensions, $n = 64$. 
Lattice Reduction Algorithms; Key to Application
## Definitions

Given a basis set, a lattice reduction technique is a process to obtain a new basis set of the lattice with shorter vectors.
Given a basis set, a lattice reduction technique is a process to obtain a new basis set of the lattice with shorter vectors.

Figure: Geometrical view of Lattice Reduction.
Gram-Schmidt Orthogonalization

The orthogonal vectors generated by the Gram-Schmidt orthogonalization procedure are denoted by \( \{\text{GS}(g_1), \ldots, \text{GS}(g_n)\} \) which spans the same space of \( \{g_1, \ldots, g_n\} \).
Gram-Schmidt Orthogonalization

The orthogonal vectors generated by the Gram-Schmidt orthogonalization procedure are denoted by \( \{ \text{GS}(g_1), \ldots, \text{GS}(g_n) \} \) which spans the same space of \( \{g_1, \ldots, g_n\} \).

**Definition**

*We define*

\[
\mu_{m,j} \triangleq \frac{\langle \text{GS}(g_m), \text{GS}(g_j) \rangle}{\| \text{GS}(g_j) \|^2},
\]

*where* \( 1 \leq m, j \leq n \).*
The orthogonal vectors generated by the Gram-Schmidt orthogonalization procedure are denoted by \{GS(g_1), \ldots, GS(g_n)\} which spans the same space of \{g_1, \ldots, g_n\}.

**Definition**

We define

\[ \mu_{m,j} \triangleq \frac{\langle GS(g_m), GS(g_j) \rangle}{\|GS(g_j)\|^2}, \]

where \(1 \leq m, j \leq n\).

**Definition**

The \(m\)-th successive minima of a lattice, denoted by \(\lambda_m\), is the radius of the smallest possible closed ball around origin containing \(m\) or more linearly independent lattice points forming a basis.
Definitions

CLLL Reduction

A generator matrix $\mathbf{G}'$ for a lattice $\Lambda$ is called **LLL-reduced** if it satisfies

1. $|\mu_{m,j}| \leq 1/2$ for all $1 \leq j < m \leq n$, and
2. $\delta \|\text{GS} (\mathbf{g}'_{m-1}) \|^2 \leq \|\text{GS} (\mathbf{g}'_m) + \mu_{m,m-1}^2 \text{GS} (\mathbf{g}'_{m-1}) \|^2$ for all $1 < m \leq n$,

where $\delta \in (1/4, 1]$ is a factor selected to achieve a good quality-complexity tradeoff.
Definitions

Mikowski Lattice Reduction

A lattice generator matrix $G'$ is called **Minkowski-reduced** if for $1 \leq m \leq n$, the vectors $g'_m$ are as short as possible.
Definitions

Mikowski Lattice Reduction

A lattice generator matrix $G'$ is called **Minkowski-reduced** if for $1 \leq m \leq n$, the vectors $g'_m$ are as short as possible.

In particular, $G'$ is Minkowski-reduced if for $1 \leq m \leq n$, the row vector $g'_m$ has minimum possible energy amongst all the other lattice points such that $\{g'_1, \ldots, g'_m\}$ can be extended to another basis of $\Lambda$. 
A generator matrix $G'$ for a lattice $\Lambda$ is called **HKZ-reduced** if it satisfies

1. $|R_{m,j}| \leq \frac{1}{2}|R_{m,m}|$ for all $1 \leq m \leq j \leq n$, and
2. $R_{j,j}$ be the length of the shortest vector of a lattice generated by the columns of the sub matrix $R([j, j + 1, \ldots, n], [j, j + 1, \ldots, n])$.

Note that $G' = QR$ is the QR decomposition of $G'$. 

Definitions

HKZ Lattice Reduction
The $m$-th row vector in $\mathbf{G}'$ is upper bounded by a scaled version of the $m$-th successive minima of $\Lambda$.

- For CLLL reduction, we have

$$\beta^{1-m} \lambda_m^2 \leq \|\mathbf{g}'_m\|^2 \leq \beta^{n-1} \lambda_m^2, \text{ for } 1 \leq m \leq n,$$

where $\beta = (\delta - 1/4)^{-1}$. 
Definitions

Properties

The $m$-th row vector in $\mathbf{G}'$ is upper bounded by a scaled version of the $m$-th successive minima of $\Lambda$.

- For CLLL reduction, we have
  \[
  \beta^{1-m} \lambda_m^2 \leq \|\mathbf{g}_m'\|^2 \leq \beta^{n-1} \lambda_m^2, \text{ for } 1 \leq m \leq n,
  \]
  where $\beta = (\delta - 1/4)^{-1}$.

- For the Minkowski reduction, we have
  \[
  \lambda_m^2 \leq \|\mathbf{g}_m'\|^2 \leq \max \left\{ 1, \left(\frac{5}{4}\right)^{n-4} \right\} \lambda_m^2, \text{ for } 1 \leq m \leq n.
  \]
The \( m \)-th row vector in \( \mathbf{G}' \) is upper bounded by a scaled version of the \( m \)-th successive minima of \( \Lambda \).

- For CLLL reduction, we have
  \[
  \beta^{1-m} \lambda_m^2 \leq \|\mathbf{g}_m'\|^2 \leq \beta^{n-1} \lambda_m^2, \quad \text{for } 1 \leq m \leq n,
  \]
  where \( \beta = (\delta - 1/4)^{-1} \).

- For the Minkowski reduction, we have
  \[
  \lambda_m^2 \leq \|\mathbf{g}_m'\|^2 \leq \max \left\{ 1, \left( \frac{5}{4} \right)^{n-4} \right\} \lambda_m^2, \quad \text{for } 1 \leq m \leq n.
  \]

- For the HKZ reduction, we have
  \[
  \frac{4\lambda_m^2}{m + 3} \leq \|\mathbf{g}_m'\|^2 \leq \frac{(m + 3)\lambda_m^2}{4}, \quad \text{for } 1 \leq m \leq n.
  \]
One Example of Using Lattice Reduction Algorithms
We consider a flat-fading MIMO channel with $n$ transmit antennas and $n$ receive antennas.
We consider a flat-fading MIMO channel with \( n \) transmit antennas and \( n \) receive antennas.

The channel matrix is denoted by \( \mathbf{G} \in \mathbb{C}^{n \times n} \), where the entries of \( \mathbf{G} \) are i.i.d. as \( \mathcal{CN}(0, 1) \).
We consider a flat-fading MIMO channel with $n$ transmit antennas and $n$ receive antennas.

The channel matrix is denoted by $\mathbf{G} \in \mathbb{C}^{n\times n}$, where the entries of $\mathbf{G}$ are i.i.d. as $\mathcal{CN}(0, 1)$.

For $1 \leq m \leq n$, the $m$-th layer is equipped with an encoder $E : \mathcal{R}^k \rightarrow \mathbb{C}^N$ which maps a message $\mathbf{m} \in \mathcal{R}^k$ over the ring $\mathcal{R}$ into a lattice codeword $\mathbf{x}_m \in \Lambda \subset \mathbb{C}^N$ in the complex space.
If $X$ denotes the matrix of transmitted vectors, the received signal $Y$ is given by

$$Y_{n \times N} = \sqrt{P}G_{n \times n}X_{n \times N} + Z_{n \times N},$$

where $P = \frac{\text{SNR}}{n}$ and SNR denotes the average signal-to-noise ratio at each receive antenna.
If $X$ denotes the matrix of transmitted vectors, the received signal $Y$ is given by

$$Y_{n \times N} = \sqrt{P} G_{n \times n} X_{n \times N} + Z_{n \times N},$$

where $P = \frac{\text{SNR}}{n}$ and SNR denotes the average signal-to-noise ratio at each receive antenna.

We assume that the entries of $Z$ are i.i.d. as $CN(0, 1)$. 

This model will be used in this section.
• This model will be used in this section.
• Lattice reductions can improve the performance of MIMO channels if employed at either transmitters or receivers.
This model will be used in this section.

Lattice reductions can improve the performance of MIMO channels if employed at either transmitters or receivers.

Lattice-reduction-aided MIMO detectors, Lattice reduction precoders, etc.
In order to uniquely recover the information symbols, the matrix $A$ must be invertible over the ring $\mathcal{R}$. Thus, we have

$$Y' = BY = \sqrt{P}BGX + BZ.$$
In order to uniquely recover the information symbols, the matrix $A$ must be invertible over the ring $\mathcal{R}$. Thus, we have

$$Y' = BY = \sqrt{P}BGX + BZ.$$ 

The goal is to project $G$ (by left multiplying it with a receiver filtering matrix $B$) onto a non-singular integer matrix $A$. 
In order to uniquely recover the information symbols, the matrix $A$ must be invertible over the ring $\mathcal{R}$. Thus, we have

$$Y' = BY = \sqrt{P}BGX + BZ.$$ 

The goal is to project $G$ (by left multiplying it with a receiver filtering matrix $B$) onto a non-singular integer matrix $A$.

For the IF receiver formulation, a suitable signal model is

$$Y' = \sqrt{P}AX + \sqrt{P}(BG - A)X + BZ,$$

where $\sqrt{P}AX$ is the desired signal component, and the effective noise is $\sqrt{P}(BG - A)X + BZ$. 
In particular, the effective noise power along the $m$-th row of $Y'$ is defined as

$$g(a_m, b_m) \triangleq \|b_m\|^2 + P\|b_mG - a_m\|^2,$$

where $a_m$ and $b_m$ denotes the $m$-th row of $A$ and $B$, respectively.
Problem Formulation

In particular, the effective noise power along the \( m \)-th row of \( Y' \) is defined as

\[
g(a_m, b_m) \triangleq \|b_m\|^2 + P\|b_m G - a_m\|^2,
\]

where \( a_m \) and \( b_m \) denotes the \( m \)-th row of \( A \) and \( B \), respectively.

Problem Given \( G \) and \( P \), the problem is to find the matrices \( B \in \mathbb{C}^{n \times n} \) and \( A \in \mathbb{Z}[i]^{n \times n} \) such that:

- The \( \max_{1 \leq m \leq n} g(a_m, b_m) \) is minimized, and
- The corresponding matrix \( A \) is invertible over the ring \( \mathcal{R} \).
Given $a$, the optimum value of $b_m$ can be obtained as

$$b_m = aG^hS^{-1}.$$
Given \( a \), the optimum value of \( b_m \) can be obtained as

\[
b_m = aG^hS^{-1}.
\]

Then, after replacing \( b_m \) in \( g(a, b_m) \), we get

\[
a_m = \arg \min_{a \in \mathbb{Z}[i]^n} aVDV^h a^h,
\]

where \( V \) is the matrix composed of the eigenvectors of \( GG^h \), and \( D \) is a diagonal matrix with \( m \)-th entry

\[
D_{m,m} = (P\rho_m^2 + 1)^{-1},
\]

where \( \rho_m \) is the \( m \)-th singular value of \( G \).
With this, we have to obtain $n$ vectors $a_m$, $1 \leq m \leq n$, which result in the first $n$ smaller values of $aVDA^h$ along with the non-singular property on $A$. 
With this, we have to obtain \( n \) vectors \( a_m, 1 \leq m \leq n \), which result in the first \( n \) smaller values of \( aVDV^h a^h \) along with the non-singular property on \( A \).

The minimization problem is the shortest vector problem for a lattice with Gram matrix \( M = VDV^h \).
With this, we have to obtain $n$ vectors $\mathbf{a}_m$, $1 \leq m \leq n$, which result in the first $n$ smaller values of $\mathbf{a}^\dagger \mathbf{V} \mathbf{D} \mathbf{V}^\dagger \mathbf{a}^\dagger$ along with the non-singular property on $\mathbf{A}$.

The minimization problem is the shortest vector problem for a lattice with Gram matrix $\mathbf{M} = \mathbf{V} \mathbf{D} \mathbf{V}^\dagger$.

Since $\mathbf{M}$ is a positive definite matrix, we can write $\mathbf{M} = \mathbf{L} \mathbf{L}^\dagger$ for some $\mathbf{L} \in \mathbb{C}^{n \times n}$ by using Choelsky decomposition.
With this, we have to obtain \( n \) vectors \( a_m, 1 \leq m \leq n \), which result in the first \( n \) smaller values of \( aVDV^h a^h \) along with the non-singular property on \( A \).

The minimization problem is the shortest vector problem for a lattice with Gram matrix \( M = VDV^h \).

Since \( M \) is a positive definite matrix, we can write \( M = LL^h \) for some \( L \in \mathbb{C}^{n \times n} \) by using Choelsky decomposition.

With this, the rows of \( L = VD^{\frac{1}{2}} \) generate a lattice, say \( \Lambda \).
With this, we have to obtain \( n \) vectors \( \mathbf{a}_m, 1 \leq m \leq n \), which result in the first \( n \) smaller values of \( \mathbf{a}^{\mathbf{V}} \mathbf{D} \mathbf{V}^h \mathbf{a}^h \) along with the non-singular property on \( \mathbf{A} \).

The minimization problem is the shortest vector problem for a lattice with Gram matrix \( \mathbf{M} = \mathbf{V} \mathbf{D} \mathbf{V}^h \).

Since \( \mathbf{M} \) is a positive definite matrix, we can write \( \mathbf{M} = \mathbf{L} \mathbf{L}^h \) for some \( \mathbf{L} \in \mathbb{C}^{n \times n} \) by using Choelsky decomposition.

With this, the rows of \( \mathbf{L} = \mathbf{V} \mathbf{D}^{\frac{1}{2}} \) generate a lattice, say \( \Lambda \).

A set of possible choices for \( \{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \) is the set of complex integer vectors, whose corresponding lattice points in \( \Lambda \) have lengths at most equal to the \( n \)-th successive minima of \( \Lambda \).
The Proposed Algorithm

The two well-known lattice reduction algorithms satisfying the above property up to constants are HKZ and Minkowski lattice reduction algorithms.
The two well-known lattice reduction algorithms satisfying the above property up to constants are HKZ and Minkowski lattice reduction algorithms.

**Input:** $G \in \mathbb{C}^{n \times n}$, and $P$.

**Output:** A unimodular matrix $A$.

1. Form the generator matrix $L = VD^{1/2}$ of a lattice $\Lambda$.
2. Reduce $L$ to $L'$ using either HKZ or Minkowski lattice reduction algorithm.
3. The $n$ rows of $L'L^{-1}$ provide $n$ rows $a_m$ of $A$ for $1 \leq m \leq n$. 
Theorem (Sakzad’13)

For a MIMO channel with $n$ transmit and $n$ receive antennas over a Rayleigh fading channel, the integer-forcing linear receiver based on lattice reduction achieves full receive diversity.
Performance against exhaustive search

![Graph](image-url)
A toy example from Cryptography
GGH involves a private key and a public key.
1. GGH involves a private key and a public key.

2. The private key of user $j$ is a generator matrix $G_j$ of a lattice $\Lambda$ with “nearly orthogonal” basis vectors and a unimodular matrix $U_j$, for $j \in \{a, b\}$. 
GGH public-key cryptosystem

Public and private keys

1. GGH involves a private key and a public key.
2. The private key of user $j$ is a generator matrix $G_j$ of a lattice $\Lambda$ with “nearly orthogonal” basis vectors and a unimodular matrix $U_j$, for $j \in \{a, b\}$.
3. The public key of user $j$ is $G'_j = U_j G_j$, which is another generator matrix of the lattice $\Lambda$. 
GGH involves a private key and a public key.

2. The private key of user $j$ is a generator matrix $G_j$ of a lattice $\Lambda$ with “nearly orthogonal” basis vectors and a unimodular matrix $U_j$, for $j \in \{a, b\}$.

3. The public key of user $j$ is $G'_j = U_j G_j$, which is another generator matrix of the lattice $\Lambda$.

4. Security parameters are $n$ and $\sigma$. 
GGH involves a private key and a public key.

The private key of user $j$ is a generator matrix $G_j$ of a lattice $\Lambda$ with “nearly orthogonal” basis vectors and a unimodular matrix $U_j$, for $j \in \{a, b\}$.

The public key of user $j$ is $G'_j = U_j G_j$, which is another generator matrix of the lattice $\Lambda$.

Security parameters are $n$ and $\sigma$.

Works based on the hardness of closest vector problem (CVP).
1. Alice wants to send a message \( m \) to Bob.
Alice wants to send a message $m$ to Bob.

She uses Bob’s public key $G'_b$ and encrypts $m$ to

$$c = mG'_b + e,$$

where $e \in \{\pm \sigma\}^n$. 
Alice wants to send a message $m$ to Bob.

She uses Bob’s public key $G_b'$ and encrypts $m$ to

$$c = mG_b' + e,$$

where $e \in \{\pm \sigma\}^n$.

Bob employs $U$ and $G$ to decrypt $c$ as follows. Bob first computes

$$cG_b^{-1} = mG_b'G_b^{-1} + eG_b^{-1} = mU_b + eG_b^{-1},$$

then

$$\lfloor cG_b^{-1} \rfloor U_b^{-1} = mU_b U_b^{-1} = m.$$
Various attacks have been proposed. Almost dead!
Various attacks have been proposed. Almost dead!

NTRU is a special instance of GGH using a circulant matrix for the public key.
1. Various attacks have been proposed. Almost dead!
2. NTRU is a special instance of GGH using a circulant matrix for the public key.
3. Increase the dimension of the lattice up to 1000.
Various attacks have been proposed. Almost dead!

NTRU is a special instance of GGH using a circulant matrix for the public key.

Increase the dimension of the lattice up to 1000.

One very famous attack on these cryptosystems is lattice reduction algorithms.
<table>
<thead>
<tr>
<th>Sphere Decoder Algorithm</th>
<th>Lattice Reduction Algorithms</th>
<th>Integer-Forcing Linear Receiver</th>
<th>Lattice-based Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GGH public-key cryptosystem

Thanks for your attention!