# PM comme un problème mathématique

Martin Minchev[1,3], Mladen Savov[1,2], Stefan Gerdjikov[1,2]

[1]FMI, Sofia University
[2]Bulgarian Academy of Sciences
[3]University of Zurich

7th December 2025

# Equilateral triangles on a hypercube

**Problem**

Let $A, B, C$ be uniformly drawn vertices of the hypercube $\{0, 1\}^d$. Denote by $p_3(d)$ the probability that $\triangle ABC$ is equilateral. Find the asymptotic of $p_3(d)$ as $d$ tends to infinity.

$$A\ \begin{array}{|c|c|c|c|}\hline \underbrace{00\ldots\ldots\ldots0}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$B\ \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{11\ldots\ldots\ldots1}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$C\ \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{11\ldots\ldots\ldots1}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$A\ \boxed{\underbrace{00\ldots\ldots\ldots0}_{k}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_B}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_C}}\boxed{00\ldots\ldots\ldots0}$$

$$B\ \boxed{\underbrace{11\ldots\ldots\ldots1}_{k}}\boxed{\underbrace{11\ldots\ldots\ldots1}_{\ell_B}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_C}}\boxed{00\ldots\ldots\ldots0}$$

$$C\ \boxed{\underbrace{11\ldots\ldots\ldots1}_{k}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_B}}\boxed{\underbrace{11\ldots\ldots\ldots1}_{\ell_C}}\boxed{00\ldots\ldots\ldots0}$$

- By symmetry, w.l.o.g. $A = (0, \ldots, 0)$,
- Pick $k$ – the number of common ones of $B$ and $C$.

$$A \; \begin{array}{|c|c|c|c|}\hline \underbrace{00\ldots\ldots\ldots0}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline\end{array}$$

$$B \; \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{11\ldots\ldots\ldots1}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline\end{array}$$

$$C \; \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{11\ldots\ldots\ldots1}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline\end{array}$$

- By symmetry, w.l.o.g. $A = (0, \ldots, 0)$,
- Pick $k$ – the number of common ones of $B$ and $C$.
- Pick $\ell_B$ – the number of ones of $B$ that are not ones of $C$.

$$A \quad \boxed{\underbrace{00\ldots\ldots\ldots0}_{k}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_B}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_C}}\boxed{00\ldots\ldots\ldots0}$$

$$B \quad \boxed{\underbrace{11\ldots\ldots\ldots1}_{k}}\boxed{\underbrace{11\ldots\ldots\ldots1}_{\ell_B}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_C}}\boxed{00\ldots\ldots\ldots0}$$

$$C \quad \boxed{\underbrace{11\ldots\ldots\ldots1}_{k}}\boxed{\underbrace{00\ldots\ldots\ldots0}_{\ell_B}}\boxed{\underbrace{11\ldots\ldots\ldots1}_{\ell_C}}\boxed{00\ldots\ldots\ldots0}$$

- By symmetry, w.l.o.g. $A = (0, \ldots, 0)$,
- Pick $k$ – the number of common ones of $B$ and $C$.
- Pick $\ell_B$ – the number of ones of $B$ that are not ones of $C$.
- Pick $\ell_C$ – the number of ones of $C$ that are not ones of $B$.

$$A\ \boxed{\underbrace{00\ldots\ldots\ldots0}_{k}\ \Big|\ \underbrace{00\ldots\ldots\ldots0}_{\ell_B}\ \Big|\ \underbrace{00\ldots\ldots\ldots0}_{\ell_C}\ \Big|\ 00\ldots\ldots\ldots0}$$

$$B\ \boxed{\underbrace{11\ldots\ldots\ldots1}_{k}\ \Big|\ \underbrace{11\ldots\ldots\ldots1}_{\ell_B}\ \Big|\ \underbrace{00\ldots\ldots\ldots0}_{\ell_C}\ \Big|\ 00\ldots\ldots\ldots0}$$

$$C\ \boxed{\underbrace{11\ldots\ldots\ldots1}_{k}\ \Big|\ \underbrace{00\ldots\ldots\ldots0}_{\ell_B}\ \Big|\ \underbrace{11\ldots\ldots\ldots1}_{\ell_C}\ \Big|\ 00\ldots\ldots\ldots0}$$

- By symmetry, w.l.o.g. $A = (0, \ldots, 0)$,
- Pick $k$ – the number of common ones of $B$ and $C$.
- Pick $\ell_B$ – the number of ones of $B$ that are not ones of $C$.
- Pick $\ell_C$ – the number of ones of $C$ that are not ones of $B$.
- To meet the condition that $\triangle ABC$ is equilateral:
  $k + \ell_B = k + \ell_C = \ell_C + \ell_B$.

$$A \ \begin{array}{|c|c|c|c|}\hline \underbrace{00\ldots\ldots\ldots0}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$B \ \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{11\ldots\ldots\ldots1}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$C \ \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{11\ldots\ldots\ldots1}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

- By symmetry, w.l.o.g. $A = (0, \ldots, 0)$,
- Pick $k$ – the number of common ones of $B$ and $C$.
- Pick $\ell_B$ – the number of ones of $B$ that are not ones of $C$.
- Pick $\ell_C$ – the number of ones of $C$ that are not ones of $B$.
- To meet the condition that $\triangle ABC$ is equilateral:
  $k + \ell_B = k + \ell_C = \ell_C + \ell_B$.
- Hence $\ell_B = \ell_C = k$.

$$A\ \begin{array}{|c|c|c|c|}\hline \underbrace{00\ldots\ldots\ldots0}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$B\ \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{11\ldots\ldots\ldots1}_{\ell_B} & \underbrace{00\ldots\ldots\ldots0}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

$$C\ \begin{array}{|c|c|c|c|}\hline \underbrace{11\ldots\ldots\ldots1}_{k} & \underbrace{00\ldots\ldots\ldots0}_{\ell_B} & \underbrace{11\ldots\ldots\ldots1}_{\ell_C} & 00\ldots\ldots\ldots0 \\ \hline \end{array}$$

- By symmetry, w.l.o.g. $A = (0, \ldots, 0)$,
- Pick $k$ – the number of common ones of $B$ and $C$.
- Pick $\ell_B$ – the number of ones of $B$ that are not ones of $C$.
- Pick $\ell_C$ – the number of ones of $C$ that are not ones of $B$.
- To meet the condition that $\triangle ABC$ is equilateral: $k + \ell_B = k + \ell_C = \ell_C + \ell_B$.
- Hence $\ell_B = \ell_C = k$.
- $p_3(d) = \frac{1}{2^{2d}} \sum_{k=0}^{d/3} \binom{d}{k,k,k,d-3k}$.

# Transposing the problem helps (1)

$$\begin{array}{c|cccccc|}
 & X^{(1)} & X^{(2)} & X^{(3)} & X^{(4)} & X^{(5)} & X^{(6)} \\
A = X_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
B = X_2 & 1 & 0 & 0 & 0 & 1 & 1 \\
C = X_3 & 1 & 1 & 1 & 0 & 1 & 0
\end{array}$$

- $X_1 = A,\ X_2 = B,\ X_3 = C.$
- $X_i = (X_i^{(1)}, \ldots, X_i^{(d)}),\ d^2(X_i, X_j) = \sum_{\ell=1}^{d} (X_i^{(\ell)} - X_j^{(\ell)})^2 = \|X_i - X_j\|^2.$

# Transposing the problem helps (2)

$$
\begin{array}{llcccccc}
 & & X^{(1)} & X^{(2)} & X^{(3)} & X^{(4)} & X^{(5)} & X^{(6)} \\
d^2(X_1, X_2) = 3 & A = X_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
d^2(X_2, X_3) = 3 & B = X_2 & 1 & 0 & 0 & 0 & 1 & 1 \\
d^2(X_3, X_1) = 4 & C = X_3 & 1 & 1 & 1 & 0 & 1 & 0
\end{array}
$$

$$
\begin{array}{lcccccc}
 & \mathbf{V}^{(1)} & \mathbf{V}^{(2)} & \mathbf{V}^{(3)} & \mathbf{V}^{(4)} & \mathbf{V}^{(5)} & \mathbf{V}^{(6)} \\
U = \|X_1 - X_3\|^2 - \|X_1 - X_2\|^2 & 0 & 1 & 1 & 0 & 0 & -1 \\
V = \|X_2 - X_3\|^2 - \|X_1 - X_2\|^2 & -1 & 1 & 1 & 0 & -1 & 0
\end{array}
$$

# Transposing the problem helps (2)

$$\begin{array}{lll|cccccc}
d^2(X_1,X_2)=3 & A = X_1 & & X^{(1)} & X^{(2)} & X^{(3)} & X^{(4)} & X^{(5)} & X^{(6)} \\
& & & \boxed{\begin{matrix}0\\1\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\\0\end{matrix}} & \boxed{\begin{matrix}0\\1\\1\end{matrix}} & \boxed{\begin{matrix}0\\1\\0\end{matrix}}
\end{array}$$

$d^2(X_1, X_2) = 3$ $\quad A = X_1$

$d^2(X_2, X_3) = 3$ $\quad B = X_2$

$d^2(X_3, X_1) = 4$ $\quad C = X_3$

$U = \|X_1 - X_3\|^2 - \|X_1 - X_2\|^2$

$V = \|X_2 - X_3\|^2 - \|X_1 - X_2\|^2$

$$\begin{array}{cccccc}
\mathbf{V}^{(1)} & \mathbf{V}^{(2)} & \mathbf{V}^{(3)} & \mathbf{V}^{(4)} & \mathbf{V}^{(5)} & \mathbf{V}^{(6)} \\
\boxed{\begin{matrix}0\\-1\end{matrix}} & \boxed{\begin{matrix}1\\1\end{matrix}} & \boxed{\begin{matrix}1\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\end{matrix}} & \boxed{\begin{matrix}0\\-1\end{matrix}} & \boxed{\begin{matrix}-1\\0\end{matrix}}
\end{array}$$

- $U^{(i)} = (X_1^{(i)} - X_3^{(i)})^2 - (X_1^{(i)} - X_2^{(i)})^2$
- $V^{(i)} = (X_2^{(i)} - X_3^{(i)})^2 - (X_1^{(i)} - X_2^{(i)})^2$

# Transposing the problem helps (2)

$$
\begin{array}{llcccccc}
 & & X^{(1)} & X^{(2)} & X^{(3)} & X^{(4)} & X^{(5)} & X^{(6)} \\
d^2(X_1, X_2) = 3 & A = X_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
d^2(X_2, X_3) = 3 & B = X_2 & 1 & 0 & 0 & 0 & 1 & 1 \\
d^2(X_3, X_1) = 4 & C = X_3 & 1 & 1 & 1 & 0 & 1 & 0
\end{array}
$$

$$
\begin{array}{lcccccc}
 & \mathbf{V}^{(1)} & \mathbf{V}^{(2)} & \mathbf{V}^{(3)} & \mathbf{V}^{(4)} & \mathbf{V}^{(5)} & \mathbf{V}^{(6)} \\
U = \|X_1 - X_3\|^2 - \|X_1 - X_2\|^2 & 0 & 1 & 1 & 0 & 0 & -1 \\
V = \|X_2 - X_3\|^2 - \|X_1 - X_2\|^2 & -1 & 1 & 1 & 0 & -1 & 0
\end{array}
$$

- $U^{(i)} = (X_1^{(i)} - X_3^{(i)})^2 - (X_1^{(i)} - X_2^{(i)})^2$
- $V^{(i)} = (X_2^{(i)} - X_3^{(i)})^2 - (X_1^{(i)} - X_2^{(i)})^2$
- $\mathbf{V}^{(\mathbf{i})} = \begin{pmatrix} U^{(i)} \\ V^{(i)} \end{pmatrix}$ for $i \leq d$ are i.i.d. $\begin{pmatrix} U \\ V \end{pmatrix}$ 2-dimensional vector.

# Transposing the problem helps (2)

$$\begin{array}{ccc|cccccc} & & & X^{(1)} & X^{(2)} & X^{(3)} & X^{(4)} & X^{(5)} & X^{(6)} \\ \hline d^2(X_1, X_2) = 3 & & A = X_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ d^2(X_2, X_3) = 3 & & B = X_2 & 1 & 0 & 0 & 0 & 1 & 1 \\ d^2(X_3, X_1) = 4 & & C = X_3 & 1 & 1 & 1 & 0 & 1 & 0 \end{array}$$

$$\begin{array}{c|cccccc} & \mathbf{V}^{(1)} & \mathbf{V}^{(2)} & \mathbf{V}^{(3)} & \mathbf{V}^{(4)} & \mathbf{V}^{(5)} & \mathbf{V}^{(6)} \\ \hline U = \|X_1 - X_3\|^2 - \|X_1 - X_2\|^2 & 0 & 1 & 1 & 0 & 0 & -1 \\ V = \|X_2 - X_3\|^2 - \|X_1 - X_2\|^2 & -1 & 1 & 1 & 0 & -1 & 0 \end{array}$$

- $U^{(i)} = (X_1^{(i)} - X_3^{(i)})^2 - (X_1^{(i)} - X_2^{(i)})^2$
- $V^{(i)} = (X_2^{(i)} - X_3^{(i)})^2 - (X_1^{(i)} - X_2^{(i)})^2$
- $\mathbf{V^{(i)}} = \begin{pmatrix} U^{(i)} \\ V^{(i)} \end{pmatrix}$ for $i \leq d$ are i.i.d. $\begin{pmatrix} U \\ V \end{pmatrix}$ 2-dimensional vector.
- $p_3(d) = \mathbb{P}(\sum_{i=1}^{d} \mathbf{V^{(i)}} = \mathbf{0})$.

# Central Limit Theorems

**Theorem (Central Limit Theorem)**

If $\mathbf{V^{(i)}} \sim \mathbf{V}$ are independent identically distributed random vectors with mean $\mathbb{E}V = \mu$ and covariance matrix $Var(V) = K$, then:

$$\frac{\sum_{i=1}^{n}(\mathbf{V^{(i)}} - \mu)}{\sqrt{n}} \to_d \mathcal{N}(0, K).$$

# Local (Central) Limit Theorem (LLT)

## Definition

Let $V = \{v_1, v_2, \ldots, v_N\} \subseteq \mathbb{R}^m$ be vectors with rank $m$. We denote by $\mathcal{L}at(V)$ the set of integer linear combinations of $V$:

$$\mathcal{L}at(V) = \{\sum_{i=1}^{N} k_i v_i \,|\, k_i \in \mathbb{Z} \text{ for } i \leq N\}.$$

We say that $\mathcal{L}at(V)$ is a lattice if it is discrete and in this case we denote by $|\mathcal{L}at(V)|$ the fundamental volume of $\mathcal{L}at(V)$.

# Local (Central) Limit Theorem (LLT)

## Definition

Let $V = \{v_1, v_2, \dots, v_N\} \subseteq \mathbb{R}^m$ be vectors with rank $m$. We denote by $\mathcal{L}at(V)$ the set of integer linear combinations of $V$:

$$\mathcal{L}at(V) = \{\sum_{i=1}^{N} k_i v_i \,|\, k_i \in \mathbb{Z} \text{ for } i \leq N\}.$$

We say that $\mathcal{L}at(V)$ is a lattice if it is discrete and in this case we denote by $|\mathcal{L}at(V)|$ the fundamental volume of $\mathcal{L}at(V)$.

## Theorem (Local Limit Theorem)

Let $V$ be centred ($\mathbb{E}V = 0$) $m$-dimensional random vector with values on an $m$-dimensional lattice $\mathcal{L}at(V)$. If $V^{(i)} \sim$ i.i.d.$V$, then:

$$\lim_{d\to\infty} \mathbb{P}(\sum_{i=1}^{d} V^{(i)} = 0).\frac{\sqrt{(2\pi d)^m |Var(V)|}}{|\mathcal{L}at(V)|} = 1$$

# Equilateral triangles become simple

## Remark

In our case $X_1, X_2, X_3 \sim \mathcal{U}(\{0, 1\})$ and

$$U = (X_1 - X_3)^2 - (X_1 - X_2)^2, \quad V = (X_2 - X_3)^2 - (X_1 - X_2)^2$$

.

# Equilateral triangles become simple

## Remark

In our case $X_1, X_2, X_3 \sim \mathcal{U}(\{0, 1\})$ and

$$U = (X_1 - X_3)^2 - (X_1 - X_2)^2, \quad V = (X_2 - X_3)^2 - (X_1 - X_2)^2$$

.

## Remark

$\mathbf{V} = \begin{pmatrix} U \\ V \end{pmatrix}$ takes values $\{(0,0), (1,1), (0,-1), (-1,0)\}$. So $m = 2$ and |Lat(V)|=1.

# Equilateral triangles become simple

## Remark

In our case $X_1, X_2, X_3 \sim \mathcal{U}(\{0, 1\})$ and

$$U = (X_1 - X_3)^2 - (X_1 - X_2)^2, \quad V = (X_2 - X_3)^2 - (X_1 - X_2)^2$$

.

## Remark

$\mathbf{V} = \begin{pmatrix} U \\ V \end{pmatrix}$ takes values $\{(0, 0), (1, 1), (0, -1), (-1, 0)\}$. So $m = 2$ and $|\mathrm{Lat}(\mathrm{V})|=1$.

## Remark

$Var(V) = \begin{pmatrix} 1/2 & 1/4 \\ 1/4 & 1/2 \end{pmatrix}$ and hence $|Var(V)| = 3.2^{-4}$. Now the LLT implies: $\lim_{d \to \infty} d\mathbb{P}(\sum_{i=1}^{d} V^{(i)} = 0) = \frac{4}{\pi\sqrt{3}}$.

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0, 1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_i X_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

1. $V_{j,k}^{(i)} = (X_j^{(i)} - X_k^{(i)})^2 - (X_n^{(i)} - X_{n-2}^{(i)})^2.$

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

1. $V_{j,k}^{(i)} = (X_j^{(i)} - X_k^{(i)})^2 - (X_n^{(i)} - X_{n-2}^{(i)})^2$.
2. Now $V^{(i)}$ is $(m-1)$-dimensional vector where $m = \frac{n(n-1)}{2}$.

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

1. $V_{j,k}^{(i)} = (X_j^{(i)} - X_k^{(i)})^2 - (X_n^{(i)} - X_{n-2}^{(i)})^2$.
2. Now $V^{(i)}$ is $(m-1)$-dimensional vector where $m = \frac{n(n-1)}{2}$.
3. $p_n(d) = \mathbb{P}(\sum_{i=1}^d \mathbf{V^{(i)}} = \mathbf{0})$.

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

1. $V_{j,k}^{(i)} = (X_j^{(i)} - X_k^{(i)})^2 - (X_n^{(i)} - X_{n-2}^{(i)})^2$.
2. Now $V^{(i)}$ is $(m-1)$-dimensional vector where $m = \frac{n(n-1)}{2}$.
3. $p_n(d) = \mathbb{P}(\sum_{i=1}^d \mathbf{V^{(i)}} = \mathbf{0})$.
4. $V_{j,k} = (X_j - X_k)^2 - (X_n - X_{n-2})^2$.

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

1. $V_{j,k}^{(i)} = (X_j^{(i)} - X_k^{(i)})^2 - (X_n^{(i)} - X_{n-2}^{(i)})^2$.
2. Now $V^{(i)}$ is $(m-1)$-dimensional vector where $m = \frac{n(n-1)}{2}$.
3. $p_n(d) = \mathbb{P}(\sum_{i=1}^{d} \mathbf{V^{(i)}} = \mathbf{0})$.
4. $V_{j,k} = (X_j - X_k)^2 - (X_n - X_{n-2})^2$.
5. $|Var(V)| = m4^{-m-1}$ where $m = \frac{n(n-1)}{2}$.

# Modelling $n$-equidistant points on a hypercube

## Problem

Let $X_1, \ldots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

1. $V_{j,k}^{(i)} = (X_j^{(i)} - X_k^{(i)})^2 - (X_n^{(i)} - X_{n-2}^{(i)})^2$.
2. Now $V^{(i)}$ is $(m-1)$-dimensional vector where $m = \frac{n(n-1)}{2}$.
3. $p_n(d) = \mathbb{P}(\sum_{i=1}^{d} \mathbf{V^{(i)}} = \mathbf{0})$.
4. $V_{j,k} = (X_j - X_k)^2 - (X_n - X_{n-2})^2$.
5. $|Var(V)| = m4^{-m-1}$ where $m = \frac{n(n-1)}{2}$.
6. By LLT: $\lim_{d\to\infty} p_n(d) \frac{\sqrt{(2\pi d)^{m-1}|Var(V)|}}{|\mathcal{L}at(V)|} = 1$.

# The structure of the Lattice (1)

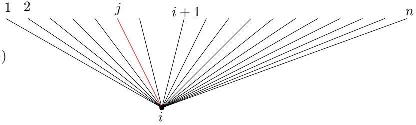
**Lemma**

Let $m = \binom{n}{2}$ and consider $\mathbb{R}^m$ with standard orthonormal basis $e_{i,j} = e_{j,i}$ indexed over $1 \leq i < j \leq n$. For a set $I \subseteq \{1, 2, \ldots, n\}$, let $H(I) = \sum_{i \in I} \sum_{j \in I^c} e_{i,j}$ and set $[i] = \{1, 2, \ldots, i\}$ for $i \leq n$.
Then lattice induced $\mathcal{L}at(H)$ by $\{H(I) \mid I \subseteq \{1, 2, \ldots, n\}\}$ is generated by the independent vectors:

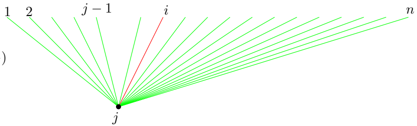
$$\{2e_{i,j} \mid i + 1 < j\} \cup \{H([i]) \mid i \leq n - 1\}.$$

Furthermore $|\mathcal{L}at(H)| = 2^{m-n+1}$.

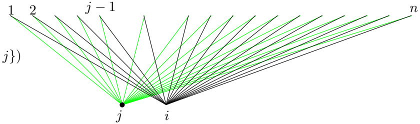
$H(\{i\})$




$H(\{j\})$

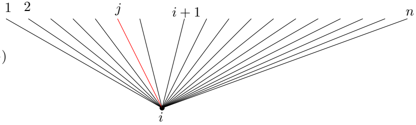



$H(\{i,j\})$

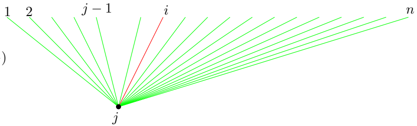



$$H(\{i\}) + H(\{j\}) - H(\{i,j\}) = 2e_{i,j}$$

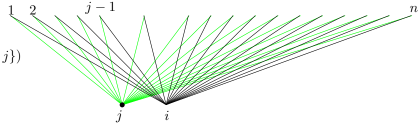
$H(\{i\})$



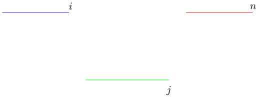

$H(\{j\})$



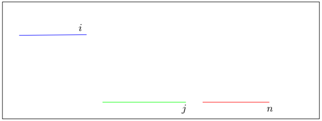

$H(\{i,j\})$



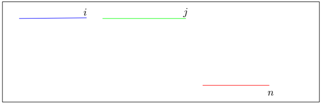

$$H(\{i\}) + H(\{j\}) - H(\{i,j\}) = 2e_{i,j}$$




$H([j] \setminus [i])$

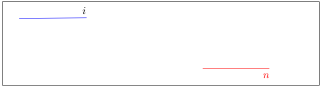



$H([i])$




$H([j])$

$2\times$




$\Sigma_{k\leq i}\,\Sigma_{\ell>j}\,2e_{k,\ell}$

# The structure of the Lattice (2)

## Remark

Let $m = \binom{n}{2}$ and consider $\mathbb{R}^m$ with standard orthonormal basis $e_{i,j} = e_{j,i}$ indexed over $1 \leq i < j \leq n$. For a set $I \subseteq \{1, 2, \ldots, n\}$, let $H(I) = \sum_{i \in I} \sum_{j \in I^c} e_{i,j}$ and $\delta(I) = 1_{|\{n-2,n\} \triangle I|=1}$.

# The structure of the Lattice (2)

## Remark

Let $m = \binom{n}{2}$ and consider $\mathbb{R}^m$ with standard orthonormal basis $e_{i,j} = e_{j,i}$ indexed over $1 \le i < j \le n$. For a set $I \subseteq \{1, 2, \dots, n\}$, let $H(I) = \sum_{i \in I} \sum_{j \in I^c} e_{i,j}$ and $\delta(I) = 1_{|\{n-2,n\} \triangle I| = 1}$.

## Lemma

The lattice induced $\mathcal{L}at(V)$ by $\{H(I) - \delta(I)\mathbf{1} \mid I \subseteq \{1, 2, \dots, n\}\}$ is generated by the independent vectors:

- $2e_{i,j}$ for $i < n-2$ and $i+1 < j$,
- $H([i])$ for $i < n-2$,
- $H[n-2] - \mathbf{1}$ and $H[n-1] - \mathbf{1}$.

Furthermore $|\mathcal{L}at(V)| = 2^{m-n}$.

# The structure of the Lattice (2)

**Sketch.**

- Clearly, the named vectors are in $\mathcal{L}at(V)$.

# The structure of the Lattice (2)

## Sketch.

- Clearly, the named vectors are in $\mathcal{L}at(V)$.
- Since $\mathbf{21} = \sum_{i<j} 2e_{i,j}$ and all $e_{i,j}$ are in the lattice $H$, we can substitute $2e_{n-2,n}$ with $\mathbf{21}$ in the generating set for $\mathcal{L}at(H)$.

# The structure of the Lattice (2)

## Sketch.

- Clearly, the named vectors are in $\mathcal{L}at(V)$.
- Since $\mathbf{21} = \sum_{i<j} 2e_{i,j}$ and all $e_{i,j}$ are in the lattice $H$, we can substitute $2e_{n-2,n}$ with $\mathbf{21}$ in the generating set for $\mathcal{L}at(H)$.
- Then for $I \subseteq [n]$:

$$H(I) = \sum_{i=1}^{n-1} a_i H([i]) + \sum_{i+1<j, i+1<n-2} 2b_{i,j}e_{i,j} + 2c\mathbf{1}.$$

# The structure of the Lattice (2)

## Sketch.

- Clearly, the named vectors are in $\mathcal{L}at(V)$.
- Since $\mathbf{21} = \sum_{i<j} 2e_{i,j}$ and all $e_{i,j}$ are in the lattice $H$, we can substitute $2e_{n-2,n}$ with $\mathbf{21}$ in the generating set for $\mathcal{L}at(H)$.
- Then for $I \subseteq [n]$:

$$H(I) = \sum_{i=1}^{n-1} a_i H([i]) + \sum_{i+1<j, i+1<n-2} 2b_{i,j} e_{i,j} + 2c\mathbf{1}.$$

- Comparing the coefficients before $e_{n-2,n}$: $\delta(I) = \sum_{i=1}^{n-1} a_i \delta([i]) + 2c$.

# The structure of the Lattice (2)

## Sketch.

- Clearly, the named vectors are in $\mathcal{L}at(V)$.
- Since $\mathbf{21} = \sum_{i<j} 2e_{i,j}$ and all $e_{i,j}$ are in the lattice $H$, we can substitute $2e_{n-2,n}$ with $\mathbf{21}$ in the generating set for $\mathcal{L}at(H)$.
- Then for $I \subseteq [n]$:

$$H(I) = \sum_{i=1}^{n-1} a_i H([i]) + \sum_{i+1<j, i+1<n-2} 2b_{i,j}e_{i,j} + 2c\mathbf{1}.$$

- Comparing the coefficients before $e_{n-2,n}$: $\delta(I) = \sum_{i=1}^{n-1} a_i\delta([i]) + 2c$.
- Summing up, $(H(I) - \delta(I)\mathbf{1}) - \sum_{i+1<j,i+1<n-2} 2b_{i,j}e_{i,j}$ equals:

$$\sum_{i=1}^{n-3} a_i H([i]) + a_{n-1}(H([n-1]) - \mathbf{1}) + a_{n-2}(H([n-2]) - \mathbf{1}).$$

# Uniform $d$-equidistant points on a hypercube

**Problem**

Let $X_1, \dots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0, 1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

# Uniform $d$-equidistant points on a hypercube

## Problem

Let $X_1, \dots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0,1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

## Remark

Recall that $m = \binom{n}{2}$:

- $|Var(V)| = m4^{-m-1}$.
- By LLT: $\lim_{d\to\infty} p_n(d) \frac{\sqrt{(2\pi d)^{m-1}|Var(V)|}}{|\mathcal{L}at(V)|} = 1$.

# Uniform $d$-equidistant points on a hypercube

## Problem

Let $X_1, \dots, X_n$ be uniformly and independently drawn vertices of the hypercube $\{0, 1\}^d$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

## Remark

Recall that $m = \binom{n}{2}$:

- $|Var(V)| = m4^{-m-1}$.
- By LLT: $\lim_{d\to\infty} p_n(d)\frac{\sqrt{(2\pi d)^{m-1}|Var(V)|}}{|\mathcal{L}at(V)|} = 1$.

## Theorem

$$\lim_{d\to\infty} p_n(d)d^{(m-1)/2} = \sqrt{\frac{2^{3m-n+1}}{m\pi^{m-1}}}.$$

## $n$-equidistant points with integer/rational coordinates. The lattice.

### Problem

Let $X$ be a random, non-constant, variable taking values on a finite subset of $\mathbb{Z}$ or on a finite subset of $\mathbb{Q}$.
Let $X_1, \dots, X_n$ be independently drawn $d$-dimensional vectors with coordinates $X_{i,j} \sim$ i.i.d$X$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

# $n$-equidistant points with integer/rational coordinates. The lattice.

## Problem

Let $X$ be a random, non-constant, variable taking values on a finite subset of $\mathbb{Z}$ or on a finite subset of $\mathbb{Q}$.
Let $X_1, \ldots, X_n$ be independently drawn $d$-dimensional vectors with coordinates $X_{i,j} \sim$ i.i.d$X$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

## Remark

Let $X \in \mathcal{X} = \{x_1, \ldots, x_k\}$. Since $|\mathcal{L}at(V)|/\sqrt{|Var(V)|}$ is scaling and translation invariant, we can centre and normalise the values $x_i$ by an appropriate factor $s$, s.t. $sx_i \in \mathbb{N}$ and $\{sx_i \,|\, i \leq k\}$ have greatest common divisor 1.
This reduces the problem to the $\{0, 1\}$-case and $|\mathcal{L}at(V)| = 2^{m-n}$.

# $n$-equidistant points with integer/rational coordinates. The volume.

## Theorem

Let $m = \binom{n}{2}$, $C = (Var(X))^2$ and $C_1 = Var((X - \mathbb{E}X)^2)$. Then

$$|Var(V)| = 4^{m-n} C^{m-n} (4C + (n-2)C_1)^{n-1}.$$

Furthermore:

$$\lim_{d \to \infty} d^{(m-1)/2} p_n(d) = \frac{1}{\sqrt{(2\pi)^{m-1} C^{m-n} (4C + (n-2)C_1)^{n-1}}}.$$

## Proof Idea (Step 1).

- Recall $V_{i,j} = (X_i - X_j)^2 - (X_n - X_{n-2})^2$. Set $C_0 = Var((X_1 - X_2)^2) = 2C - 2C_1$.

## Proof Idea (Step 1).

- Recall $V_{i,j} = (X_i - X_j)^2 - (X_n - X_{n-2})^2$. Set $C_0 = Var((X_1 - X_2)^2) = 2C - 2C_1$.
- Write $\alpha = \{i, j\}$ and $\beta = \{k, \ell\}$, $A_\alpha = A_{i,j} := (X_i - X_j)^2$, $\gamma = \{1, 2\}$

$$Cov(V_\alpha, V_\beta) = Cov(A_\alpha, A_\beta) - Cov(A_\gamma, A_\alpha) - Cov(A_\gamma, A_\beta) + Cov(A_\gamma, A_\gamma).$$

$\square$

## Proof Idea (Step 1).

- Recall $V_{i,j} = (X_i - X_j)^2 - (X_n - X_{n-2})^2$. Set $C_0 = Var((X_1 - X_2)^2) = 2C - 2C_1$.
- Write $\alpha = \{i,j\}$ and $\beta = \{k,\ell\}$, $A_\alpha = A_{i,j} := (X_i - X_j)^2$, $\gamma = \{1,2\}$

$$Cov(V_\alpha, V_\beta) = Cov(A_\alpha, A_\beta) - Cov(A_\gamma, A_\alpha) - Cov(A_\gamma, A_\beta) + Cov(A_\gamma, A_\gamma).$$

- $Cov(A_\alpha, A_\beta) = \begin{cases} 0 \text{ for } \alpha \cap \beta = \emptyset \\ C_0 \text{ for } \alpha = \beta, \\ C_1 \text{ for } |\alpha \cap \beta| = 1 \end{cases}$

## Proof Idea (Step 1).

- Recall $V_{i,j} = (X_i - X_j)^2 - (X_n - X_{n-2})^2$. Set $C_0 = Var((X_1 - X_2)^2) = 2C - 2C_1$.
- Write $\alpha = \{i,j\}$ and $\beta = \{k,\ell\}$, $A_\alpha = A_{i,j} := (X_i - X_j)^2$, $\gamma = \{1,2\}$

$$Cov(V_\alpha, V_\beta) = Cov(A_\alpha, A_\beta) - Cov(A_\gamma, A_\alpha) - Cov(A_\gamma, A_\beta) + Cov(A_\gamma, A_\gamma).$$

- $Cov(A_\alpha, A_\beta) = \begin{cases} 0 \text{ for } \alpha \cap \beta = \emptyset \\ C_0 \text{ for } \alpha = \beta, \\ C_1 \text{ for } |\alpha \cap \beta| = 1 \end{cases}$
- So with $h_{\alpha,\beta} = \begin{cases} 1 \text{ if } |\alpha \cap \beta| = 1 \\ 0, \text{otherwise} \end{cases}$. Then:

$$Cov(V_\alpha, V_\beta) = C_0(1 + 1_{\alpha=\beta}) - C_1(h_{\alpha,\{1,2\}}) + h_{\beta,\{1,2\}}).$$

$\square$

## Proof Idea (Step 2).

- $h_{\alpha,\beta} = \begin{cases} 1 \text{ if } |\alpha \cap \beta| = 1 \\ 0, \text{otherwise} \end{cases}$ .

$\square$

## Proof Idea (Step 2).

- $h_{\alpha,\beta} = \begin{cases} 1 \text{ if } |\alpha \cap \beta| = 1 \\ 0, \text{otherwise} \end{cases}$.
- The structure of $h$ encodes the adjacency matrix of the line graph of the complete graph on $n$ vertices.

□

## Proof Idea (Step 2).

- $h_{\alpha,\beta} = \begin{cases} 1 \text{ if } |\alpha \cap \beta| = 1 \\ 0, \text{otherwise} \end{cases}$ .
- The structure of $h$ encodes the adjacency matrix of the line graph of the complete graph on $n$ vertices.
- To study it, one can start with the $m \times n$ incidence matrix (edge by vertex) and multiply by its transposed.

$\square$

## Proof Idea (Step 2).

- $h_{\alpha,\beta} = \begin{cases} 1 \text{ if } |\alpha \cap \beta| = 1 \\ 0, \text{otherwise} \end{cases}$ .
- The structure of $h$ encodes the adjacency matrix of the line graph of the complete graph on $n$ vertices.
- To study it, one can start with the $m \times n$ incidence matrix (edge by vertex) and multiply by its transposed.
- This approach reveals useful eigenvectors and eigenvalues, e.g. $m - n$ of the eigenvalues are $0$, $n - 1$ are $n - 2$ and one is $2n - 2$.

$\square$

## Proof Idea (Step 2).

- $h_{\alpha,\beta} = \begin{cases} 1 \text{ if } |\alpha \cap \beta| = 1 \\ 0, \text{otherwise} \end{cases}$ .
- The structure of $h$ encodes the adjacency matrix of the line graph of the complete graph on $n$ vertices.
- To study it, one can start with the $m \times n$ incidence matrix (edge by vertex) and multiply by its transposed.
- This approach reveals useful eigenvectors and eigenvalues, e.g. $m - n$ of the eigenvalues are $0$, $n - 1$ are $n - 2$ and one is $2n - 2$.
- In our case the matrix $Var(V)$ is skewed and represents a $(m - 1)$-projection.

□

## Proof Idea (Step 3).

- $A = \left(\begin{array}{c|c} C_0 & C_0\mathbf{1} \\ \hline \mathbf{0} & Var(V) \end{array}\right).$

$\square$

## Proof Idea (Step 3).

- $A = \left(\begin{array}{c|c} C_0 & C_0 \mathbf{1} \\ \hline \mathbf{0} & Var(V) \end{array}\right)$.
- $\mathcal{B} = \{\mathbf{1}, H_{1,2}, H_2, \ldots, H_n\}$ are linearly independent where:

$$H_i = \sum_{j \neq i} e_{i,j} \text{ and } H_{1,2} = H_1 + H_2 - 2e_{1,2}.$$

$\square$

## Proof Idea (Step 3).

- $A = \left(\begin{array}{c|c} C_0 & C_0\mathbf{1} \\ \hline \mathbf{0} & Var(V) \end{array}\right)$.
- $\mathcal{B} = \{\mathbf{1}, H_{1,2}, H_2, \ldots, H_n\}$ are linearly independent where:

$$H_i = \sum_{j \neq i} e_{i,j} \text{ and } H_{1,2} = H_1 + H_2 - 2e_{1,2}.$$

- For $v \perp \mathcal{B}$, $Av = (C_0 - 2C_1)v$.

$\square$

## Proof Idea (Step 3).

- $A = \left(\begin{array}{c|c} C_0 & C_0\mathbf{1} \\ \hline \mathbf{0} & Var(V) \end{array}\right)$.
- $\mathcal{B} = \{\mathbf{1}, H_{1,2}, H_2, \dots, H_n\}$ are linearly independent where:

$$H_i = \sum_{j \neq i} e_{i,j} \text{ and } H_{1,2} = H_1 + H_2 - 2e_{1,2}.$$

- For $v \perp \mathcal{B}$, $Av = (C_0 - 2C_1)v$.
- $A_{|\mathcal{B}}$ has an almost diagonal form:

$$\begin{pmatrix} C_0 m & C_0(2n-4) & C_0(n-2) - C_1(n-4) & C_0(n-1) & \dots & C_0(n-1) \\ -C_1 m & C_0 - (2n-2)C_1 & -C_1(n-1) & -C_1(n-1) & \dots & -C_(n-1) \\ 0 & 0 & C_0 + C_1(n-4) & 0 & \dots & 0 \\ 0 & -C_1(n-4) & 0 & C_0 + C_1(n-4) & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -C_1(n-4) & 0 & 0 & \dots & C_0 + C_1(n-4) \end{pmatrix}$$

□

# $n$-equidistant points with real coordinates. Model

## Problem

Let $X$ be a random, non-constant, variable taking values on a finite subset of $\mathbb{R}$.
Let $X_1, \ldots, X_n$ be independently drawn $d$-dimensional vectors with coordinates $X_{i,j} \sim$ i.i.d$X$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

# $n$-equidistant points with real coordinates. Model

## Problem

Let $X$ be a random, non-constant, variable taking values on a finite subset of $\mathbb{R}$.
Let $X_1, \ldots, X_n$ be independently drawn $d$-dimensional vectors with coordinates $X_{i,j} \sim$ i.i.d$X$. Denote by $p_n(d)$ the probability that all the line segments $X_iX_j$, $i \neq j$, be of equal length. Find the asymptotic of $p_n(d)$ as $d$ tends to infinity.

## Remark

W.l.o.g. $X$ takes values on $\mathcal{X} = \{x_0 = 0, x_1, \ldots, x_k\}$. Consider:

$$\mathcal{X}_1 = \{2x_ix_j \,|\, 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \,|\, i \leq k\} \cup \mathcal{X}_1$$

and their spans $\mathcal{L} = span_{\mathbb{Q}}(\mathcal{X}_1)$. Note $\mathcal{L} = span_{\mathbb{Q}}(\mathcal{X}_2)$. So if $\ell = dim(\mathcal{L})$ we can identify $\mathcal{L} \simeq \mathbb{Q}^\ell$, fix a referent basis $\mathcal{B}$ for $\mathcal{L}$ and obtain bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for $\mathcal{L}at(\mathcal{X}_1)$ and $\mathcal{L}at(\mathcal{X}_2)$.

# $n$-equidistant points with real coordinates. Hamel and the Lattice

## Remark

Recall $m = \binom{n}{2}$ and $\{e_{i,j} \,|\, 1 \leq i < j \leq n\}$ is a standard basis of $\mathbb{R}^m$.
Further $H(I) = \sum_{i \in I} \sum_{j \notin I} e_{i,j}$, where $[i] = \{1, 2, \ldots, i\}$.

# $n$-equidistant points with real coordinates. Hamel and the Lattice

## Remark

Recall $m = \binom{n}{2}$ and $\{e_{i,j} \mid 1 \le i < j \le n\}$ is a standard basis of $\mathbb{R}^m$. Further $H(I) = \sum_{i \in I} \sum_{j \notin I} e_{i,j}$, where $[i] = \{1, 2, \ldots, i\}$.

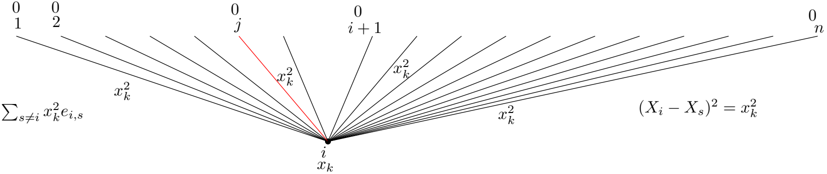
## Lemma

Let $H_X : \mathcal{X}^n \to \mathbb{R}^m$ be the function $H_X(\mathbf{x}) = \sum_{i<j} (x_i - x_j)^2 e_{i,j}$.
Then the vectors:

- $u \otimes H([i])$ for $u \in \mathcal{B}_2$ and $i < n$ together with
- $v \otimes e_{i,j}$ for $v \in \mathcal{B}_1$, $i + 1 < j \le n$

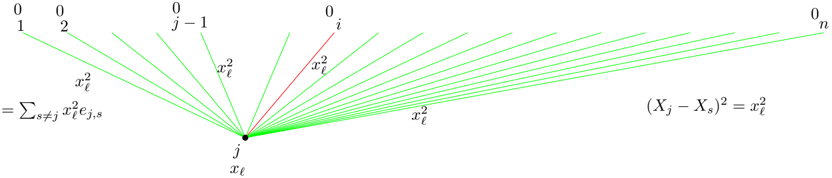
form a basis for $\mathcal{L}at(H_{\mathcal{X}}) := \mathcal{L}at\, Im(H_{\mathcal{X}})$ considered as a lattice on $\mathcal{L} \otimes \mathbb{Q}^m$.

# Hamel and the Lattice



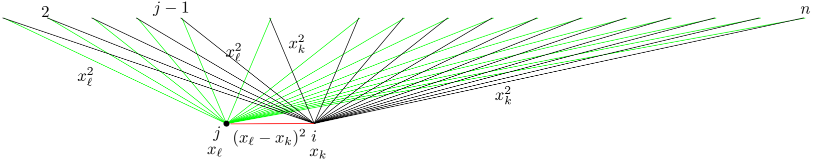

$H_X(\{i\}) = \sum_{s\neq i} x_k^2 e_{i,s}$

$(X_i - X_s)^2 = x_k^2$




$H_X(\{j\}) = \sum_{s\neq j} x_\ell^2 e_{j,s}$

$(X_j - X_s)^2 = x_\ell^2$




$H_X(\{i,j\}) = \sum_{s\neq i,j}(x_k^2 e_{i,s} + x_\ell^2 e_{j,s}) + (x_k - x_\ell)^2 e_{i,j}$

$H_X(\{i\}) + H_X(\{j\}) - H_X(\{i,j\}) = 2x_k x_\ell e_{i,j}$

# Hamel and the Lattice (2)

**Remark**

$$\mathcal{X}_1 = \{2x_i x_j \mid 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \mid i \leq k\} \cup \mathcal{X}_1$$

$\mathcal{B}_1$ and $\mathcal{B}_2$ are bases for $\mathcal{L}at(\mathcal{X}_1)$ and $\mathcal{L}at(\mathcal{X}_2)$.

# Hamel and the Lattice (2)

## Remark

$$\mathcal{X}_1 = \{2x_i x_j \mid 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \mid i \leq k\} \cup \mathcal{X}_1$$

$\mathcal{B}_1$ and $\mathcal{B}_2$ are bases for $\mathcal{L}at(\mathcal{X}_1)$ and $\mathcal{L}at(\mathcal{X}_2)$.

## Lemma

Let $H_X^* : \mathcal{X}^n \to \mathbb{R}^m$ be: $H_X^*(\mathbf{x}) = \sum_{i<j}((x_i - x_j)^2 - (x_n - x_{n-2})^2)e_{i,j}$. Then the vectors:

- $u \otimes H([i])$ for $u \in \mathcal{B}_2$ and $i < n-2$, together with
- $u \otimes (H([n-2]) - \mathbf{1})$ and $u \otimes (H([n-1]) - \mathbf{1})$ for $u \in \mathcal{B}_2$ and
- $v \otimes e_{i,j}$ for $v \in \mathcal{B}_1$, $i+1 < j$ and $i < n-2$

form a basis for $\mathcal{L}at(H_{\mathcal{X}}^*) := \mathcal{L}at\, Im(H_{\mathcal{X}}^*)$ considered as a lattice on $\mathcal{L} \otimes \mathbb{Q}^{m-1}$. Furthermore the fundamental volume of this lattice is:

$$|\mathcal{L}at(H_{\mathcal{X}}^*)| = |det\mathcal{B}_1|^{m-n}|det\mathcal{B}_2|^{n-1} = |\mathcal{L}at(\mathcal{X}_1)|^{m-n}|\mathcal{L}at(\mathcal{X}_2)|^{n-1}.$$

# $n$-equidistant points with real coordinates. General case

**Remark**

Recall $\mathcal{X} = \{x_0 = 0, x_1, \ldots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_i x_j \mid 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \mid i \leq k\} \cup \mathcal{X}_1.$$

### Remark

Recall $\mathcal{X} = \{x_0 = 0, x_1, \ldots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_i x_j \,|\, 1 \le i \le j \le k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \,|\, i \le k\} \cup \mathcal{X}_1.$$

### Remark

Let $X_1, X_2, X_3$ be three independent copies of $X$ taking values on $\mathcal{X}$. Let $Y_1 \simeq (X_1 - X_2)^2$ and $Y_2 \simeq (X_1 - X_3)^2$ considered as $\mathbb{Q}^\ell$-random vectors in $\mathcal{L} = span(\mathcal{X}_1)$. Set $C = Var(Y_1)$ and $C_1 = Cov(Y_1, Y_2)$.

# $n$-equidistant points with real coordinates. General case

## Remark

Recall $\mathcal{X} = \{x_0 = 0, x_1, \ldots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_i x_j \,|\, 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \,|\, i \leq k\} \cup \mathcal{X}_1.$$

## Remark

Let $X_1, X_2, X_3$ be three independent copies of $X$ taking values on $\mathcal{X}$. Let $Y_1 \simeq (X_1 - X_2)^2$ and $Y_2 \simeq (X_1 - X_3)^2$ considered as $\mathbb{Q}^\ell$-random vectors in $\mathcal{L} = span(\mathcal{X}_1)$. Set $C = Var(Y_1)$ and $C_1 = Cov(Y_1, Y_2)$.

## Theorem

$\lim_{d\to\infty} p_n(d).d^{\ell(m-1)/2} = \dfrac{|\mathcal{L}(\mathcal{X}_1)|^{m-n}|\mathcal{L}(\mathcal{X}_2)|^{n-1}}{2^{m-n}\sqrt{m^\ell(2\pi)^{\ell(m-1)}|C|^{m-n}|(4C+(n-2)C_1)|^{n-1}}}.$

# $n$-equidistant points with real coordinates. Galois and the Lattice

## Remark

Recall $\mathcal{X} = \{x_0 = 0, x_1, \dots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_i x_j \mid 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \mid i \leq k\} \cup \mathcal{X}_1.$$

# $n$-equidistant points with real coordinates. Galois and the Lattice

## Remark

Recall $\mathcal{X} = \{x_0 = 0, x_1, \dots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_i x_j \,|\, 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \,|\, i \leq k\} \cup \mathcal{X}_1.$$

## Remark

Let $X_1, X_2, X_3$ be three independent copies of $X$ taking values on $\mathcal{X}$. Let $Y_1 \simeq (X_1 - X_2)^2$ and $Y_2 \simeq (X_1 - X_3)^2$ considered as $\mathbb{Q}^\ell$-random vectors in $\mathcal{L} = span(\mathcal{X}_1)$. Set $C = Var(Y_1)$ and $C_1 = Cov(Y_1, Y_2)$.

# $n$-equidistant points with real coordinates. Galois and the Lattice

**Remark**

Recall $\mathcal{X} = \{x_0 = 0, x_1, \ldots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_i x_j \,|\, 1 \leq i \leq j \leq k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \,|\, i \leq k\} \cup \mathcal{X}_1.$$

**Remark**

Let $X_1, X_2, X_3$ be three independent copies of $X$ taking values on $\mathcal{X}$. Let $Y_1 \simeq (X_1 - X_2)^2$ and $Y_2 \simeq (X_1 - X_3)^2$ considered as $\mathbb{Q}^\ell$-random vectors in $\mathcal{L} = span(\mathcal{X}_1)$. Set $C = Var(Y_1)$ and $C_1 = Cov(Y_1, Y_2)$.

**Lemma**

If $x_i = \sqrt{q_i}$ for $i \leq k$, where $q_i \in \mathbb{Q}^+$, then:

1. $|\mathcal{L}at\mathcal{X}_1| = 2|\mathcal{L}at\mathcal{X}_2|$.
2. $\lim_{d\to\infty} p_n(d).d^{\ell(m-1)/2} = \dfrac{|\mathcal{L}(\mathcal{X}_2)|^{m-1}}{\sqrt{m^\ell (2\pi)^{\ell(m-1)} |C|^{m-n} |(4C+(n-2)C_1)|^{n-1}}}$.

# Galois and the Lattice

**Sketch.**

1. Since the problem is invariant w.r.t. scaling with positive rational numbers, we can assume that $q_i \in \mathbb{N}$.

**Sketch.**

1. Since the problem is invariant w.r.t. scaling with positive rational numbers, we can assume that $q_i \in \mathbb{N}$.
2. If $x_i x_j \in \mathbb{N}$, then $gcd(x_i^2, x_j^2, x_i x_j) = gcd(x_i^2, x_j^2)$, therefore:

$$gcd(\{2x_i^2 \mid i \leq k\} \cup \{2x_i x_j \mid x_i x_j \in \mathbb{N}\}) = 2gcd(\{x_i^2 \mid i \leq k\})$$

□

# Galois and the Lattice

## Sketch.

1. Since the problem is invariant w.r.t. scaling with positive rational numbers, we can assume that $q_i \in \mathbb{N}$.
2. If $x_i x_j \in \mathbb{N}$, then $gcd(x_i^2, x_j^2, x_i x_j) = gcd(x_i^2, x_j^2)$, therefore:

$$gcd(\{2x_i^2 \mid i \leq k\} \cup \{2x_i x_j \mid x_i x_j \in \mathbb{N}\}) = 2gcd(\{x_i^2 \mid i \leq k\})$$

3. To conclude the proof, it suffices to prove that if $t_i$ are distinct square-free natural numbers then:

$$\sum_{i=1}^{k} s_i \sqrt{t_i} \in \mathbb{Q} \iff s_i = 0 \text{ for all } i \leq k.$$

$\square$

1. This follows by a well-known result from Galois Theory. Let $\{p_i | \mid i \leq n\}$ be distinct prime numbers and $p$ be square-free co-prime with every $p_i$. Then $p \notin K_n = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$. In particular $[K_n : \mathbb{Q}] = 2^n$.

$\square$

1. This follows by a well-known result from Galois Theory. Let $\{p_i | \mid i \leq n\}$ be distinct prime numbers and $p$ be square-free co-prime with every $p_i$. Then $p \notin K_n = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$. In particular $[K_n : \mathbb{Q}] = 2^n$.
2. This implies that $\{\sqrt{\prod_{j \in I} p_j} \mid I \subseteq [n]\}$ is a basis of $K_n$ as a linear space over $\mathbb{Q}$.

$\square$

1. This follows by a well-known result from Galois Theory. Let $\{p_i| \mid i \leq n\}$ be distinct prime numbers and $p$ be square-free co-prime with every $p_i$. Then $p \notin K_n = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$. In particular $[K_n : \mathbb{Q}] = 2^n$.
2. This implies that $\{\sqrt{\prod_{j \in I} p_j} \mid I \subseteq [n]\}$ is a basis of $K_n$ as a linear space over $\mathbb{Q}$.
3. If $\{t_i \mid i \leq k\}$ are distinct square-free natural numbers then taking their different prime factors $p_1, \ldots, p_n$, we see that $t_i$ are distinct elements of $\{\prod_{j \subseteq I} p_j \mid I \subseteq [n]\}$ so the claim follows.

$\square$

### Remark

Again Recall $\mathcal{X} = \{x_0 = 0, x_1, \dots, x_k\}$ and

$$\mathcal{X}_1 = \{2x_ix_j \mid 1 \le i \le j \le k\} \text{ and } \mathcal{X}_2 = \{x_i^2 \mid i \le k\} \cup \mathcal{X}_1.$$

Let $x_i^2 \in \mathcal{L}$ correspond to the vector $u_i \in \mathbb{Q}^\ell$ and $2x_ix_j \in \mathcal{L}$ be mapped to $v_{i,j} \in \mathbb{Q}^\ell$.

Then we introduce the matrix $A = \begin{pmatrix} u_1 \\ u_2 \\ \dots \\ u_k \\ v_{1,2} \\ \dots \\ v_{k-1,k} \end{pmatrix} = \left(\frac{U}{V}\right).$

# $n$-equidistant points with real coordinates. Smith's Normal Form and the Lattice (2)

## Remark

W.l.o.g we may and we do assume that $A$ is integer-valued and that one of the entries of $A$ is odd.

# $n$-equidistant points with real coordinates. Smith's Normal Form and the Lattice (2)

## Remark

W.l.o.g we may and we do assume that $A$ is integer-valued and that one of the entries of $A$ is odd.

## Lemma

Assume that $A \pmod 2$ has full rank $\ell$ over $\mathbb{Z}_2$ and $V \pmod 2$ has rank $r$ over $\mathbb{Z}_2$. Then:

1. $|\mathcal{L}at(\mathcal{X}_1)| = 2^{\ell - r}|\mathcal{L}at(\mathcal{X}_2)|$.
2. $|\mathcal{L}at(H^*_{\mathcal{X}})| = 2^{(m-n)(\ell-r)}|\mathcal{L}at(\mathcal{X}_2)|^{m-1}$.
3. $\lim_{d\to\infty} p_n(d).d^{\ell(m-1)/2}$ is equal to:

$$\frac{2^{(m-n)(\ell-r)}|\mathcal{L}(\mathcal{X}_2)|^{m-1}}{2^{m-1}\sqrt{m^\ell(2\pi)^{\ell(m-1)}|C|^{m-n}|(4C+(n-2)C_1)|^{n-1}}}.$$

**Idea.**

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:

# Smith and the Lattice

**Idea.**

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:
2. Consider a matrix $A \in M_{k,\ell}(\mathbb{Z})$.

## Idea.

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:
2. Consider a matrix $A \in M_{k,\ell}(\mathbb{Z})$.
3. Set $A(0) = A$.

# Smith and the Lattice

## Idea.

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:
2. Consider a matrix $A \in M_{k,\ell}(\mathbb{Z})$.
3. Set $A(0) = A$.
4. Given $A(j)$ find the greatest common divisor $g(j)$ of the elements of $A(j)$.

# Smith and the Lattice

## Idea.

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:
2. Consider a matrix $A \in M_{k,\ell}(\mathbb{Z})$.
3. Set $A(0) = A$.
4. Given $A(j)$ find the greatest common divisor $g(j)$ of the elements of $A(j)$.
5. Using elementary operations additions and subtractions of rows/columns reduce $A(j)$ to:

$$A(j) = \begin{pmatrix} g(j) & 0 \\ 0 & A(j+1) \end{pmatrix}.$$

## Idea.

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:
2. Consider a matrix $A \in M_{k,\ell}(\mathbb{Z})$.
3. Set $A(0) = A$.
4. Given $A(j)$ find the greatest common divisor $g(j)$ of the elements of $A(j)$.
5. Using elementary operations additions and subtractions of rows/columns reduce $A(j)$ to:

$$A(j) = \begin{pmatrix} g(j) & 0 \\ 0 & A(j+1) \end{pmatrix}.$$

6. The product of the non-zero $g(j)$ is the desired quantity.

# Smith and the Lattice

## Idea.

1. The Smith's algorithm determines a fundamental volume of a lattice as follows:
2. Consider a matrix $A \in M_{k,\ell}(\mathbb{Z})$.
3. Set $A(0) = A$.
4. Given $A(j)$ find the greatest common divisor $g(j)$ of the elements of $A(j)$.
5. Using elementary operations additions and subtractions of rows/columns reduce $A(j)$ to:

$$A(j) = \begin{pmatrix} g(j) & 0 \\ 0 & A(j+1) \end{pmatrix}.$$

6. The product of the non-zero $g(j)$ is the desired quantity.
7. Comparing how this procedure transforms $\mathcal{X}_1$ and $\mathcal{X}_2$, the result follows.

Revue de la filière mathématiques RMS, 134-2, 2024.
URL https://www.rms-math.com.

Olaf Kraft.
A multidimensional local limit theorem for lattice distributions.
Institute of Statistics Mimeo Series No. 530, North Carolina State University. Dept. of Statistics. 1967.
URL https://repository.lib.ncsu.edu/items/9c2dc08b-ca05-46bf-b7e3-3ecd12e887c0.

Stefan Gerdjikov, Martin Minchev, and Mladen Savov
On the probability of n equidistant points in high-dimensional lattices.
arXiv:2502.03440v1