Geometry of random (-1/+1)-polytopes

A survey of recent results on random $\{-1,1\}$-polytopes in Asymptotic Convex Analysis

Alain Pajor (Marne la Vallée)

Random $\{-1,1\}$-polytopes demonstrate extremal behavior with respect to many geometric characteristics.

Random (-1/+1)-polytopes

A (-1/+1)-polytope is a convex polytope generated by vertices of the discrete cube $\{-1,+1\}^n$. We shall discuss here the centrally symmetric case, that is:

$$K_{n,N} = K_{n,N}(X_1, X_2, \ldots, X_N) = K_{n,N}(\omega)$$

is the symmetric convex hull of vertices $X_1, X_2, \ldots, X_N$ of the cube or the symmetric convex hull of the rows of a ± 1 matrix ω

Random (-1/+1)-polytopes

A (-1/+1)-polytope is a convex polytope generated by vertices of the discrete cube $\{-1,+1\}^n$. We shall discuss here the centrally symmetric case, that is:

$$K_{n,N} = K_{n,N}(X_1, X_2, \ldots, X_N) = K_{n,N}(\omega)$$

is the symmetric convex hull of vertices $X_1, X_2, \ldots, X_N$ of the cube or the symmetric convex hull of the rows of a ± 1 matrix ω

$$\omega = \begin{pmatrix} \omega_{11} & \cdots & \omega_{1n} \\ \omega_{21} & \cdots & \omega_{2n} \\ \omega_{31} & \cdots & \omega_{3n} \\ \vdots & \ddots & \vdots \\ \omega_{N1} & \cdots & \omega_{Nn} \end{pmatrix}$$

Random (-1/+1)-polytopes

A (-1/+1)-polytope is a convex polytope generated by vertices of the discrete cube $\{-1,+1\}^n$. We shall discuss here the centrally symmetric case, that is:

$$K_{n,N} = K_{n,N}(X_1, X_2, \ldots, X_N) = K_{n,N}(\omega)$$

is the symmetric convex hull of vertices $X_1, X_2, \ldots, X_N$ of the cube or the symmetric convex hull of the rows of a ± 1 matrix ω

$$\omega = \begin{pmatrix} \omega_{11} & \cdots & \omega_{1n} \\ \omega_{21} & \cdots & \omega_{2n} \\ \omega_{31} & \cdots & \omega_{3n} \\ \vdots & \ddots & \vdots \\ \omega_{N1} & \cdots & \omega_{Nn} \end{pmatrix}$$

We assume (most of the time) that

$$2n \leq N \leq 2^n$$

Random (-1/+1)-polytopes: definition

A random (-1,+1)-polytope is defined by N i.i.d. vertices of the cube $X_1, X_2, \ldots, X_N$: each vertices is distributed according to the uniform distribution,
or
$K_{n,N} = K_{n,N}(\omega)$ is defined by a random Bernoulli matrix ω.

Random (-1/+1)-polytopes: definition

A random (-1,+1)-polytope is defined by N i.i.d. vertices of the cube $X_1, X_2, \dots, X_N$: each vertices is distributed according to the uniform distribution,
or
$K_{n,N} = K_{n,N}(\omega)$ is defined by a random Bernoulli matrix ω.

Important note: at least one difference between these polytopes and the convex hull of random points on the sphere (or Gaussian vectors, or random points from the cube), this is the existence of big mass in some small slabs.

Random (-1/+1)-polytopes: definition

A random (-1,+1)-polytope is defined by N i.i.d. vertices of the cube $X_1, X_2, \dots, X_N$: each vertices is distributed according to the uniform distribution,
or
$K_{n,N} = K_{n,N}(\omega)$ is defined by a random Bernoulli matrix ω.

Important note: at least one difference between these polytopes and the convex hull of random points on the sphere (or Gaussian vectors, or random points from the cube), this is the existence of big mass in some small slabs.

- More precisely, let $\theta \in \mathbb{R}^n$ be a non zero vector and let X be a random point on the sphere, then,

$$\mathbb{P}(| < \theta, X > | \leq t) = O(t)$$

Random (-1/+1)-polytopes: definition

A random (-1,+1)-polytope is defined by N i.i.d. vertices of the cube $X_1, X_2, \dots, X_N$: each vertices is distributed according to the uniform distribution,
or
$K_{n,N} = K_{n,N}(\omega)$ is defined by a random Bernoulli matrix ω.

Important note: at least one difference between these polytopes and the convex hull of random points on the sphere (or Gaussian vectors, or random points from the cube), this is the existence of big mass in some small slabs.

- More precisely, let $\theta \in \mathbb{R}^n$ be a non zero vector and let X be a random point on the sphere, then,

$$\mathbb{P}(| < \theta, X > | \leq t) = O(t)$$

- This is no more true if X is a random vertex of the cube; for instance, for any $t > 0$,

$$\mathbb{P}(| < (1, 1, 0, \dots, 0), X > | \leq t) \geq 0.5$$

This phenomena which depends on the direction θ, makes a geometric and technical difference in the study of inradius, number of faces, etc...

This phenomena which depends on the direction θ, makes a geometric and technical difference in the study of inradius, number of faces, etc...

- The discrete situation on $\{-1,+1\}^n$ generates a singularity when $N=n$. For the study of volume, inradius,...the case when $N \to n$ or $N=n$ is of different nature and contains many open problems, see Komlós, Kahn-Komlós-Szemerédi, Tao-Vu and the survey of Ziegler.

This phenomena which depends on the direction θ, makes a geometric and technical difference in the study of inradius, number of faces, etc...

Definition:

- We say that a random polytope satisfies a certain property, if the set of ω such that $K_{n,N}(\omega)$ satisfies this property is overwhelming.

This phenomena which depends on the direction θ, makes a geometric and technical difference in the study of inradius, number of faces, etc...

Definition:

- We say that a random polytope satisfies a certain property, if the set of ω such that $K_{n,N}(\omega)$ satisfies this property is overwhelming.

High probability means, with a probability larger than

$$1 - \exp(-f(n,N)) \quad \text{with} \quad f(n,N) \to \infty$$

as $n \to \infty$. The best possible would be $f(n,N) \simeq cN$ (for some $c > 0$), but this is not always possible, sometimes $f(n,N) \simeq cn$, or at least logarithmic.

This phenomena which depends on the direction θ, makes a geometric and technical difference in the study of inradius, number of faces, etc...

Definition:

- We say that a random polytope satisfies a certain property, if the set of ω such that $K_{n,N}(\omega)$ satisfies this property is overwhelming.

High probability means, with a probability larger than

$$1 - \exp(-f(n,N)) \quad \text{with} \quad f(n,N) \to \infty$$

as $n \to \infty$. The best possible would be $f(n,N) \simeq cN$ (for some $c > 0$), but this is not always possible, sometimes $f(n,N) \simeq cn$, or at least logarithmic.

Note: The level of this probability is useful for proving the existence of $K_{n,N}$ satisfying many properties (as we shall see later).

This phenomena which depends on the direction θ, makes a geometric and technical difference in the study of inradius, number of faces, etc...

Definition:

- We say that a random polytope satisfies a certain property, if the set of ω such that $K_{n,N}(\omega)$ satisfies this property is overwhelming.

High probability means, with a probability larger than

$$1 - \exp(-f(n,N)) \quad \text{with} \quad f(n,N) \to \infty$$

as $n \to \infty$. The best possible would be $f(n,N) \simeq cN$ (for some $c > 0$), but this is not always possible, sometimes $f(n,N) \simeq cn$, or at least logarithmic.

Note: $c, c_1, C, \dots$ will denote some universal constants.

I. Estimating the volume (1)

The upper bound (Carl-P., Gluskin, Bárány-Füredi)

$$\mathrm{vol}(K_{n,N})^{1/n} \leq c\sqrt{\ln(2N/n)}\,/\,\sqrt{n}$$

is deterministic (valid for the convex hull of N points on the sphere of radius $\sqrt{n}$).

I. Estimating the volume (1)

The upper bound (Carl-P., Gluskin, Bárány-Füredi)

$$\mathrm{vol}(K_{n,N})^{1/n} \leq c\sqrt{\ln(2N/n)}\,/\,\sqrt{n}$$

is deterministic (valid for the convex hull of N points on the sphere of radius $\sqrt{n}$).

Note that

- The volume of the unit Euclidean ball B_2^n satisfies $\mathrm{vol}(B_2^n)^{1/n} \sim 1/\sqrt{n}$

I. Estimating the volume (1)

The upper bound (Carl-P., Gluskin, Bárány-Füredi)

$$\mathrm{vol}(K_{n,N})^{1/n} \leq c\sqrt{\ln(2N/n)}\,/\,\sqrt{n}$$

is deterministic (valid for the convex hull of N points on the sphere of radius $\sqrt{n}$).

Lower bound, for random polytopes: (Litvak, P., Rudelson, Tomczak)

Theorem [LPRT] *Let* $2n \leq N \leq 2^n$*. For every* $\beta \in (0, 1/2)$ *one has*

$$\mathrm{vol}(K_{n,N})^{1/n} \geq c\sqrt{\beta\ln(2N/n)}\,/\,\sqrt{n}$$

with probability larger than

$$1 - \exp\left(-c' n^{\beta} N^{1-\beta}\right).$$

I. Estimating the volume (1)

The upper bound (Carl-P., Gluskin, Bárány-Füredi)

$$\mathrm{vol}(K_{n,N})^{1/n} \leq c\sqrt{\ln(2N/n)}\,/\,\sqrt{n}$$

is deterministic (valid for the convex hull of N points on the sphere of radius $\sqrt{n}$).

Lower bound, for random polytopes: (Litvak, P., Rudelson, Tomczak)

Theorem [LPRT] *Let $2n \leq N \leq 2^n$. For every $\beta \in (0, 1/2)$ one has*

$$\mathrm{vol}(K_{n,N})^{1/n} \geq c\sqrt{\beta \ln(2N/n)}\,/\,\sqrt{n}$$

with probability larger than

$$1 - \exp\left(-c' n^{\beta} N^{1-\beta}\right).$$

This is optimal and improves a result from Giannopoulos-Hartzoulaki, where $N \geq n \ln n$ and with probability $1 - \exp(-cn)$.

I. Estimating the volume (2)

Theorem [LPRT], [GH] *There exist* c_1, c_2 *such that for every* $\beta \in (0, 1/2)$ *and any* $2n \leq N \leq 2^n$, *one has*

$$K_N \supset c_1 \left(B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \right)$$

with probability larger than

$$1 - \exp\left(-c_2 n^\beta N^{1-\beta}\right) .$$

I. Estimating the volume (2)

Theorem [LPRT], [GH] *There exist* c_1, c_2 *such that for every* $\beta \in (0, 1/2)$ *and any* $2n \leq N \leq 2^n$, *one has*

$$K_N \supset c_1 \left(B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \right)$$

with probability larger than

$$1 - \exp\left(-c_2 n^\beta N^{1-\beta}\right).$$

Observe that

$$B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \supset \sqrt{\frac{\beta \ln(2N/n)}{n}} B_\infty^n$$

I. Estimating the volume (2)

Theorem [LPRT], [GH] *There exist* c_1, c_2 *such that for every* $\beta \in (0, 1/2)$ *and any* $2n \leq N \leq 2^n$, *one has*

$$K_N \supset c_1 \left(B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \right)$$

with probability larger than

$$1 - \exp\left(-c_2 n^\beta N^{1-\beta} \right).$$

Observe that

$$B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \supset \sqrt{\frac{\beta \ln(2N/n)}{n}} B_\infty^n$$

There exists a (-1,1)-polytope with polynomially many vertices containing a cube of size $\sim \sqrt{\ln n/n}$. (Question from a paper of Brieden, Gritzmann, Kannan, Klee, Lovász, Simonovits on computing the inradius for the ℓ_∞ metric)

I. Estimating the volume (2)

Theorem [LPRT], [GH] *There exist* c_1, c_2 *such that for every* $\beta \in (0, 1/2)$ *and any* $2n \leq N \leq 2^n$, *one has*

$$K_N \supset c_1 \left(B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \right)$$

with probability larger than

$$1 - \exp\left(-c_2 n^\beta N^{1-\beta}\right).$$

Observe that

$$B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n \supset \sqrt{\frac{\beta \ln(2N/n)}{n}} B_\infty^n$$

Dyer-Füredi-McDiarmird determined the threshold $N = N(n)$ such that a random polytope contains most of the volume. Let $v_n = \mathbb{E}\mathrm{vol} K_N$ and $\kappa = 2/\sqrt{e}$, then

$v_n \to 0$ if $N(n) \leq (\kappa - \varepsilon)^n$ and $v_n \to 1$ if $N(n) \geq (\kappa + \varepsilon)^n$

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume?

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume? Yes (P.-Rudelson).

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume? Yes (P.-Rudelson).
Let $e_1, \dots, e_p$ and $f_1, \dots, f_q$ be the canonical basis of $\mathbb{R}^p$ and $\mathbb{R}^q$ resp.
Let W be a Hadamard matrix of size $q \times q$ (assuming that q is a power of 2). Set $n = pq$ and define

$$S = \left\{ \sum_1^p \varepsilon_i e_i \bigotimes W f_j \right\}$$

where

$$\varepsilon_i = \pm 1, i = 1, \dots, p, j = 1, \dots, q$$

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume? Yes (P.-Rudelson).
Let $e_1, \ldots, e_p$ and $f_1, \ldots, f_q$ be the canonical basis of $\mathbb{R}^p$ and $\mathbb{R}^q$ resp.
Let W be a Hadamard matrix of size $q \times q$ (assuming that q is a power of 2). Set $n = pq$ and define

$$S = \left\{ \sum_1^p \varepsilon_i e_i \bigotimes W f_j \right\}$$

where

$$\varepsilon_i = \pm 1, i = 1, \ldots, p, j = 1, \ldots, q$$

Then

$$S \subset \{-1, 1\}^n.$$

The symmetric convex hull of S is a (-1,+1)-polytope of $\mathbb{R}^n$ with $N = q2^p$ vertices.

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume? Yes (P.-Rudelson).
Let $e_1, \dots, e_p$ and $f_1, \dots, f_q$ be the canonical basis of $\mathbb{R}^p$ and $\mathbb{R}^q$ resp.
Let W be a Hadamard matrix of size $q \times q$ (assuming that q is a power of 2). Set $n = pq$ and define

$$S = \left\{ \sum_1^p \varepsilon_i e_i \bigotimes W f_j \right\}$$

where

$$\varepsilon_i = \pm 1, i = 1, \dots, p, j = 1, \dots, q$$

Then

$$S \subset \{-1, 1\}^n.$$

The symmetric convex hull of S is a (-1,+1)-polytope of $\mathbb{R}^n$ with $N = q2^p$ vertices.

- One can check that it has maximal volume.

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume? Yes (P.-Rudelson).
Let $e_1, \ldots, e_p$ and $f_1, \ldots, f_q$ be the canonical basis of $\mathbb{R}^p$ and $\mathbb{R}^q$ resp.
Let W be a Hadamard matrix of size $q \times q$ (assuming that q is a power of 2). Set $n = pq$ and define

$$S = \left\{ \sum_1^p \varepsilon_i e_i \bigotimes W f_j \right\}$$

where

$$\varepsilon_i = \pm 1, i = 1, \ldots, p, j = 1, \ldots, q$$

Then

$$S \subset \{-1, 1\}^n.$$

The symmetric convex hull of S is a (-1,+1)-polytope of $\mathbb{R}^n$ with $N = q2^p$ vertices.

- One can check that this explicit polytope do not have super-exponentially many facets.

An explicit example with extremal volume

Question (Bárány): can one construct an explicit (-1,+1)-polytope with almost maximal volume? Yes (P.-Rudelson).
Let $e_1, \dots, e_p$ and $f_1, \dots, f_q$ be the canonical basis of $\mathbb{R}^p$ and $\mathbb{R}^q$ resp.
Let W be a Hadamard matrix of size $q \times q$ (assuming that q is a power of 2). Set $n = pq$ and define

$$S = \left\{ \sum_1^p \varepsilon_i e_i \bigotimes W f_j \right\}$$

where

$$\varepsilon_i = \pm 1, i = 1, \dots, p, j = 1, \dots, q$$

Then

$$S \subset \{-1, 1\}^n.$$

The symmetric convex hull of S is a (-1,+1)-polytope of $\mathbb{R}^n$ with $N = q2^p$ vertices.

Question: can one construct a (-1,+1)-polytope with polynomially many vertices and containing a cube of size $\sqrt{\ln n/n}$?

II. Estimating the inradius

Theorem [LPRT],[GH] *There exist* $c, c' > 0$ *such that for any* $N \geq 2n$ *one has*

$$cB_2^n \subset K_{n,N}$$

with probability larger than $1 - e^{-c'N}$.

II. Estimating the inradius

Theorem [LPRT],[GH] *There exist* $c, c' > 0$ *such that for any* $N \geq 2n$ *one has*

$$cB_2^n \subset K_{n,N}$$

with probability larger than $1 - e^{-c'N}$*.*

More can be said when N is large enough (Mendelson, P., Rudelson):

Let $0 < \varepsilon < 1/2$ *and let* $N \geq c(\varepsilon) n \ln^2 n$ *then*

$$(1 - \varepsilon) B_2^n \subset K_{n,N}$$

with high probability.

II. Estimating the inradius

Theorem [LPRT],[GH] *There exist* $c, c' > 0$ *such that for any* $N \geq 2n$ *one has*

$$cB_2^n \subset K_{n,N}$$

with probability larger than $1 - e^{-c'N}$.

More can be said when N is large enough (Mendelson, P., Rudelson):

Let $0 < \varepsilon < 1/2$ *and let* $N \geq c(\varepsilon) n \ln^2 n$ *then*

$$(1-\varepsilon)B_2^n \subset K_{n,N}$$

with high probability.

Probably $N \geq cn/\varepsilon^2$ should be the right order.

II. Estimating the inradius

Theorem [LPRT],[GH] *There exist* $c, c' > 0$ *such that for any* $N \geq 2n$ *one has*

$$cB_2^n \subset K_{n,N}$$

with probability larger than $1 - e^{-c'N}$*.*

More can be said when N is large enough (Mendelson, P., Rudelson):

Let $0 < \varepsilon < 1/2$ *and let* $N \geq c(\varepsilon) n \ln^2 n$ *then*

$$(1 - \varepsilon) B_2^n \subset K_{n,N}$$

with high probability.

Probably $N \geq cn/\varepsilon^2$ should be the right order.

Estimating the inradius is an opened problem when $N \sim n$.

IV. Estimating metric entropy (1)

Random $(-1, +1)$-polytope have the largest possible Euclidean-metric entropy (among convex sets in $\sqrt{n}B_2^n$, with at most N vertices).

IV. Estimating metric entropy (1)

Definition: A subset of $K_{n,N}$ is ε-separated with respect to the Euclidean metric if the distance between every two distinct points in the subset is larger than ε. We denote the maximal cardinality of an ε-separated subset of $K_{n,N}$ by $D(K_{n,N}, \varepsilon B_2^n)$.

IV. Estimating metric entropy (1)

Definition: A subset of $K_{n,N}$ is ε-separated with respect to the Euclidean metric if the distance between every two distinct points in the subset is larger than ε. We denote the maximal cardinality of an ε-separated subset of $K_{n,N}$ by $D(K_{n,N}, \varepsilon B_2^n)$.

Theorem [MPR]:*There exist absolute constants c_i, $0 \leq i \leq 4$, and κ such that if $N \geq 2n$ and if we set*

$$H(\varepsilon) = c_3 n \begin{cases} \ln\left(\frac{\sqrt{\ln(2N/n)}}{\varepsilon}\right) & \text{if } \varepsilon \leq \kappa\sqrt{\ln(N/n)}, \\ \frac{1}{\varepsilon^2}\ln\left(\frac{c_4 N \varepsilon^2}{n}\right) & \text{if } \kappa\sqrt{\ln(N/n)} \leq \varepsilon \leq \sqrt{n} \end{cases}$$

then with probability at least $1 - \exp(-c_0 n)$, for any $c_1 \exp(\exp(-c_2 n)) \leq \varepsilon \leq \sqrt{n}$,

$$\ln D(K_{n,N}, \varepsilon B_2^n) \geq H(\varepsilon).$$

IV. Estimating metric entropy (1)

Definition: A subset of $K_{n,N}$ is ε-separated with respect to the Euclidean metric if the distance between every two distinct points in the subset is larger than ε. We denote the maximal cardinality of an ε-separated subset of $K_{n,N}$ by $D(K_{n,N}, \varepsilon B_2^n)$.

Theorem [MPR]:*There exist absolute constants* c_i, $0 \leq i \leq 4$, *and* κ *such that if* $N \geq 2n$ *and if we set*

$$H(\varepsilon) = c_3 n \begin{cases} \ln\left(\frac{\sqrt{\ln(2N/n)}}{\varepsilon}\right) & \text{if } \varepsilon \leq \kappa\sqrt{\ln(N/n)}, \\ \frac{1}{\varepsilon^2}\ln\left(\frac{c_4 N \varepsilon^2}{n}\right) & \text{if } \kappa\sqrt{\ln(N/n)} \leq \varepsilon \leq \sqrt{n} \end{cases}$$

then with probability at least $1 - \exp(-c_0 n)$, *for any* $c_1 \exp(\exp(-c_2 n)) \leq \varepsilon \leq \sqrt{n}$,

$$\ln D(K_{n,N}, \varepsilon B_2^n) \geq H(\varepsilon).$$

The reverse inequality is always true [MPR]: $\ln D(K_{n,N}, \varepsilon B_2^n) \lesssim H(\varepsilon)$.

Theorem [MPR]: *There exist absolute constants* c_i, $0 \le i \le 4$, *and* κ *such that if* $N \ge 2n$ *and if we set*

$$H(\varepsilon) = c_3 n \begin{cases} \ln\left(\frac{\sqrt{\ln(2N/n)}}{\varepsilon}\right) & \text{if } \varepsilon \le \kappa\sqrt{\ln(N/n)}, \\ \frac{1}{\varepsilon^2}\ln\left(\frac{c_4 N \varepsilon^2}{n}\right) & \text{if } \kappa\sqrt{\ln(N/n)} \le \varepsilon \le \sqrt{n} \end{cases}$$

then high probability $\ln D(K_{n,N}, \varepsilon B_2^n) \ge H(\varepsilon)$.

Theorem [MPR]: *There exist absolute constants* c_i, $0 \le i \le 4$, *and* κ *such that if* $N \ge 2n$ *and if we set*

$$H(\varepsilon) = c_3 n \begin{cases} \ln\left(\frac{\sqrt{\ln(2N/n)}}{\varepsilon}\right) & \text{if } \varepsilon \le \kappa\sqrt{\ln(N/n)}, \\ \frac{1}{\varepsilon^2}\ln\left(\frac{c_4 N\varepsilon^2}{n}\right) & \text{if } \kappa\sqrt{\ln(N/n)} \le \varepsilon \le \sqrt{n} \end{cases}$$

then high probability $\ln D(K_{n,N}, \varepsilon B_2^n) \ge H(\varepsilon)$.

Proof: The threshold appears at the level $\varepsilon \sim \kappa\sqrt{\ln(N/n)}$.

Below this level, the entropy is of volumic nature. The body $K_{n,N}$ may be essentially flat; Steiner formula may be used to estimate the volume of $K_{n,N} + \varepsilon B_2^n$ and to conclude for the entropy.

Above this level, it is of combinatorial nature;. First compute the metric entropy of the subsets I of $\{1, \dots, N\}$ of a given cardinality m for the Hamming metric. This yields to a family of points $(\sum_{i \in I} X_i/m)$ of $K_{n,N}$ and using concentration inequalities we show that most of them are $\sqrt{n/m}$- separated (m will be defined so that $\varepsilon \sim \sqrt{n/m}$) .

V. Estimating the number of faces (1)

Let $f_{n-1}(K_{n,N})$ be the number of facets of the polytope. Bárány and Pór have shown that this number may be super-exponential:

$$\max_N \mathbb{E} f_{n-1}(K_{n,N}) \geq (cn/\ln n)^{n/4}.$$

V. Estimating the number of faces (1)

Let $f_{n-1}(K_{n,N})$ be the number of facets of the polytope. Bárány and Pór have shown that this number may be super-exponential:

$$\max_N \mathbb{E} f_{n-1}(K_{n,N}) \geq (cn/\ln n)^{n/4}.$$

This was improved recently by Gatzouras, Giannopoulos and Markoulakis to

$$\max_N \mathbb{E} f_{n-1}(K_{n,N}) \geq (cn/\ln n)^{n/2}.$$

probably not far to be optimal.

V. Estimating the number of faces (1)

Let $f_{n-1}(K_{n,N})$ be the number of facets of the polytope. Bárány and Pór have shown that this number may be super-exponential:

$$\max_N \mathbb{E} f_{n-1}(K_{n,N}) \geq (cn/\ln n)^{n/4}.$$

This was improved recently by Gatzouras, Giannopoulos and Markoulakis to

$$\max_N \mathbb{E} f_{n-1}(K_{n,N}) \geq (cn/\ln n)^{n/2}.$$

probably not far to be optimal.
More precisely, they show that there are positive constants a, b such that for $n^a \leq N \leq \exp(bn)$, one has

$$\mathbb{E} f_{n-1}(K_{n,N}) \geq (\ln N/\ln n^a)^{n/2}.$$

V. Estimating the number of faces (2)

For lower dimensional faces, Kaibel has established the following threshold:

$$\mathbb{E} f_k(K_{n,N}) / \binom{n}{k+1} \to 1 \text{ if } N(n) \leq 2^{(\tau_k - \varepsilon)n}$$

$$\mathbb{E} f_k(K_{n,N}) / \binom{n}{k+1} \to 0 \text{ if } N(n) \geq 2^{(\tau_k + \varepsilon)n}$$

V. Estimating the number of faces (2)

For lower dimensional faces, Kaibel has established the following threshold:

$$\mathbb{E} f_k(K_{n,N})/\binom{n}{k+1} \to 1 \text{ if } N(n) \le 2^{(\tau_k-\varepsilon)n}$$

$$\mathbb{E} f_k(K_{n,N})/\binom{n}{k+1} \to 0 \text{ if } N(n) \ge 2^{(\tau_k+\varepsilon)n}$$

Theorem [MPT=Mendelson-P.-Tomczak]: *There exists $C > 0$ such that for any $2n \le N \le 2^n$, the following holds: a random $\{-1,+1\}$-polytope $K_{n,N}$ is m-neighbourly (it has the maximum possible number of m-dimensional faces) for all dimension m such that $m \le Cn/\ln(N/n)$.*

V. Estimating the number of faces (2)

For lower dimensional faces, Kaibel has established the following threshold:

$$\mathbb{E}f_k(K_{n,N})/\binom{n}{k+1} \to 1 \text{ if } N(n) \le 2^{(\tau_k-\varepsilon)n}$$

$$\mathbb{E}f_k(K_{n,N})/\binom{n}{k+1} \to 0 \text{ if } N(n) \ge 2^{(\tau_k+\varepsilon)n}$$

Theorem [MPT=Mendelson-P.-Tomczak]: *There exists $C > 0$ such that for any $2n \le N \le 2^n$, the following holds: a random $\{-1,+1\}$-polytope $K_{n,N}$ is m-neighbourly (it has the maximum possible number of m-dimensional faces) for all dimension m such that $m \le Cn/\ln(N/n)$.*

The existence of such polytopes generated by Gaussian vectors probably goes back to Donoho and Candes-Tao, the best estimate was given recently by Rudelson and Vershynin (in the Gaussian case).

V. Estimating the number of faces (2)

For lower dimensional faces, Kaibel has established the following threshold:

$$\mathbb{E} f_k(K_{n,N}) / \binom{n}{k+1} \to 1 \text{ if } N(n) \leq 2^{(\tau_k - \varepsilon)n}$$

$$\mathbb{E} f_k(K_{n,N}) / \binom{n}{k+1} \to 0 \text{ if } N(n) \geq 2^{(\tau_k + \varepsilon)n}$$

Theorem [MPT=Mendelson-P.-Tomczak]: *There exists $C > 0$ such that for any $2n \leq N \leq 2^n$, the following holds: a random $\{-1, +1\}$-polytope $K_{n,N}$ is m-neighbourly (it has the maximum possible number of m-dimensional faces) for all dimension m such that $m \leq Cn/\ln(N/n)$.*

The existence of such polytopes generated by Gaussian vectors probably goes back to Donoho and Candes-Tao, the best estimate was given recently by Rudelson and Vershynin (in the Gaussian case).

Our approach is based on a recent work on random matrices and on a result of Candes and Tao in error correcting code theory.

We first show that the matrix ω satisfies a restricted orthonormality property, when restricted to sparse vectors.

V. Estimating the number of faces (3)

Let $\Gamma = {}^T\omega$ and for $m \leq n$ let $U_m = \cup B_2^I$ where $|I| \leq m$, be the set of sparse vectors of the Euclidean unit ball of $\mathbb{R}^N$ with support not larger than m.

Theorem [MPT]: *There exists* $c > 0$ *such that for any* $0 < \varepsilon < 1$ *and any* $m \leq n \leq N$ *satisfying*

$$m \ln(N/m) \leq cn\varepsilon^2$$

the following holds with high probability : for every $x \in U_m$ *one has*

$$(1 - \varepsilon)|x| \leq |\Gamma x|/\sqrt{n} \leq (1 + \varepsilon)|x|.$$

Define δ_m to be the smallest number such that for every $x \in U_m$ one has

$$(1 - \delta_m)|x| \leq |\Gamma x|/\sqrt{n} \leq (1 + \delta_m)|x|.$$

Candes and Tao have shown that if $\delta_m + \delta_{2m} + \delta_{3m} < 1$ then for any sparse vector c supported by a set of cardinality less than m, c is the unique minimizer to the following Basis Pursuit program

$$\min \|d\|_{\ell_1} \quad \Gamma d = \Gamma c.$$

V. Estimating the number of faces (4)

Geometry of faces: The optimization problem

$$\min \|d\|_{\ell_1} \quad \Gamma d = \Gamma c.$$

can be cast as a linear programming problem. One can check that unicity of a solution (for any point c of U_m) is equivalent by duality to say that $K_{n,N}$ is m-neighbourly.

V. Estimating the number of faces (4)

Geometry of faces: The optimization problem

$$\min \|d\|_{\ell_1} \quad \Gamma d = \Gamma c.$$

can be cast as a linear programming problem. One can check that unicity of a solution (for any point c of U_m) is equivalent by duality to say that $K_{n,N}$ is m-neighbourly.

The result of Candes and Tao is of deterministic nature, it gives for a given matrix, conditions for an exact reconstruction of a sparse vector.

V. Estimating the number of faces (4)

Geometry of faces: The optimization problem

$$\min \|d\|_{\ell_1} \quad \Gamma d = \Gamma c.$$

can be cast as a linear programming problem. One can check that unicity of a solution (for any point c of U_m) is equivalent by duality to say that $K_{n,N}$ is m-neighbourly.

The result of Candes and Tao is of deterministic nature, it gives for a given matrix, conditions for an exact reconstruction of a sparse vector.

The result of MPT gives a range of the parameters for a Bernoulli matrix to satisfy this CT property.

V. Estimating the number of faces (5)

Inspired by the paper from Candes and Tao, MPT analyse the following random model: let ω be the matrix obtained by choosing n times, independently, a row from an N by N Hadamard matrix, uniformly on $1, \dots N$ (so it is not a selector process).

V. Estimating the number of faces (5)

Theorem [MPT]: *There exists* $c > 0$ *such that for any* $2n \leq N \leq 2^n$*, the following holds: a random polytope* $K_{n,N}$ *as above is* m*-neighbourly, for* $m \leq Cn/\ln^2(N)$*.*

V. Estimating the number of faces (5)

Theorem [MPT]: *There exists* $c > 0$ *such that for any* $2n \leq N \leq 2^n$*, the following holds: a random polytope* $K_{n,N}$ *as above is* m*-neighbourly, for* $m \leq Cn/\ln^2(N)$*.*

This model has the following property:

Let A be the matrix obtained as complement of ω in the Hadamard matrix. Then A is a $N \times (N-n)$ ± 1 matrix satisfying

$$\Gamma A = 0$$

V. Estimating the number of faces (5)

Theorem [MPT]: *There exists* $c > 0$ *such that for any* $2n \leq N \leq 2^n$*, the following holds: a random polytope* $K_{n,N}$ *as above is* m*-neighbourly, for* $m \leq Cn/\ln^2(N)$*.*

This model has the following property:

Let A be the matrix obtained as complement of ω in the Hadamard matrix. Then A is a $N \times (N-n)$ ± 1 matrix satisfying

$$\Gamma A = 0$$

This ± 1 matrix is a $(N-n, N, m)$-error correcting code. If $x \in \mathbb{R}^{N-n}$ is an unknown vector and we are given a vector $y' \in \mathbb{R}^N$ that differs from the encoded vector $y = Ax$ on at most m coordinates then x can be exactly reconstructed from the minimization problem

$$\min \|y' - Az\|_{\ell_1} \quad z \in R^{N-n}.$$

We assume here that $m \leq Cn/\ln^2(N)$.

III. Estimating the VC dimension

Definition: The VC (Vapnik-Cervonenkis) dimension of $K_{n,N}$, denoted by $\mathrm{VC}(K_{n,N})$, is the largest k such that there exists a k dimensional coordinate projection of $K_{n,N}$ containing a cube of size 2ε.

III. Estimating the VC dimension

Definition: The VC (Vapnik-Cervonenkis) dimension of $K_{n,N}$, denoted by $\mathrm{VC}(K_{n,N})$, is the largest k such that there exists a k dimensional coordinate projection of $K_{n,N}$ containing a cube of size 2ε.

Deterministic upper bound (Mendelson-Vershynin):

$$\mathrm{VC}(K_{n,N}, \varepsilon) \lesssim \min\left(\frac{\ln(N\varepsilon^2)}{\varepsilon^2}, n\right).$$

III. Estimating the VC dimension

Definition: The VC (Vapnik-Cervonenkis) dimension of $K_{n,N}$, denoted by $\mathrm{VC}(K_{n,N})$, is the largest k such that there exists a k dimensional coordinate projection of $K_{n,N}$ containing a cube of size 2ε.

Deterministic upper bound (Mendelson-Vershynin):

$$\mathrm{VC}(K_{n,N}, \varepsilon) \lesssim \min\left(\frac{\ln(N\varepsilon^2)}{\varepsilon^2}, n\right).$$

Theorem [MPR] *With high probability, one has*

$$\forall \varepsilon \in (0,1) \quad \mathrm{VC}(K_{n,N}, \varepsilon) \simeq \min\left(\frac{\ln(N\varepsilon^2)}{\varepsilon^2}, n\right).$$

III. Estimating the VC dimension

Definition: The VC (Vapnik-Cervonenkis) dimension of $K_{n,N}$, denoted by $\mathrm{VC}(K_{n,N})$, is the largest k such that there exists a k dimensional coordinate projection of $K_{n,N}$ containing a cube of size 2ε.

Deterministic upper bound (Mendelson-Vershynin):

$$\mathrm{VC}(K_{n,N},\varepsilon) \lesssim \min\left(\frac{\ln(N\varepsilon^2)}{\varepsilon^2}, n\right).$$

Theorem [MPR] *With high probability, one has*

$$\forall\varepsilon \in (0,1) \quad \mathrm{VC}(K_{n,N},\varepsilon) \simeq \min\left(\frac{\ln(N\varepsilon^2)}{\varepsilon^2}, n\right).$$

Therefore, there exists N ±1-vectors of $\mathbb{R}^n$, such that the VC dimension of the convex hull at every scale ε is the worst possible. This is possible because of the high level of concentration.