Notes for High-Dimensional Probability Second Edition by Roman Vershynin

Gallant Tsao

July 8, 2025

Contents

4 Random Matrices

This chapter mostly focuses on the theory regarding random matrices - nets, covering and packing numbers. Applications include community detection, covariance estimation, and spectral clustering.

4.1 A Quick Refresher on Linear Algebra

4.1.1 Singular Value Decomposition

Theorem 4.1.1 (SVD)**.** Any $m \times n$ matrix A with real entries can be written as

$$A = \sum_{i=1}^{r} \sigma_i u_i v_i^T \text{ where } r = \min(m, n).$$

Here $\sigma_i > 0$ are the singular values of A, $u_I \in \mathbb{R}^m$ are orthonormal vectors called the left singular vectors of A, and $v_i \in \mathbb{R}^n$ are orthonormal vectors called the right singular vectors of A.

Proof. WLOG, we can assume that $m \geq n$ or else we can just take the transpose. Since $A^T A \in \mathbb{R}^{n \times n}$ is a symmetric positive semidefinite matrix, the spectral theorem tells us that its eigenvalues are $\sigma_1^2, \ldots, \sigma_n^2$ and corresponding orthonormal eigenvectors $v_1, \ldots, v_n \in \mathbb{R}^n$, so that $A^T A v_i = \sigma_i^2 v_i$. The vectors Av_i are orthogonal:

$$\langle Av_i, Av_j \rangle = \langle A^T A v_i, v_j \rangle = \sigma_i^2 \langle v_i, v_j \rangle = \sigma_i^2 \delta ij.$$

Therefore, there exist orthonormal vectors $u_1, \ldots, u_n \in \mathbb{R}^n$ such that

$$Av_i = \sigma_i u_i, \quad i = 1, \ldots, n.$$

For the above, for all i with $\sigma_i \neq 0$, the vectors u_i are uniquely defined and ensures that they are orthonormal. If $\sigma_i = 0$, then $Av_i = 0$ holds triviall. In this case, we can pick any u_i while keeping orthonormality.
Since $v_1, \ldots, v_n$ form an orthonormal basis of $\mathbb{R}^n$, we can write $I_n = \sum_{i=1}^n v_i v_i^T$. Multiplying by A on the left and plugging the equation above gives

$$A = \sum_{i=1}^{n} (Av_i) v_i^T = \sum_{i=1}^{n} \sigma_i u_i v_i^T.$$

□

Remark 4.1.2 (Geometric interpretation)**.** SVD gives a geometric view of matrices: it stretches the orthogonal direction of v_i by σ_i, then rotates the space, mapping the orthonormal basis v_i to u_i.

Remark 4.1.3 (SVD matrix form)**.** We can set $\sigma_i = 0$ for $i > r$ and arrange them in weakly decreasing order. Then by extending $\{u_i\}$ and $\{v_i\}$ to orthonormal bases in $\mathbb{R}^m$ and $\mathbb{R}^n$, we get

$$A = U \Sigma V^T$$

where U is the $m \times m$ matrix with left singular vectors u_i as columns, V is the $n \times n$ orthogonal matrix with right singular vectors v_i as columns, and Σ is the $m \times n$ diagonal matrix with the singular values σ_i on the diagonal. If A is symmetric, we get the spectral decomposition instead:

$$A = U \Lambda U^T.$$

Remark 4.1.4 (Spectral decomposition v.s. SVD)**.** The spectral and singular value decompositions are tightly connected. Since

$$AA^T = \sum_{i=1}^{r} \sigma_i^2 u_i u_i^T \text{ and } A^T A = \sum_{i=1}^{r} \sigma_i^2 v_i v_i^T$$

the left singular vectors u_i of A are the eigenvectors of AA^T, while the right singular vectors v_i of A are the eigenvectors of $A^T A$, and the singular values σ_i of A are

$$\sigma_i(A) = \sqrt{\lambda_i(AA^T)} = \sqrt{\lambda_i(A^T A)}.$$

Remark 4.1.5 (Orthogonal projection)**.** Consider the orthogonal projection P in $\mathbb{R}^n$ onto a k-dimensional subspace E. The projection of a vector x onto E is given by $Px = \sum_{i=1}^{k} \langle u_i, x \rangle u_i$ where $u_1, \dots, u_k$ is an orthonormal basis of E. We can rewrite this as

$$P = \sum_{i=1}^{k} u_i u_i^T = UU^T$$

where U is the $n \times k$ matrix with orthonormal columns u_i. In particular, P is a symmetric matrix with eigenvalues $\underbrace{1, \dots, 1}_{k}, \underbrace{0, \dots, 0}_{n-k}$.

4.1.2 Min-max Theorem

There is another optimization-based description of eigenvalues:

Theorem 4.1.6 (Min-max theorem for eigenvalues)**.** The k-th largest eigenvalue of an $n \times n$ symmetric matrix A can be written as

$$\lambda_k(A) = \max_{\dim E = k} \min_{x \in S(E)} x^T A x = \min_{\dim E = n-k+1} \max_{x \in S(E)} x^T A x,$$

where the first max/min is taking with respect to all subspaces of a fixed dimension, and $S(E)$ denotes the Euclidean unit sphere of E, i.e. the set of all unit vectors in E.

Proof. Let us focus on the first equation. To prove the upper bound on λ_k, we need to find a k-dimensional subspace E such that

$$x^T A x \geq \lambda_k \text{ for all } x \in S(E).$$

To find the set E, take the spectral decomposition $A = \sum_{i=1}^{n} \lambda_i u_i u_i^T$ and pick the subspace $E = \operatorname{span}(u_1, \dots, u_k)$. The eigenvectors form an orthonormal basis of E, so any vector $x \in S(E)$ can be written as $x = \sum_{i=1}^{k} a_i u_i$. Then by orthonormality of u_i and monotonicity of λ_i, we get

$$x^T A x = \sum_{i=1}^{k} \lambda_i a_i^2 \leq \lambda_k \sum_{i=1}^{k} a_i^2 = \lambda_k$$

and we have the upper bound. For the lower bound on λ_k, we need to find $x \in S(E)$ such that $x^T A x \leq \lambda_k$. Here we let the subspace be $F = \operatorname{span}(u_k, \dots, u_n)$.
Since $\dim E + \dim F = n + 1$, the intersection of E and F is nontrivial hence there is a unit vector $x \in E \cap F$. Writing $x = \sum_{i=k}^{n} a_i u_i$, we get

$$x^T A x = \sum_{i=k}^{n} \lambda_i a_i^2 \geq \lambda_k \sum_{i=k}^{n} a_i^2 = \lambda_k.$$

Then we get the lower bound, and hence the first equality is done.
The second equality is by applying the same technique to $-A$ and reversing the eigenvalues. $\square$

Applying section 4.1.2 to $A^T A$ and using remark 4.1.4, we get

Corollary 4.1.7 (Min-max theorem for singular values)**.** Let $A \in \mathbb{R}^{m\times n}$ with singular values $\sigma_1 \geq \cdots \geq \sigma_n \geq 0$. Then

$$\sigma_k(A) = \max_{\dim E = k} \min_{x\in S(E)} \|Ax\|_2 = \min_{\dim E = n-k+1} \max_{x\in S(E)} \|Ax\|_2$$

with the same notation as section 4.1.2.

4.1.3 Frobenius and Operator Norms

Definition 4.1.8. For a matrix $A \in \mathbb{R}^{m\times n}$, the Frobenius norm is

$$\|A\|_F := \left(\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}^2 \right)^{1/2}.$$

The operator norm of A is the smallest number K such that

$$\|Ax\|_2 \leq K\|x\|_2 \text{ for all } x \in \mathbb{R}^n.$$

Equivalently,

$$\|A\| = \max_{x\neq 0} \frac{\|Ax\|_2}{\|x\|_2} = \max_{\|x\|_2\leq 1} \|Ax\|_2 = \max_{\|x\|_2=1} \|Ax\|_2 = \max_{\|x\|_2=\|y\|_2=1} |y^T Ax|.$$

From the Frobenius norm, we can get that

$$\langle A, B\rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}B_{ij} = \mathrm{tr}(A^T B).$$

Also, from above we can get

$$\|A\|_F^2 = \langle A, A\rangle = \mathrm{tr}(A^T A).$$

For the operator norm, the first three equations follows by rescaling, and the last one comes from the duality formula:

$$\|Ax\| = \max_{\|y\|_2=1} \langle Ax, y\rangle .$$

Here the absolute sign does not matter.

Remark 4.1.9 (Other operator norms)**.** We can replace the ℓ^2 norm in definition 4.1.8 with other norms to get a more general concept of operator norms (Exercise 4.18-4.22).

4.1.4 The Matrix Norms and the Spectrum

Lemma 4.1.10 (Orthogonal invariance)**.** The Frobenius and spectral norms are orthogonal invariant, meaning that for any A and orthogonal matrices Q, R with proper dimensions, we have

$$\|QAR\|_F = \|A\|_F \text{ and } \|QAR\| = \|A\|.$$

Proof. For the Frobenius norm, by one of the formulas above,

$$\begin{aligned} \|QAR\|_F &= \mathrm{tr}(R^T ATQ^T QAR) \\ &= \mathrm{tr}(R^T A^T AR) \\ &= \mathrm{tr}(RR^T A^T A) \\ &= \mathrm{tr}(A^T A) \\ &= \|A\|_F^2. \end{aligned}$$

For the spectral norm, by an equivalent characterization, $\|QAR\|$ is obtained by maximizing the bilinear form $y^T QARx = (Qy)^T A(Rx)$ over all unit vectors x, y. Since Q, R are orthogonal, Qy and Rx also range over all unit vectors, so we just get $\|A\|$ as a result. □

Lemma 4.1.11 (Matrix norms via singular values)**.** For any $A \in \mathbb{R}^{m\times n}$ with singular values $\sigma_1 \geq \cdots \geq \sigma_n$,

$$\|A\|_F = \left(\sum_{i=1}^{n} \sigma_i^2\right)^{1/2} \quad \text{and } \|A\| = \sigma_1.$$

Proof. For the Frobenius norm, by orthogonal invariance (lemma 4.1.10),

$$\|A\|_F = \|U\Sigma V^T\|_F = \|\Sigma\|_F$$

which directly gives us the result.
The result for the operator norm directly follows from corollary 4.1.7 with $k = 1$. □

Remark 4.1.12 (Symmetric matrices)**.** For a symmetric matrix A with eigenvalues λ_k,

$$\|A\| = \max_k |\lambda_k| = \max_{\|x\|=1} |x^T Ax|.$$

The first equality becomes lemma 4.1.11 since the singular values of A are $|\lambda_k|$. The min-max theorem (section 4.1.2) gives $|\lambda_k| \leq \max_{\|x\|=1} |x^T Ax|$, proving the upper bound in the equation above. The lower bound can be proven by taking $x - y$ in the definition of the operator norm (definition 4.1.8).

4.1.5 Low-rank Approximation

For a given matrix A, what is the closest approximation to it for a given matrix of rank k? The answer is just truncating the SVD of A:

Theorem 4.1.13 (Eckart-Young-Mirski theorem)**.** Let $A = \sum_{i=1}^{n} \sigma_i u_i v_i^T$. Then for any $1 \leq k \leq n$,

$$\min_{\text{rank}(B)=k} \|A - B\| = \sigma_{k+1}.$$

The minimum is attained at $B = \sum_{i=1}^{k} \sigma_i u_i v_i^T$.

Proof. If $B \in \mathbb{R}^{m\times n}$ has rank k, $\dim \ker(B) = n - k$. Then the min-max theorem (corollary 4.1.7) for $k + 1$ instead of k gives

$$\|A - b\| \geq \max_{x\in S(E)} \|(A - B)x\|_2 = \max_{x\in S(E)} \|Ax\|_2 \geq \sigma_{k+1}.$$

In the opposite direction, setting $B = \sum_{i=1}^{k} \sigma_i u_i v_i^T$ gives $A - b = \sum_{i=k+1}^{n} \sigma_i u_I v_i^T$. The maximal singular value of this matrix σ_{k+1}, which is the same as its operator norm by lemma 4.1.11. □

4.1.6 Perturbation Theory

We can also study how eigenvalues/eigenvectors change under matrix perturbations:

Lemma 4.1.14 (Weyl inequality)**.** The k-th largest eigenvalue of symmetric matrices A, B satisfy

$$|\lambda_k(A) - \lambda_k(B)| \leq \|A - B\|.$$

Similarly, the k-th largest singular values of general rectangular matrices satisfy

$$|\sigma_k(A) - \sigma_k(B)| \leq \|A - B\|.$$

A similar result holds for eigenvectors, however we have to track the same eigenvector before and after the perturbation. If the eigenvalues are too close, a small perturbation can swap them, leading to huge error since their eigenvectors are orthogonal and far apart.

Theorem 4.1.15 (Davis-Kahan inequality)**.** Consider two symmetric matrices A, B with spectral decompositions

$$A = \sum_{i=1}^{n} \lambda_i u_i u_i^T, \ B = \sum_{i=1}^{n} \mu_i v_i v_i^T,$$

where the eigenvalues are weakly decreasing. Assume the the k-th largest eigenvalue of A is δ-seperated from the rest:

$$\min_{i \neq k} |\lambda_k - \lambda_i| = \delta > 0.$$

Then the angle between the eigenvectors u_k and v_k satisfies

$$\sin \angle u_k, v_k \leq \frac{2\|A - B\|}{\delta}.$$

The theorem above can be derived via a stronger result of Davis-Kahan focusing on spectral projections - the orthogonal projections onto the span of some subset of eigenvectors:

Lemma 4.1.16 (Davis-Kahan inequality for spectral projections)**.** Consider A, B as in theorem 4.1.15. Let I, J be two δ-seperated subsets of $\mathbb{R}$, with I being an interval. Then the spectral projections

$$P = \sum_{i:\lambda_i \in I} u_i u_i^T \text{ and } Q = \sum_{j:\lambda_j \in J} v_j v_j^T \text{ satisfy } \|QP\| \leq \frac{\|A - B\|}{\delta}.$$

Proof. WLOG, assume I is finite and closed. Adding the same multiple of Identity to A and B, we can center I as $[-r, r]$, so that $|\lambda_i| \leq r$ for $i \in I$ and $|\mu_j| \geq r + \delta$ for $\mu_j \in J$. The idea is to see how P and Q interact through $H := B - A$:

$$\|H\| \geq \|QHP\| = \|QBP - QAP\| \geq \|QBP\| - \|QAP\|.$$

The spectral projection A commutes with B, hence

$$\|QBP\| \geq \|BQP\| \geq (r + \delta)\|QP\|.$$

To see the last inequality, the image of Q is spanned by orthogonal vectors v_j with $|\mu_j| \geq r + \delta$. The matrix B maps each such vector v_j to $\mu_j v_j$, hence scaling it by at least $r + \delta$. Thus B expands the norm of any vector in the image of Q by at least $r + \delta$ so

$$\|BQPx\|_2 \geq (r + \delta)\|QPx\|_2 \text{ for any } x.$$

Taking the supremum over all unit vectors gives the result with the operator norm.
Also, $AP = PAP = \sum_{i:\lambda_i \in I} \lambda_i u_i u_i^T$ so

$$\|QAP\| = \|QPAP\| \leq \|QP\| \cdot \|AP\| \leq r\|AP\|,$$

because $\|AP\| = \max_{i:\lambda_i \in I} |\lambda_i| \leq r$. Putting the two bounds together we get

$$\|H\| = \|B - A\| \geq \delta\|QP\|,$$

which completes the proof. □

Proof for theorem 4.1.15. Since the LHS is a trig angle, we can assume that $\varepsilon := \|A - B\| \leq \delta/2$ or else the inequality holds trivially. By Weyl inequality (lemma 4.1.14), $|\lambda_j - \mu_j| \leq \varepsilon$ for each j hence

$$\min_{j:j \neq k} |\lambda_k - \mu_k| \geq \min_{j:j \neq k} |\lambda_k - \lambda_j| - \varepsilon = \delta - \varepsilon \geq \delta/2.$$

Apply lemma 4.1.16 for the $\delta/2$-seperated subsets $I = \{\lambda_k\}$ and $J = \{\mu_j : j \neq k\}$ to get $\|QP\| \leq 2\varepsilon/\delta$. Since P and $I_n - Q$ are the orthogonal projections on the directions of u_k and v_k respectively,

$$\|QP\| = \max_{\|x\|=1} \|QPx\|_2 = \|Qu_k\|_2 = \sin \angle(u_k, v_k).$$

Combining this with the inequality on $\|QP\|$ above completes the proof. □

4.1.7 Isometries

The singular values of a matrix A satisfy (by the min-max theorem)

$$\sigma_n \|x - y\|_2 \leq \|Ax - Ay\|_2 \leq \sigma_1 \|x - y\|_2.$$

The extreme singular values set the limits on how the linear map A distorts space.
A matris is an isometry if

$$\|Ax\|_2 = \|x\|_2 \text{ for all } x \in \mathbb{R}^n.$$

Notice that A need not be a square matrix. T
For $A \in \mathbb{R}^{m \times n}$ with $m \geq n$, the following are equivalent:

(a) The columns of A are orthonormal, i.e. $A^T A = I_n$,

(b) A is an isometry,

(c) All singular values of A are 1.

There is a stronger result where the properties hold approximately instead of exactly (useful when dealing with random matrices):

Lemma 4.1.17 (Approximate isometries)**.** Let $A \in \mathbb{R}^{m \times n}$ with $m \geq n$ and let $\varepsilon \geq 0$. The following are equivalent:

(a) $\|A^T A - I_n\| \leq \varepsilon$.

(b) $(1 - \varepsilon)\|x\|_2^2 \leq \|Ax\|_2^2 \leq (1 + \varepsilon)\|x\|_2^2$ for any $x \in \mathbb{R}^n$.

(c) $1 - \varepsilon \leq \sigma_n^2 \leq \sigma_1^2 \leq 1 + \varepsilon$.

Proof. (a) $\Leftrightarrow$ (b) By rescaling, we can assume that $\|x\|_2 = 1$ in (b). Then we have

$$\|A^T A - I_n\| = \max_{\|x\|_2 = 1} |x^T (A^T A - I_n) x| = \max_{\|x\|_2 = 1} |\|Ax\|_2^2 - 1|,$$

The above being bounded by ε is equivalent to (b) for all unit vectors x.
(b) $\Leftrightarrow$ (c) follows from the relationship for singular values distorting space from above. $\square$

Remark 4.1.18. Here is a more handy version of (a) $\Rightarrow$ (c) in lemma 4.1.17. For $z \in \mathbb{R}$ and $\delta \geq 0$,

$$|z^2 - 1| \leq \max(\delta, \delta^2) \implies |z - 1| \leq \delta.$$

Then substituting $\varepsilon = \max(\delta, \delta^2)$, we get

$$\|A^T A - I_n\| \leq \max(\delta, \delta^2) \implies 1 - \delta \leq \sigma_n \leq \sigma_1 \leq 1 + \delta.$$

4.2 Nets, Covering, and Packing

The ε-net argument is useful for analysis of random matrices. It is also connected to ideas like covering, packing, entropy, volume, and coding.

Definition 4.2.1. Let (T, d) be a metric space. Consider $K \subset T$ and $\varepsilon > 0$. A subset $\mathcal{N} \subset T$ is called an ε-net of K is every point in K is within distance ε of some point in $\mathcal{N}$, i.e.

$$\forall x \in K \exists x_0 \in \mathcal{N} : \ d(x, x_0) \leq \varepsilon.$$

Equivalently, $\mathcal{N}$ is an ε-net of K if the balls of radius ε centered at points in $\mathcal{N}$ cover K, like in the figure below:

(a) This covering of a polygon K by six ε-balls shows that $\mathcal{N}(K, \varepsilon) \leq 6$.

(b) $\mathcal{P}(K, \varepsilon) \geq 6$ means that there exist six ε-separated points in K; the $\varepsilon/2$-balls centered at these points are disjoint.

Figure 4.1 Covering and packing

Definition 4.2.2. The smallest cardinality of an ε-net of K is called the covering number of K, and is denoted $\mathcal{N}(K, d, \varepsilon)$.

Remark 4.2.3 (Compactness)**.** An important result in real analysis says that a subset K of a complete metric space (T, d) is precompact (i.e. the closure of K is compact) if and only if

$$N(K, d, \varepsilon) < \infty \text{ for every } \varepsilon > 0.$$

We can think about the covering numbers as a quantitative measure of how compact K is.

Definition 4.2.4. A subset $\mathcal{N}$ of a metric space (T, d) is ε-seperated if

$$d(x, y) > \varepsilon \text{ for any distinct points } x, y \in \mathcal{N}.$$

The largest possible cardinality of an ε-seperated subset of a given $K \subset T$ is called the packing number of K and is denoted $\mathcal{P}(K, d, \varepsilon)$.

Remark 4.2.5 (Packing balls into K)**.** If $\mathcal{N}$ is ε-seperated, the closed $\varepsilon/2$-balls centered at points in $\mathcal{N}$ are disjoint by the triangle inequality, hence we can always pack into K at least $\mathcal{P}(K, d, \varepsilon)$ disjoint $\varepsilon/2$-balls.

Lemma 4.2.6 (Nets from seperated sets)**.** Let $\mathcal{N}$ be a maximal ε-seperated subset of K, i.e. adding any new point to $\mathcal{N}$ destroys the seperation property. Then $\mathcal{N}$ is an ε-net of K.

Proof. Let $x \in K$. We want to show that there exists $x_0 \in \mathcal{N}$ such that $d(x, x_0) \leq \varepsilon$. If $x \in \mathcal{N}$, the conclusion is trivial by choosing $x_0 = x$. Suppose $x \notin \mathcal{N}$. The maximality assumption implies that $\mathcal{N} \cup \{x\}$ is not ε-seperated, meaning $d(x, x_0) \leq \varepsilon$ for some $\varepsilon \in \mathcal{N}$. ☐

Remark 4.2.7 (Constructing a net)**.** The lemma above (lemma 4.2.6) gives an iterative algorithm to construct an ε-net for a given set K. Pick $x_1 \in K$ arbitrarily, then pick $x_2 \in K$ that is farther than ε from x_1, then pick x_3 that it is farther than ε from both x_1 and x_2, and so on. If K is compact, then the process will stop in a finite number of iterations!

Lemma 4.2.8 (Equivalence of covering and packing numbers)**.** For any set $K \subset T$ and $\varepsilon > 0$,

$$\mathcal{P}(K, d, 2\varepsilon) \leq \mathcal{N}(K, d, \varepsilon) \leq \mathcal{P}(K, d, \varepsilon).$$

Proof. The upper bound follows from lemma 4.2.6 because the packing number is exactly the number that makes $\mathcal{N}$ a maximal ε-seperated set.
For the lower bound, take any 2ε-seperated subset $\mathcal{P} = \{x_i\}$ in K and any ε-net $\mathcal{N} = \{y_j\}$ of K. By definition, each point x_i is in the ε-ball centered at some point y_j. Since any closed ε ball cannot contain two 2ε-seperated points, each ε-ball centered at y_j can contain at most one x_i. The pigeonhole principle gives $|\mathcal{P}| \leq |\mathcal{N}|$. Since $\mathcal{P}$ and $\mathcal{N}$ are arbitrary, the bound follows. □

4.2.1 Covering Numbers and Volume

This sections is about covers with $T = \mathbb{R}^n$ with the Eudlidean metric

$$d(x, y) = \|x - y\|_2.$$

Therefore, we can omit the metric when denoting the covering and packing numbers:

$$\mathcal{N}(K, \varepsilon) = \mathcal{N}(K, d, \varepsilon).$$

How do the covering numbers relate to the most classical measure, the volume of K in $\mathbb{R}^n$?

Definition 4.2.9 (Minkowski sum)**.** Let $A, B \subseteq \mathbb{R}^n$. The Minkowski sum is defined as

$$A + B := \{A + B : \ a \in A, b \in B\}.$$

Below is an example of the Minkowski sum of two sets on the plane:

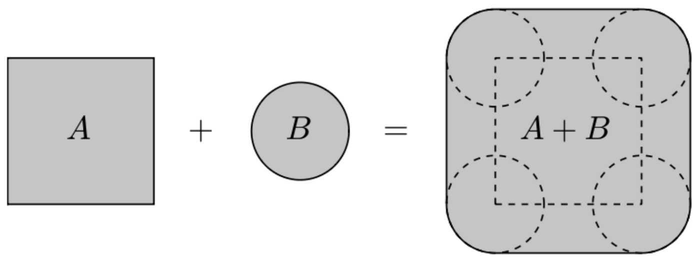

Figure 4.2 Minkowski sum of a square and a circle is a square with rounded corners.

Proposition 4.2.10 (Covering numbers and Volume)**.** Let $K \subset \mathbb{R}^n$ and $\varepsilon > 0$. Then

$$\frac{\text{Vol}(K)}{\text{Vol}(\varepsilon B_2^n)} \leq \mathcal{N}(K, \varepsilon) \leq \mathcal{P}(K, \varepsilon) \leq \frac{\text{Vol}(K + (\varepsilon/2)B_2^n)}{\text{Vol}((\varepsilon/2)B_2^n)},$$

where B_2^n denotes the unit ball in $\mathbb{R}^n$.

Proof. The middle inequality was already proven in lemma 4.2.8, hence we focus on the left and right bounds.
(**Lower bound**) Let $N := \mathcal{N}(K, \varepsilon)$. Then K can be covered by N balls with radii ε. Comparing the volumes,

$$\text{Vol}(K) \leq N \cdot \text{Vol}(\varepsilon B_2^n),$$

which gives the lower bound.
(**Upper bound**) Let $N := \mathcal{P}(K, \varepsilon)$. Then we can find N disjoint closed $\varepsilon/2$-balls with centers $x_i \in K$. While these balls may not fit entirely in K (Figure 4-1), they do fit in a slightly inflated set, namely $K + (\varepsilon/2)B_2^n$ (Basically putting balls at the boundary of K). Comparing the volume gives

$$N \cdot \text{Vol}((\varepsilon/2)B_2^n) \leq \text{Vol}(K + (\varepsilon/2)B_2^n),$$

which completes the upper bound. □

An important consequence of the volumetric bound is that the covering (hence packing) numbers are typically *exponential* in the dimension n:

Corollary 4.2.11 (Covering numbers of the Euclidean ball)**.** The covering numbers of the unit Euclidean ball B_2^n satisfy the following for any $\varepsilon > 0$:

$$\left(\frac{1}{\varepsilon}\right)^n \leq \mathcal{N}(B_2^n, \varepsilon) \leq \left(\frac{2}{\varepsilon} + 1\right)^n.$$

Proof. The lower bound immediately follows from proposition 4.2.10, since the volumd in $\mathbb{R}^n$ scale as $\mathrm{Vol}(\varepsilon B_2^n) = \varepsilon^n \mathrm{Vol}(B_2^n)$.
The upper bound follows from proposition 4.2.10 as well:

$$\mathcal{N}(B_2^n, \varepsilon) \leq \frac{\mathrm{Vol}((1+\varepsilon/2)B_2^n)}{\mathrm{Vol}((\varepsilon/2)B_2^n)} = \frac{(1+\varepsilon/2)^n}{(\varepsilon/2)^n} = \left(\frac{2}{\varepsilon} + 1\right)^n.$$

□

To simplify corollary 4.2.11, we can divide this into two cases for ε:
For $\varepsilon \in (0, 1]$, we have

$$\left(\frac{1}{\varepsilon}\right)^n \leq \mathcal{N}(B_2^n, \varepsilon) \leq \left(\frac{3}{\varepsilon}\right)^n.$$

In the other case where $\varepsilon > 1$, one ε-ball covers the unit ball hence $\mathcal{N}(B_2^n, \varepsilon) = 1$.

Remark 4.2.12 (Volume of the ball)**.** The proof of corollary 4.2.11 works with the volume of the Euclidean ball but never actually calculates it! We can compute the volume geometrically, probabilistically, and analytically (Exercises 4.27-4.29), and also extend this notion of volume to ℓ^p balls (Exercise 4.30).

Remark 4.2.13 (How to construct a net?)**.** We have an algorithm to construct nets already (remark 4.2.7), but for the Euclidean ball, we can also use a scaled integer lattice (Exercise 4.31), or just use random points (Exercise 4.39).

We can also use covering/packing notions for other objects via volumetric arguments, here is another example:

Definition 4.2.14. The Hamming cube $\{0, 1\}^n$ consists of all binary strings of length n. To turn it into a metric space, we define the hamming distance as the number of bits where the strings x and y differ:

$$d_H(x, y) := |\{i : \ x(i) \neq y(i)\}|, \ x, y \in \{0, 1\}^n.$$

Proposition 4.2.15 (Covering and packing numbers of the Hamming cube)**.** The covering and packing numbers of the Hamming cube $K = \{0, 1\}^n$ satisfy the following for any integer $m \in \{0, \ldots, n\}$:

$$\frac{2^n}{\sum_{k=0}^{m} \binom{n}{k}} \leq \mathcal{N}(K, d_H, m) \leq \mathcal{P}(K, d_H, m) \leq \frac{2^n}{\sum_{k=0}^{\lfloor m/2 \rfloor} \binom{n}{k}}.$$

Proof. Use the volumetric argument from above using cardinality instead of the volume (Exercise 4.32).
□

4.3 Application: Error Correcting Codes

4.4 Upper Bounds on Subgaussian Random Matrices