Collection of ROB 501 Lecture Notes
J.W. Grizzle

Fall 2015

Rob 501 Fall 2014
Lecture 01
Typeset by: Jimmy Amin
Proofread by: Ross Hartley

Introduction to Mathematical Arguments

Notation:

$\mathbb{N} = \{1, 2, 3, \cdots\}$ Natural numbers or counting numbers

$\mathbb{Z} = \mathcal{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ Integers or whole numbers

$\mathbb{Q} = \left\{ \dfrac{m}{q} | m, q \in \mathbb{Z}, q \neq 0, \text{no common factors (reduce all fractions)} \right\}$ Rational numbers

$\mathbb{R}$ = Real numbers

$\mathbb{C} = \{\alpha + j\beta \mid \alpha, \beta \in \mathbb{R},\ j^2 = \text{-}1\}$ Complex numbers

$\forall$ means "for every", "for all", "for each".

$\exists$ means "for some", "there exist(s)", "there is/are", "for at least one".

$\sim$ means "not". In books, and some of our handouts, you see $\neg$.

$p \Rightarrow q$ means "if p is true, then q is true.".

$p \iff q$ means "p is true if and only if q is true".

$p \iff q$ is logically equivalent to:

(a) $p \Rightarrow q$ and
(b) $q \Rightarrow p$.

The <u>contrapositive</u> of $p \Rightarrow q$ is $\sim q \Rightarrow \sim p$ (logically equivalent).

The <u>converse</u> of $p \Rightarrow q$ is $q \Rightarrow p$.

<u>Relation</u>: $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$

However, in general, $(p \Rightarrow q)$ DOES NOT IMPLY $(q \Rightarrow p)$, and vice-versa

$\square$ = Q.E.D. (Latin:"quod erat demonstrandum" = "thus it was demonstrated")

Review of Some Proof Techniques

Direct Proofs: We derive a result by applying the rules of logic to the given assumptions, definitions, axioms, and (already) known theorems.

Example:
Def. An integer n is even if $n = 2k$ for some integer k; it is odd if $n = 2k + 1$ for some integer k. Prove that the sum of two odd integers is even.

(Remark: In a definition, "if" means "if and only if".)

Proof: Let a and b be odd integers.
Hence, there exist integers k_1 and k_2 such that

$$a = 2k_1 + 1$$
$$b = 2k_2 + 1$$

It follows that

$$a + b = (2k_1 + 1) + (2k_2 + 1) = 2(k_1 + k_2 + 1)$$

Because $(k_1 + k_2 + 1)$ is an integer, $a + b$ is even. $\square$

Proof by Contrapositive: To establish $p \Rightarrow q$, we prove it logical equivalent, $\sim q \Rightarrow \sim p$.

As an example, let n be an integer. Prove that if n^2 is even, then n is even.

$p = n^2$ is even, $\sim p = n^2$ is odd
$q = n$ is even, $\sim q = n$ is odd

Our proof of $p \Rightarrow q$ is to show $\sim q \Rightarrow \sim p$. (i.e., if n is odd, then n^2 is odd.)
Assume n is odd. $\therefore$ $n = 2k+1$, for some integer k.
Therefore

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Because $(2k^2 + 2k)$ is an integer, we are done. $\square$

Proof by Exhaustion: Reduce the proof to a finite number of cases, and then prove each case separately.

Proofs by Induction:

First Principle of Induction (Standard Induction): Let $P(n)$ denote a statement about the natural numbers with the following properties:

(a) Base case: $P(1)$ is true

(b) Induction part: If $P(k)$ is true, then $P(k+1)$ is true.

$\therefore$ $P(n)$ is true for all $n \geq 1$ ($n \geq$ base case)

Example:
Claim: For all $n \geq 1$, $1 + 3 + 5 + \cdots + (2n-1) = n^2$
Proof:

Step 1: Base case: $n = 1 : 1^2 = 1 = n$

Step 2: Assume $1 + 3 + 5 + \cdots + (2k-1) = k^2 = n^2$

Step 3: To show $1+3+5+\cdots+(2k-1)+(2(k+1)-1) = (k+1)^2 = n^2$

By the induction step,

$$1 + 3 + 5 + \cdots + (2k-1) + (2(k+1)-1) = k^2 + (2(k+1)-1)$$

But,

$$k^2 + (2(k+1) - 1) = k^2 + 2k + 2 - 1 = k^2 + 2k + 1 = (k+1)^2$$

which is what we wanted to show. $\square$

Rob 501 Fall 2014
Lecture 02
Typeset by: Ross Hartley
Proofread by: Jimmy Amin

Review of Some Proof Techniques (Continued)

Second Principle of Induction (Strong Induction): Let $P(n)$ be a statement about the natural numbers with the following properties:

(a) Base Case: $P(1)$ is true.

(b) Induction: If $P(j)$ is true for all $1 \leq j \leq k$, then $P(k+1)$ is true.

Conclusion: $P(n)$ is true for all $n \geq 1$ ($n \geq$ Base Case).

Fact: Two principles of induction are equivalent. Sometimes, the second method is easier to apply.

Example:
Def.: A natural number n is composite if it can be factored as $n = a \cdot b$, where a and b are natural numbers satisfying $1 < a, b < n$. Otherwise, n is prime.

Theorem: (Fundamental Theorem of Arithmetic) Every natural number $n \geq 2$ can be factored as a product of one or more primes.

Proof:

Base Case: The number 2 can be written as the product of a single prime.

Induction: Assume that every integer between 2 and k can be written as the product of one or more primes.

<u>To Show:</u> $k+1$ can be written as the product of one or more primes.

There are two cases:

<u>Case 1:</u> $k+1$ is prime. We are done because $k+1$ is the product of one or more primes (itself).

<u>Case 2:</u> $k+1$ is composite. Then, there exist two natural numbers a and b, $1 < a, b \leq k$, such that $k+1 = a \cdot b$

Therefore, by the induction step:

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_i, \; for\ some\ primes\ p_i$$
$$b = q_1 \cdot q_2 \cdot \cdots \cdot q_j, \; for\ some\ primes\ q_j$$

Hence, $a \cdot b = (p_1 \cdot p_2 \cdot \cdots \cdot p_i) \cdot (q_1 \cdot q_2 \cdot \cdots \cdot q_j)$ is a product of primes. $\square$

Proof by Contradiction: We want to show that a statement p is true. We assume instead that the statement is false. We derive a "contradiction", meaning some statement that is obviously false, such as "$1+1=3$". More generally, we derive that R is true and R is also false (This is a contradiction.) We conclude that $\sim p$ is impossible (led to a contradiction). Hence, p must be true!

Example: Prove that $\sqrt{2}$ is an irrational number.
<u>Proof by Contradiction:</u> Assume $\sqrt{2}$ is rational.
Conclusion: There exist natural numbers m and n, $(n \neq 0)$, m and n have no common factors, such that

$$\sqrt{2} = \frac{m}{n}$$

$\therefore 2 = \frac{m^2}{n^2} \Rightarrow 2n^2 = m^2 \Rightarrow m^2$ is even $\Rightarrow m$ has to be even. (Proven in previous lecture, product of even numbers is even.)
$\therefore \exists$ a natural number k such that $m = 2k$

$\therefore 2n^2 = (2k)^2 = 4k^2$
$\therefore n^2 = 2k^2 \Rightarrow n^2$ is even $\Rightarrow n$ is even
Conclusion, m and n have 2 as a common factor. This contradicts m and n having no common factors.
Hence, $\sqrt{2}$ is not a rational number.
$\therefore \sqrt{2}$ must be irrational. $\square$

Explanation:
$p : \sqrt{2}$ irrational.
We start with the assumption that $(\sim p :)\sqrt{2}$ is a rational number.
Based on that assumption, we can deduce that $(R :)\ \exists m, n, n \neq 0, m$ and n do not have common factors such that $\sqrt{2} = \frac{m}{n}$.
However, from $\sqrt{2} = \frac{m}{n}$, we can show that $(\sim R :)$ m and n have 2 as a common factor.
$\therefore R \wedge (\sim R)$, which is a contradiction.
Conclusion: $\sim p$ is impossible.
$\therefore p$ is true.

Proof Types: In conclusion, we have following proof techniques.

- Direct Proof: $p \Rightarrow q$
- Proof by Contrapositive: $\sim q \Rightarrow \sim p$
  (Start with the conclusion being false, that is $\sim q$ and do logical steps to arrive at $\sim p$)
- Proof by Contradiction: $p \wedge (\sim q)$
  (Assume p is true and q is false. Find that both R and $\sim R$ and true, which is a contradiction.)

Negating a Statement:
Examples:

$p : x \geq 0 \qquad\qquad \sim p : x < 0$

$p : \forall x \in \mathbb{R}, f(x) > 0 \quad \sim p : \exists x \in \mathbb{R},\ f(x) \leq 0$

In general, $\sim \forall = \exists$ and $\sim \exists = \forall$.

Exercise: Let $y \in \mathbb{R}$,
$p : \forall \delta > 0, \exists x \in \mathbb{Q}$ such that $|x - y| < \delta$
What is $\sim p$?
Answer:
$\sim p : \exists \delta > 0, \forall x \in \mathbb{Q}$ such that $|x - y| \geq \delta$

Key Properties of Real Numbers: Let A be a non-empty subset of $\mathbb{R}$.

Def.

(1) A is bounded from above if $\exists b \in \mathbb{R}$ such that $x \in A \Rightarrow x \leq b$.

(2) A number $b \in \mathbb{R}$ is an upper bound for A if $\forall x \in A, x \leq b$.

(3) A number b is a least upper bound for A if

(i) b is an upper bound for A, and

(ii) b is less than or equal to every upper bound.

Notation: Least upper bound of A is denoted by $sup(A)$, the supremum of A.

Theorem: Every subset of $\mathbb{R}$ that is upper bounded has a supremum.
This is FALSE for $\mathbb{Q}$.
Here is a classical example:
Assume $A = \{x \in \mathbb{Q} | x^2 < 2\}$
An obvious candidate for the supremum is $x = \sqrt{2}$, but $\sqrt{2}$ is irrational.

Rob 501 Fall 2014
Lecture 03
Typeset by: Pedro Di Donato
Proofread by: Mia Stevens

Abstract Linear Algebra

Def: **<u>Field:</u>** (Chen, 2nd edition, page 8) : A field consists of a set, denoted by $\mathcal{F}$, of elements called *scalars* and two operations called addition "+" and multiplication "·"; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:

1. To every pair of elements α and β in $\mathcal{F}$, there correspond an element $\alpha+\beta$ in $\mathcal{F}$ called the *sum* of α and β, and an element $\alpha \cdot \beta$ in $\mathcal{F}$ called *product* of α and β.
2. Addition and multiplication are respectively commutative: For any α and β in $\mathcal{F}$,
$$\alpha + \beta = \beta + \alpha \qquad\qquad \alpha \cdot \beta = \beta \cdot \alpha$$
3. Addition and multiplication are respectively associative: For any α, β, γ in $\mathcal{F}$,
$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad\qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$
4. Multiplication is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,
$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$
5. $\mathcal{F}$ contains an element, denoted by 0, and an element, denoted by 1, such that $\alpha + 0 = \alpha$, $1 \cdot \alpha = \alpha$ for every α in $\mathcal{F}$.
6. To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha + \beta = 0$. The element β is called the *additive inverse*.

7. To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha \cdot \gamma = 1$. The element γ is called the *multiplicative inverse.*

Remark: $\mathbb{R}$ is a typical example of a field.

Examples	Non-examples
$\mathbb{R}$	Irrational (Fails axiom 1)
$\mathbb{C}$	2×2 matrices, real coeff. (Fails axiom 2)
$\mathbb{Q}$	2×2 diagonal matrices real coeff. (Fails axiom 7)

Def: **Vector Space (Linear Space)** (Chen 2nd Edition, page 9) A linear space over a field $\mathcal{F}$, denoted by $(\mathcal{X}, \mathcal{F})$, consists of a set, denoted by $\mathcal{X}$, of elements called *vectors*, a field $\mathcal{F}$, and two operations called *vector addition* and *scalar multiplication.* The two operations are defined over $\mathcal{X}$ and $\mathcal{F}$ such that they satisfy all the following conditions:

1. To every pair of vectors x^1 and x^2 in $\mathcal{X}$, there corresponds a vector $x^1 + x^2$ in $\mathcal{X}$, called the sum of x^1 and x^2 [1].
2. Addition is commutative: For any x^1, x^2 in $\mathcal{X}$, $x^1 + x^2 = x^2 + x^1$.
3. Addition is associative: For any x^1, x^2, and x^3 in $\mathcal{X}$, $\left(x^1 + x^2\right) + x^3 = x^1 + \left(x^2 + x^3\right)$.
4. $\mathcal{X}$ contains a vector, denoted by $\mathbf{0}$, such that $\mathbf{0}+x = x$ for every x in $\mathcal{X}$. The vector $\mathbf{0}$ is called the zero vector or the origin.
5. To every x in $\mathcal{X}$, there is a vector $\bar{x}$ in $\mathcal{X}$, such that $x + \bar{x} = 0$.
6. To every α in $\mathcal{F}$, and every x in $\mathcal{X}$, there corresponds a vector $\alpha \cdot x$ in $\mathcal{X}$ called the *scalar product* of α and x.
7. Scalar multiplication is associative: For any α, β in $\mathcal{F}$ and any x in $\mathcal{X}$, $\alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x$.

[1] We use x^1, x^2, x^3 to denote different *vectors*. It *does not* denote powers!

8. Scalar multiplication is distributive with respect to vector addition: For any α in $\mathcal{F}$ and any x^1, x^2 in $\mathcal{X}$, $\alpha \cdot \left(x^1 + x^2\right) = \alpha \cdot x^1 + \alpha \cdot x^2$.
9. Scalar multiplication is distributive with respect to scalar addition: For any α, β in $\mathcal{F}$ and any x in $\mathcal{X}$, $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$.
10. For any x in $\mathcal{X}$, $1 \cdot x = x$, where 1 is the element 1 in $\mathcal{F}$.

Remark: $\mathcal{F}$ = field, $\mathcal{X}$ = set of vectors

Examples:

1. Every field forms a vector space over itself. $(\mathcal{F}, \mathcal{F})$. Examples: $(\mathbb{R}, \mathbb{R})$, $(\mathbb{C}, \mathbb{C})$, $(\mathbb{Q}, \mathbb{Q})$.
2. $\mathcal{X} = \mathbb{C}$, $\mathcal{F} = \mathbb{R}$: $(\mathbb{C}, \mathbb{R})$.
3. $\mathcal{F} = \mathbb{R}$, $D \subset \mathbb{R}$ (examples: $D = [a, b]\,; D = (0, \infty)\,; D = \mathbb{R}$) and $\mathcal{X} = \{f : D \to \mathbb{R}\} = \{\text{functions from } D \text{ to } \mathbb{R}\}$
   $f, g \in \mathcal{X}$, define $f + g \in \mathcal{X}$ by $\forall t \in D,\ (f + g)(t) := f(t) + g(t)$ and let $\alpha \in \mathbb{R},\ \alpha \cdot f \in \mathcal{X}$, define $f \cdot g \in \mathcal{X}$ by $\forall t \in D, (\alpha \cdot f)(t) = \alpha \cdot f(t)$.
4. Let $\mathcal{F}$ be a field and define $\mathcal{F}^n$ the set of n-tuples written as columns
   $$\mathcal{F}^n = \left\{ \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \middle| \alpha_i \in \mathcal{F}, 1 \leq i \leq n \right\} = \mathcal{X}$$
   $$\text{Vector Addition: } \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{bmatrix}$$
   $$\text{Scalar Multiplication: } \alpha \cdot x = \begin{bmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{bmatrix}$$
5. $\mathcal{X} = \mathcal{F}^{n \times m} = \{n \times m \text{ matrices with coefficients in } \mathcal{F}\}$

Non-examples:

1. $\mathcal{X} = \mathbb{R}, \mathcal{F} = \mathbb{C}, (\mathbb{R}, \mathbb{C})$ - Fails the definition of scalar multiplication (and others).
2. $\mathcal{X} = \{x \geq 0, x \in \mathbb{R}\}, \mathcal{F} = \mathbb{R}$ - Fails the definition of scalar multiplication (and others).

Def: **Subspace:** Let $(\mathcal{X}, \mathcal{F})$ be a vector space, and let $\mathcal{Y}$ be a subset of $\mathcal{X}$. Then $\mathcal{Y}$ is a subspace if using the rules of vector addition and scalar multiplication defined in $(\mathcal{X}, \mathcal{F})$, we have that $(\mathcal{Y}, \mathcal{F})$ is a vector space.

Remark: To apply the definition, you have to check axioms 1 to 10.

Proposition: (Tools to check that something is a subspace) Let $(\mathcal{X}, \mathcal{F})$ be a vector space and $\mathcal{Y} \subset \mathcal{X}$. Then, the following are equivalent (TFAE):

1. $(\mathcal{Y}, \mathcal{F})$ is a subspace.
2. $\forall y^1, y^2 \in \mathcal{Y}, y^1 + y^2 \in \mathcal{Y}$ (closed under vector addition), and $\forall y \in \mathcal{Y}$ and $\alpha \in \mathcal{F}, \alpha y \in \mathcal{Y}$ (closed under scalar multiplication).
3. $\forall y^1, y^2 \in \mathcal{Y}$, $\forall \alpha \in \mathcal{F}, \alpha \cdot y^1 + y^2 \in \mathcal{Y}$.

Example: $(\mathcal{X}, \mathcal{F}), \mathcal{F} = \mathbb{R}$, $\mathcal{X} = \{f : (-\infty, \infty) \to \mathbb{R}\}$,
$\mathcal{Y} = \{\text{polynomials with real coefficients}\}$
Is $\mathcal{Y}$ a subspace? Yes, by part 2 of the proposition.

Non-example: $\mathcal{X} = \mathbb{R}^2, \mathcal{F} = \mathbb{R}$
$\mathcal{Y} = \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{R}^2 \middle| x_1 + x_2 = 3 \right\}$.
Let $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathcal{Y}$ and $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \in \mathcal{Y}$. Then, $\begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \end{bmatrix} \notin \mathcal{Y}$ because $x_1 + y_1 + x_2 + y_2 = 6$

Therefore, $x + y \notin \mathcal{Y}$, which means that this space is not closed under vector addition! Thus, it is not a subspace!

Note: Every vector space needs to contain the $\mathbf{0}$ vector.

ROB 501 Fall 2014
Lecture 04
Typeset by: Xiangyu Ni
Proofread by: Sulbin Park

Abstract Linear Algebra (Continued)

Def. Let $(\mathcal{X}, \mathcal{F})$ be a vector space. A linear combination is a finite sum of the form $\alpha_1 x^1 + \alpha_2 x^2 + \cdots + \alpha_n x^n$ where $n \geq 1, \alpha_i \in \mathcal{F}, x^i \in \mathcal{X}$.

Remark: $x^i = \begin{bmatrix} {x_1}^i \\ {x_2}^i \\ \vdots \\ {x_n}^i \end{bmatrix}$, where x^i means individual vectors, not powers.

Something of the form $\sum_{k=1}^{\infty} \alpha_k v^k$ is not a linear combination because it is not finite.

Def. A finite set of vectors $\{v^1, \ldots, v^k\}$ is linearly dependent if $\exists \alpha_i \in \mathcal{F}$ not all zero such that $\alpha_1 v^1 + \alpha_2 v^2 + \cdots + \alpha_k v^k = 0$. Otherwise, the set is linearly independent.

Remark: For a linearly independent set $\{v^1, \ldots, v^k\}$, $\alpha_1 v^1 + \alpha_2 v^2 + \cdots + \alpha_k v^k = 0 \iff \alpha_1 = 0, \alpha_2 = 0, \ldots, \alpha_k = 0$.

Def. An arbitrary set of vectors $\mathcal{S} \subset \mathcal{X}$ is linearly independent if every finite subset is linearly independent.

Remark: Suppose $\{v^1, \ldots, v^k\}$ is a linearly dependent set. Then, $\exists \alpha_1, \ldots, \alpha_k$ are not all zero such that $\alpha_1 v^1 + \alpha_2 v^2 + \cdots + \alpha_k v^k = 0$.

Suppose $\alpha_1 \neq 0$

$$\begin{aligned} \alpha_1 v^1 &= -\alpha_2 v^2 - \alpha_3 v^3 - \cdots - \alpha_k v^k \\ v^1 &= -\frac{\alpha_2}{\alpha_1} v^2 - \frac{\alpha_3}{\alpha_1} v^3 - \cdots - \frac{\alpha_k}{\alpha_1} v^k \end{aligned}$$

$\therefore v^1$ is a linear combination of the $\{v^2, \ldots, v^k\}$.

Example: $\mathcal{X} = \mathbb{P}(t) = \{$set of polynomials with real coefficients$\}$. $\mathcal{F} = \mathbb{R}$.
Claim: The monomials are linearly independent. In particular, for each $n \geq 0$, the set $\{1, t, \ldots, t^n\}$ is linearly independent.

Proof: Let $\alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n = o =$zero polynomial. We need to show that $\alpha_0 = \alpha_1 = \cdots = \alpha_n = 0$.
Recall that $p(t) \equiv 0$, $\frac{d^k p(t)}{dt^k}|_{t=0} = 0$ for $k = 0, 1, 2, \ldots$.
$p(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n$
$0 = p(0) \iff \alpha_0 = 0$
$0 = \frac{dp(t)}{dt}|_{t=0} = (\alpha_1 + 2\alpha_2 t + \cdots + n\alpha_n t^{n-1})|_{t=0} \iff \alpha_1 = 0$
$\vdots$
Etc. $\square$

Example: Let $\mathcal{X} = \{2 \times 3$ matrices with real coefficients$\}$. Let $v^1 = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix}$, $v^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $v^3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, $v^4 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.

$\{v^1, v^2\}$ is a linearly independent set.
$\alpha_1 v^1 + \alpha_2 v^2 = 0 \iff \begin{bmatrix} \alpha_1 & 0 & 0 \\ 2\alpha_1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha_2 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
$\iff \alpha_1 = \alpha_2 = 0$.

$\{v^1, v^2, v^4\}$ is a linearly dependent set.
$\alpha_1 v^1 + \alpha_2 v^2 + \alpha_4 v^4 = 0$
$\iff \begin{bmatrix} \alpha_1 & 0 & 0 \\ 2\alpha_1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha_2 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ \alpha_4 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
$\iff \alpha_1 = 1, \alpha_2 = -1, \alpha_4 = -2.$

Remark: $\mathcal{F}$ is important when determining whether a set is linearly independent or not. For example, let $\mathcal{X} = \mathbb{C}$ and $v^1 = 1$, $v^2 = j = \sqrt{-1}$. v^1 and v^2 are linearly independent when $\mathcal{F} = \mathbb{R}$. However, they are linearly dependent when $\mathcal{F} = \mathbb{C}$.

Def. Let $\mathcal{S}$ be a subset of a vector space $(\mathcal{X}, \mathcal{F})$. The span of $\mathcal{S}$, denoted span$\{\mathcal{S}\}$, is the set of all linear combinations of elements of $\mathcal{S}$.
span$\{\mathcal{S}\} = \{x \in \mathcal{X} | \exists n \geq 1, \alpha_1, \dots \alpha_n \in \mathcal{F}, v^1, \dots, v^n \in \mathcal{S}, x = \alpha_1 v^1 + \cdots + \alpha_n v^n\}$.

Remark: span$\{\mathcal{S}\}$ is a subset.

Example: Let $\mathcal{X} = \{f : \mathbb{R} \to \mathbb{R}\}$ and $\mathcal{F} = \mathbb{R}$. $\mathcal{S} = \{1, t, t^2, \dots\} = \{t^k | k \geq 0\}$. span$\{\mathcal{S}\} = \mathbb{P}(t) = \{\text{polynomials with real coefficients}\}$.

Is $e^t \in$ span$\{\mathcal{S}\}$? No. Although e^t can be written as a sum of polynomials (Taylor Series), the number of components of that sum is infinite. While, the linear combination has to be finite.

Def. A set of vectors $\mathcal{B}$ in $(\mathcal{X}, \mathcal{F})$ is a basis for $\mathcal{X}$ if

- $\mathcal{B}$ is linearly independent.
- span$\{\mathcal{B}\} = \mathcal{X}$.

Example: $(\mathcal{F}^n, \mathcal{F})$ where $\mathcal{F}$ is $\mathbb{R}$ or $\mathbb{C}$. $e^1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $e^2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}$, $\ldots$, $e^n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$.

$\{e^1, e^2, \ldots, e^n\}$ is both linearly independent and its span is $\mathcal{F}^n$.
$\therefore$ It is a basis.
It is called the <u>Natural Basis</u>.

Moreover, $\{e^1, e^2, \ldots, e^n, je^1, je^2, \ldots, je^n\}$ is a basis for $\mathbb{C}^n$ in $(\mathbb{C}^n, \mathbb{R})$. However, it is not a basis for $\mathbb{C}^n$ in $(\mathbb{C}^n, \mathbb{C})$.

Let $v^1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $v^2 = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 0 \end{bmatrix}$, $\ldots$, $v^n = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$. $\{v^1, v^2, \ldots, v^n\}$ is also a basis for $(\mathcal{F}^n, \mathcal{F})$ where $\mathcal{F}$ is $\mathbb{R}$ or $\mathbb{C}$.

Example: The infinite set $\{1, t, \ldots, t^n, \ldots\}$ is a basis for $(\mathbb{P}(t), \mathbb{R})$.

Def. Let $n > 0$ be an integer. The vector space $(\mathcal{X}, \mathcal{F})$ has finite dimension n if

- there exists a set with n linearly independent vectors, and
- any set with $n + 1$ or more vectors is linearly dependent.

$(\mathcal{X}, \mathcal{F})$ is infinite dimensional if for every $n > 0$, there is a linearly independent set with n or more elements in it.

Examples:
$\dim(\mathcal{F}^n, \mathcal{F}) = n$
$\dim(\mathbb{C}^n, \mathbb{R}) = 2n$
$\dim(\mathbb{P}(t), \mathbb{R}) = \infty$

Theorem: Let $(\mathcal{X}, \mathcal{F})$ be an n-dimensional vector space (n is finite). Then, any set of n linearly independent vectors is a basis.

<u>Proof:</u> Let $(\mathcal{X}, \mathcal{F})$ be n-dimensional and let $\{v^1, \cdots, v^n\}$ be a linearly independent set.
To show: $\forall x \in \mathcal{X}$, $\exists \alpha_1, \ \cdots, \ \alpha_n \in \mathcal{F}$ such that $x = \alpha_1 v^1 + \cdots + \alpha_n v^n$.
How: Because $(\mathcal{X}, \mathcal{F})$ is n-dimensional, $\{x, v^1, \cdots, v^n\}$ is a linearly dependent set. Otherwise, the $\dim \mathcal{X} > n$ which it isn't. Hence, $\exists \beta_0, \beta_1, \cdots, \beta_n \in \mathcal{F}$, NOT ALL ZERO, such that $\beta_0 x + \beta_1 v^1 + \cdots + \beta_n v^n = 0$.
Claim: $\beta_0 \neq 0$
Proof: Suppose that $\beta_0 = 0$. Then,

1. At least one of $\beta_1, \ \cdots, \ \beta_n$ is non-zero.
2. $\beta_1 v^1 + \cdots + \beta_n v^n = 0$.

1 and 2 above, imply that $\{v^1, \cdots, v^n\}$ is a linearly dependent set, which is a contradiction. Hence, $\beta_0 = 0$ cannot hold. Completing the proof, we write

$$\begin{aligned} \beta_0 x &= -\beta_1 x^1 - \cdots - \beta_n v^n \\ x &= \left(\frac{-\beta_1}{\beta_0}\right) v^1 + \cdots + \left(\frac{-\beta_n}{\beta_0}\right) v^n \\ \therefore \alpha_1 &= \frac{-\beta_1}{\beta_0}, \cdots, \alpha_n = \frac{-\beta_n}{\beta_0}. \ \square \end{aligned}$$

ROB 501 Fall 2014
Lecture 05
Typeset by: Meghan Richey
Proofread by: Su-Yang Shieh

Abstract Linear Algebra (Continued)

Proposition: Let $(\mathcal{X}, \mathcal{F})$ be a vector space with basis $\{v^1, \cdots, v^n\}$. Let $x \in \mathcal{X}$. Then, $\exists$ unique coefficients $\alpha_1, \cdots, \alpha_n$ such that $x = \alpha_1 v^1 + \alpha_2 v^2 + \cdots + \alpha_n v^n$.

Proof: Suppose x can also be written as $x = \beta_1 v^1 + \beta_2 v^2 + \cdots + \beta_n v^n$.
We need to show: $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \cdots, \alpha_n = \beta_n$.

$$0 = x - x = (\alpha_1 - \beta_1)v^1 + \cdots + (\alpha_n - \beta_n)v^n$$

By linear independence of $\{v^1, \cdots, v^n\}$, we can obtain that $\alpha_1 - \beta_1 = 0, \cdots, \alpha_n - \beta_n = 0$.
Hence, $\alpha_1 = \beta_1, \ \cdots, \ \alpha_n = \beta_n$, that is, the coefficients are unique. $\square$

Def: $x \in \mathcal{X}$, $x = \alpha_1 v^1 + \cdots + \alpha_n v^n$. x uniquely defines $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \in \mathcal{F}^n$.

$[x]_v = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$ is the representation of x with respect to the basis $v = \{v^1, \cdots, v^n\}$ if and only if $x = \alpha_1 v^1 + \cdots + \alpha_n v^n$.

Example: $\mathcal{F} = \mathbb{R}$, $\mathcal{X} = \{2 \times 2 \text{ matrices with real coefficients}\}$

Basis 1: $v^1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $v^2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $v^3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $v^4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Basis 2: $w^1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $w^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $w^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $w^4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$x = \begin{bmatrix} 5 & 3 \\ 1 & 4 \end{bmatrix} = 5w^1 + 2w^2 + 1w^3 + 4w^4$

Therefore, $[x]_w = \begin{bmatrix} 5 \\ 2 \\ 1 \\ 4 \end{bmatrix} \in \mathbb{R}^4$.

Easy Facts:

1. Addition of vectors in $(\mathcal{X}, \mathcal{F}) \equiv$ Addition of the representations in $(\mathcal{F}^n, \mathcal{F})$.
$$[x+y]_v = [x]_v + [y]_v$$

2. Scalar multiplication in $(\mathcal{X}, \mathcal{F}) \equiv$ Scalar multiplication with the representations in $(\mathcal{F}^n, \mathcal{F})$.
$$[\alpha x]_v = \alpha [x]_v$$

3. Once a basis is chosen, any n-dimensional vector space $(\mathcal{X}, \mathcal{F})$ "looks like" $(\mathcal{F}^n, \mathcal{F})$.

Change of Basis Matrix: Let $\{u^1, \cdots, u^n\}$ and $\{\bar{u}^1, \cdots, \bar{u}^n\}$ be two bases for $(\mathcal{X}, \mathcal{F})$. Is there a relation between $[x]_u$ and $[x]_{\bar{u}}$?

Theorem: $\exists$ an invertible matrix P, with coefficients in $\mathcal{F}$, such that $\forall x \in (\mathcal{X}, \mathcal{F})$, $[x]_{\bar{u}} = P[x]_u$.
Moreover, $P = [P_1|P_2|\cdots|P_n]$ with $P_i = [u^i]_{\bar{u}} \in \mathcal{F}^n$ where P_i is the i^{th} column of the matrix P and $[u^i]_{\bar{u}}$ is the representation of u^i with respect to $\bar{u}$.

<u>Proof:</u> Let $x = \alpha_1 u^1 + \cdots + \alpha_n u^n = \bar{\alpha}_1 \bar{u}^1 + \cdots + \bar{\alpha}_n \bar{u}^n$.

$$\alpha = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = [x]_u$$

$$\bar{\alpha} = \begin{bmatrix} \bar{\alpha}_1 \\ \bar{\alpha}_2 \\ \vdots \\ \bar{\alpha}_n \end{bmatrix} = [x]_{\bar{u}}$$

$$\bar{\alpha} = [x]_{\bar{u}} = \Big[\sum_{i=1}^{n} \alpha_i u^i \Big]_{\bar{u}} = \sum_{i=1}^{n} \alpha_i [u^i]_{\bar{u}} = \sum_{i=1}^{n} \alpha_i P_i = P\alpha.$$

Therefore, $\bar{\alpha} = P\alpha = P[x]_u$.

Now we need to show that P is invertible:
Define $\bar{P} = [\bar{P}_1 | \bar{P}_2 | \cdots | \bar{P}_n]$ with $\bar{P}_i = [\bar{u}^i]_u$.
Do the same calculations and obtain $\alpha = \bar{P}\bar{\alpha}$.
Then, we can obtain that $\alpha = \bar{P}P\alpha$ and $\bar{\alpha} = P\bar{P}\bar{\alpha}$.
Therefore, $P\bar{P} = \bar{P}P = I$.
In conclusion, $\bar{P}$ is the inverse of P ($\bar{P} = P^{-1}$). $\square$

Example: $\mathcal{X} = \{2 \times 2 \text{ matrices with real coefficients}\}$, $\mathcal{F} = \mathbb{R}$.

$$u = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

$$\bar{u} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

We have following relations:
$\alpha = P\bar{\alpha}$, $P_i = [u^i]_{\bar{u}}$, $\bar{\alpha} = \bar{P}\alpha$, $\bar{P}_i = [\bar{u}^i]_u$. ($\bar{P}^{-1} = P$, $P^{-1} = \bar{P}$)
Typically, compute the easier of P or $\bar{P}$, and compute the other by inversion.

We choose to compute $\bar{P}$

$$\bar{P}_1 = [\bar{u}^1]_u = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\bar{P}_2 = [\bar{u}^2]_u = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\bar{P}_3 = [\bar{u}^3]_u = \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix}$$

$$\bar{P}_4 = [\bar{u}^4]_u = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Therefore, $\bar{P}= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and $P = \bar{P}^{-1}$

Def. Let A be an $n \times n$ matrix with complex coefficients. A scalar $\lambda \in \mathbb{C}$ is an eigenvalue (e-value) of A, if $\exists$ a non-zero vector $v \in \mathbb{C}^n$ such that $Av = \lambda v$. Any such vector v is called an eigenvector (e-vector) associated with λ. Eigenvectors are not unique.

To find eigenvalues, we need to know conditions under which $\exists v \neq 0$ such that $Av = \lambda v$.

$$Av = \lambda v \iff (\lambda I - A)v = 0 \iff \det(\lambda I - A) = 0$$

Example: $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, det(\lambda I - A) = \lambda^2 + 1 = 0.$
Therefore, the eigenvalues are $\lambda_1 = j, \lambda_2 = -j$.
To find eigenvectors, we need to solve $(A - \lambda_i I)v^i = 0$.
The eigenvectors are $v^1 = \begin{bmatrix} 1 \\ j \end{bmatrix}, v^2 = \begin{bmatrix} 1 \\ -j \end{bmatrix}$.
Note that both eigenvalues and eigenvectors are complex conjugate pairs.

ROB 501 Fall 2014
Lecture 06
Typeset by: Katie Skinner
Proofread by: Meghan Richey
Edited by Grizzle: 24 Sept 2015

Abstract Linear Algebra (Continued)

Def. $\Delta(\lambda) = \det(\lambda I - A)$ is called the characteristic polynomial. $\Delta(\lambda) = 0$ is called the characteristic equation.

$$\Delta(\lambda) = (\lambda - \lambda_1)^{m_1}(\lambda - \lambda_2)^{m_2} \cdots (\lambda - \lambda_p)^{m_p}$$

where $\lambda_1, \cdots, \lambda_p$ are the distinct eigenvalues, and m_i is the multiplicity of λ_i such that

$$m_1 + m_2 + \cdots + m_p = n$$

Theorem: Let A be an $n \times n$ matrix with coefficients in $\mathbb{R}$ or $\mathbb{C}$. If the e-values $\{\lambda_1, \cdots, \lambda_n\}$ are distinct, that is, $\lambda_i \neq \lambda_j$ for all $1 \leq i \neq j \leq n$, then the e-vectors $\{v^1, \cdots, v^n\}$ are linearly independent in $(\mathbb{C}^n,\mathbb{C})$.

Remark: Restatement of the theorem: If $\{\lambda_1, \cdots, \lambda_n\}$ are distinct then $\{v^1, \cdots, v^n\}$ is a basis for $(\mathbb{C}^n,\mathbb{C})$.

Proof: We prove the contrapositive and show there is a repeated e-value ($\lambda_i = \lambda_j$ for some $i \neq j$).

$\{v^1, \cdots, v^n\}$ linearly dependent $\Rightarrow \exists\ \alpha_1, \cdots, \alpha_n \in \mathbb{C}$, not all zero, such that $\alpha_1 v^1 + \cdots + \alpha_n v^n = 0 (*)$.

Without loss of generality, we can suppose $\alpha_1 \neq 0$. (that is, we can always reorder of e-values so that the first coefficient is nonzero.)

Because v^i is an e-vector,

$$(A - \lambda_j I)v^i = Av^i - \lambda_j v^i = \lambda_i v^i - \lambda_j v^i = (\lambda_i - \lambda_j)v^i$$

Side Note: It is an easy exercise to show

$(A-\lambda_2 I)(A-\lambda_3 I)\cdots(A-\lambda_n I)v^i = (\lambda_i-\lambda_2)(\lambda_i-\lambda_3)\cdots(\lambda_i-\lambda_n)v^i, 2 \leq i \leq n$

Let $i = 1$

$$(\lambda_1 - \lambda_2)(\lambda_1 - \lambda_3)\cdots(\lambda_1 - \lambda_n)v^1$$

Let $i = 2$

$$(\lambda_2 - \lambda_2)(\lambda_2 - \lambda_3)\cdots(\lambda_2 - \lambda_n)v^2 = 0$$

Etc.

Combining the above with $(*)$, we obtain

$$0 = (A - \lambda_2 I)(A - \lambda_3 I)\cdots(A - \lambda_n I)(\alpha_1 v^1 + \cdots + \alpha_n v^n)$$

$$= \alpha_1(\lambda_1 - \lambda_2)(\lambda_1 - \lambda_3)\cdots(\lambda_1 - \lambda_n)v^1$$

We know $\alpha_1 \neq 0$, as stated above, and $v^1 \neq 0$, by definition of e-vectors.

$$\therefore 0 = (\lambda_1 - \lambda_2)(\lambda_1 - \lambda_3)\cdots(\lambda_1 - \lambda_n)$$

At least one the terms $(\lambda_1 - \lambda_k)$, $2 \leq k \leq n$, must be zero, and thus there is a repeated e-value $\lambda_1 = \lambda_k$ for some $2 \leq k \leq n$. $\square$

Def. Let $(\mathcal{X}, \mathcal{F})$ and $(\mathcal{Y}, \mathcal{F})$ be vector spaces. $\mathcal{L} : \mathcal{X} \to \mathcal{Y}$ is a linear operator if for all $x, z \in \mathcal{X}$, $\alpha, \beta \in \mathcal{F}$,

$$\mathcal{L}(\alpha x + \beta z) = \alpha\mathcal{L}(x) + \beta\mathcal{L}(z)$$

Equivalently,

$$\mathcal{L}(x + z) = \mathcal{L}(x) + \mathcal{L}(z)$$
$$\mathcal{L}(\alpha x) = \alpha\mathcal{L}(x)$$

Example:

1. Let A be an $n \times m$ matrix with coefficients in $\mathcal{F}$.

   Define $\mathcal{L} : \mathcal{F}^m \to \mathcal{F}^n$ by $\mathcal{L}(x) = Ax$, then $\mathcal{L}$ is a linear operator. Check that linearity and multiplication by scalar are satisfied to prove this.

2. Let $\mathcal{X} = \{\text{polynomials whose degrees} \leq 3\}, \mathcal{F} = \mathbb{R}, \mathcal{Y} = \mathcal{X}$. Then for $p \in \mathcal{X}, \mathcal{L}(p) = \frac{d}{dt}p(t)$.

Def. Let $(\mathcal{X}, \mathcal{F})$ and $(\mathcal{Y}, \mathcal{F})$ be finite dimensional vector spaces, and $\mathcal{L} : \mathcal{X} \to \mathcal{Y}$ be a linear operator. A matrix representation of $\mathcal{L}$ with respect to a basis $\{u^1, \cdots, u^m\}$ for $\mathcal{X}$ and $\{v^1, \cdots, v^n\}$ for $\mathcal{Y}$ is an $n \times m$ matrix A, with coefficients in $\mathcal{F}$, such that $\forall x \in \mathcal{X}$, $\left[\mathcal{L}(x)\right]_{\{v^1,\cdots,v^n\}} = A\left[x\right]_{\{u^1,\cdots,u^m\}}$.

Theorem: Let $(\mathcal{X}, \mathcal{F})$ and $(\mathcal{Y}, \mathcal{F})$ be finite dimensional vector spaces, $\mathcal{L} : \mathcal{X} \to \mathcal{Y}$ a linear operator, $\{u^1, \cdots, u^m\}$ a basis for $\mathcal{X}$ and $\{v^1, \cdots, v^n\}$ a basis for $\mathcal{Y}$, then $\mathcal{L}$ has a matrix representation $A = \left[A_1 | \cdots | A_m\right]$, where the i^{th} column of A is given by

$$A_i = \left[\mathcal{L}(u^i)\right]_{\{v^1,\cdots,v^n\}}, \quad 1 \leq i \leq m$$

Proof: $x \in \mathcal{X}, x = \alpha_1 u^1 + \cdots + \alpha_m u^m$ so that its representation is

$$\left[x\right]_{\{u^1,\cdots,u^m\}} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix} \in \mathcal{F}^m$$

As in the theorem, we define

$$A_i = \left[\mathcal{L}(u^i)\right]_{\{v^1,\cdots,v^n\}}, \quad 1 \leq i \leq m$$

.

Using linearity

$$\begin{aligned}\mathcal{L}(x) &= \mathcal{L}(\alpha_1 u^1 + \cdots + \alpha_m u^m)\\ &= \alpha_1 \mathcal{L}(u^1) + \cdots + \alpha_m \mathcal{L}(u^m)\end{aligned}$$

Hence, computing representations, we have

$$\begin{aligned}[\mathcal{L}(x)]_{\{v^1,\cdots,v^n\}} &= [\alpha_1 \mathcal{L}(u^1) + \cdots + \alpha_m \mathcal{L}(u^m)]_{\{v^1,\cdots,v^n\}}\\ &= \alpha_1 [\mathcal{L}(u^1)]_{\{v^1,\cdots,v^n\}} + \cdots + \alpha_m [\mathcal{L}(u^m)]_{\{v^1,\cdots,v^n\}}\\ &= \alpha_1 A_1 + \cdots + \alpha_m A_m\\ &= \left[A_1 | A_2 | \cdots | A_m\right] \begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_m\end{bmatrix}\\ &= A \left[x\right]_{\{u^1,\cdots,u^m\}}\end{aligned}$$

$$\therefore \left[\mathcal{L}(x)\right]_{\{v^1,\cdots,v^n\}} = A \left[x\right]_{\{u^1,\cdots,u^m\}} \ \square$$

Example:

$\mathcal{F} = \mathbb{R}, \mathcal{X} = \{\text{polynomials, degrees} \leq 3\}, \mathcal{Y} = \{\text{polynomials, degrees} \leq 3\}$.

Put the same basis on $\mathcal{X}$ and $\mathcal{Y}$, $\{1, t, t^2, t^3\}$. Let $\mathcal{L} : \mathcal{X} \to \mathcal{Y}$ be differentiation. Find the matrix representation, A, which will be a real 4×4 matrix.

<u>Solution:</u> Compute A column by column, where $A = \big[A_1|A_2|A_3|A_4\big]$.

$$A_1 = \big[\mathcal{L}(1)\big]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$A_2 = \big[\mathcal{L}(t)\big]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$A_3 = \big[\mathcal{L}(t^2)\big]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}$$

$$A_4 = \big[\mathcal{L}(t^3)\big]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} 0 \\ 0 \\ 3 \\ 0 \end{bmatrix}$$

and thus

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Let's check that it makes sense

$$p(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3$$

and

$$\big[p(t)\big]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

$$A[p(t)]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_1 \\ 2a_2 \\ 3a_3 \\ 0 \end{bmatrix}$$

Does this correspond to differentiating the polynomial $p(t)$? We see that

$$\frac{d}{dt}p(t) = a_1 + 2a_2 t + 3a_3 t^2$$

$$[\frac{d}{dt}p(t)]_{\{1,t,t^2,t^3\}} = \begin{bmatrix} a_1 \\ 2a_2 \\ 3a_3 \\ 0 \end{bmatrix}$$

and thus, yes indeed,

$$A[p(t)]_{\{1,t,t^2,t^3\}} = [\frac{d}{dt}p(t)]_{\{1,t,t^2,t^3\}}$$

.

Rob 501 Fall 2014
Lecture 07
Typeset by: Zhiyuan Zuo
Proofread by: Vittorio Bichucher
Revised by Ni on 31 October 2015

Abstract Linear Algebra (Continued)

Elementary Properties of Matrices (Assumed Known)

$A = n \times m$ matrix with coefficients in $\mathbb{R}$ or $\mathbb{C}$.

Def. Rank of $A = \#$ of linearly independent columns of A.

Theorem: $\text{rank}(A) = \text{rank}(A^\top) = \text{rank}(AA^\top) = \text{rank}(A^\top A)$.

Corollary: # of linearly independent rows = # of linearly independent columns.

Normed Spaces:

Let Field $\mathcal{F}$ be $\mathbb{R}$ or $\mathbb{C}$,

Def. A function $\|\cdot\|$: $\mathcal{X} \to \mathbb{R}$ is a norm if it satisfies

(a) $\|x\| \geq 0, \forall x \in \mathcal{X}$ and $\|x\| = 0 \Leftrightarrow\ x = 0$

(b) Triangle inequality: $\|x + y\| \leq \|x\| + \|y\|, \forall x, y \in \mathcal{X}$

(c) $\|\alpha x\| = |\alpha| \cdot \|x\|, \forall x \in \mathcal{X}, \alpha \in \mathcal{F}, \begin{cases} \text{If } \alpha \in \mathbb{R}, |\alpha| \text{ means the absolute value} \\ \text{If } \alpha \in \mathbb{C}, |\alpha| \text{ means the magnitude} \end{cases}.$

Examples:

1 $\mathcal{F} = \mathbb{R}$ or $\mathbb{C}$, $\mathcal{X} = \mathbb{F}^n$.

i) $\|x\|_2 = \left(\sum_{i=1}^{n} |x_i|^2\right)^{\frac{1}{2}}$, Two norm, Euclidean norm

ii) $\|x\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{\frac{1}{p}}$, $1 \leq p < \infty$, p-norm

iii) $\|x\|_\infty = \max\limits_{1\le i\le n} |x_i|$, max-norm, sup-norm, ∞-norm

2 $\mathcal{F} = \mathbb{R}$, $\mathcal{D} \subset \mathbb{R}$, $\mathcal{D} = [a, b]$, $a < b < \infty$,
$\mathcal{X} = \{f : \mathcal{D} \to \mathbb{R} \mid f \text{ is continuous}\}$.

i) $\|f\|_2 = (\int_a^b |f(t)|^2 \, \mathrm{d}t)^{\frac{1}{2}}$
ii) $\|f\|_p = (\int_a^b |f(t)|^p \, \mathrm{d}t)^{\frac{1}{p}}$, $1 \le p < \infty$
iii) $\|f\|_\infty = \max\limits_{a\le t\le b} |f(t)|$, which is also written $\|f\|_\infty = \sup\limits_{a\le t\le b} |f(t)|$

Def. $(\mathcal{X}, \mathcal{F}, \|\cdot\|)$ is called a normed space.
Distance: For $x, y \in \mathcal{X}$, $d(x, y) := \|x - y\|$ is called the distance from x to y.
Note: $d(x, y) = d(y, x)$.
Distance to a set: Let $S \subset \mathcal{X}$ be a subset.

$$d(x, S) := \inf_{y\in S} \|x - y\|$$

If $\exists x^* \in S$ such that $d(x, S) = \|x - x^*\|$, then x^* is a best approximation of x by elements of S.
Sometimes, write $\hat{x}$ for x^* because we are really thinking of the solution as an approximation.

Important questions:

a) When does an x^* exist?

b) How to characterize (compute) x^* such that $\|x - x^*\| = d(x, S)$, $x^* \in S$?

c) If a solution exists, is it unique?

Notation: When x^* (or $\hat{x}$) exists, we write $x^* = \arg\min\limits_{y\in S} \|x - y\|$.

Inner Product Space:
Recall: $z = \alpha + j\beta \in \mathbb{C}$, $\alpha, \beta \in \mathbb{R}$, $\bar{z} = z$'s complex conjugate $= \alpha - j\beta$

Def. Let $(\mathcal{X}, \mathbb{C})$ be a vector space, a function $\langle \cdot\,, \cdot \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{C}$ is an inner product if

(a) $\langle a, b \rangle = \overline{\langle b, a \rangle}$.

(b) $\langle \alpha_1 x_1 + \alpha_2 x_2, y \rangle = \alpha_1 \langle x_1, y \rangle + \alpha_2 \langle x_2, y \rangle$, linear in the left argument. Sum can also appear on the right, just use the property (a).

(c) $\langle x, x \rangle \ \geq \ 0$ for any $x \in \mathcal{X}$, and $\langle x, x \rangle \ = \ 0 \Leftrightarrow x = 0$. ($\langle x, x \rangle$ is a real number. Therefore, it can be compared to 0.)

Remarks:

1) $\langle x, x \rangle \ = \ \overline{\langle x, x \rangle}$, by (a). Hence, $\langle x, x \rangle$ is always a real number.

2) If the vector space is defined as $(\mathcal{X}, \mathbb{R})$, replace (a) with (a$'$) $\langle a, b \rangle \ = \ \langle b, a \rangle$

Examples:

a) $(\mathbb{C}^n, \mathbb{C})$, $\langle x, y \rangle \ = \ x^\top \overline{y} \ = \ \sum\limits_{i=1}^{n} x_i \overline{y_i}$.

b) $(\mathbb{R}^n, \mathbb{R})$, $\langle x, y \rangle \ = \ x^\top y \ = \ \sum\limits_{i=1}^{n} x_i y_i$.

c) $\mathcal{F} = \mathbb{R}$, $\mathcal{X} = \{A \,|\, n \times m \text{ real matrices}\}$, $\langle A, B \rangle \ = \ \mathrm{tr}(AB^\top) \ = \ \mathrm{tr}(A^\top B)$.

d) $\mathcal{X} = \{f : [a, b] \to \mathbb{R}, f \text{ continuous}\}$, $\mathcal{F} = \mathbb{R}$, $\langle f, g \rangle \ = \ \int_a^b f(t) g(t)\, \mathrm{d}t$.

Theorem: (Cauchy-Schwarz Inequality) Let $\mathcal{F}$ be $\mathbb{R}$ or $\mathbb{C}$, $(\mathcal{X}, \mathcal{F}, \langle \cdot\,, \cdot \rangle)$ be an inner product space. Then, for all $x, y \in \mathcal{X}$

$$|\langle x, y \rangle| \ \leq \ \langle x, x \rangle^{1/2} \langle y, y \rangle^{1/2}.$$

Proof: (Will assume $\mathcal{F} = \mathbb{R}$).

If $y = 0$, the result is clearly to true.
Assume $y \neq 0$ and let $\lambda \in \mathbb{R}$ to be chosen, we have

$$\begin{aligned} 0 \;\leq\; & \langle x - \lambda y,\, x - \lambda y\rangle \\ =& \langle x,\, x - \lambda y\rangle - \lambda\langle y,\, x - \lambda y\rangle \\ =& \langle x, x\rangle - \lambda\langle x, y\rangle - \lambda\langle y, x\rangle + \lambda^2\langle y, y\rangle \\ =& \langle x, x\rangle - 2\lambda\langle x, y\rangle + \lambda^2\langle y, y\rangle. \end{aligned}$$

Now, select $\lambda = \langle x, y\rangle/\langle y, y\rangle$.
Then,

$$\begin{aligned} 0 \leq & \langle x - \lambda y, x - \lambda y\rangle \\ =& \langle x, x\rangle - 2|\langle x, y\rangle|^2/\langle y, y\rangle + |\langle x, y\rangle|^2/\langle y, y\rangle \\ =& \langle x, x\rangle - |\langle x, y\rangle|^2/\langle y, y\rangle. \end{aligned}$$

Therefore, we can conclude that $|\langle x, y\rangle|^2 \leq \langle x, x\rangle\langle y, y\rangle \Rightarrow |\langle x, y\rangle| \leq \langle x, x\rangle^{1/2}\langle y, y\rangle^{1/2}$. $\square$

Rob 501 Fall 2014
Lecture 08
Typeset by: Sulbin Park
Proofread by: Ming-Yuan Yu

Orthogonal Bases

Corollary: Let $(\mathcal{X}, \mathcal{F}, \langle \cdot, \cdot \rangle)$ be an inner product space. Then,

$$\|x\| := \langle x, x\rangle^{1/2} = \sqrt{\langle x, x\rangle}$$

is a norm.

Proof: (For $\mathcal{F} = \mathbb{R}$) will only check the triangle inequality $\|x+y\| \leq \|x\| + \|y\|$, which is equivalent to showing

$$\begin{aligned}
\|x+y\|^2 &\leq \|x\|^2 + \|y\|^2 + 2\|x\| \cdot \|y\| \\
\|x+y\|^2 &= \langle x+y, x+y\rangle \\
&= \langle x, x+y\rangle + \langle y, x+y\rangle \\
&= \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle \\
&= \|x\|^2 + \|y\|^2 + 2\langle x, y\rangle \\
&\leq \|x\|^2 + \|y\|^2 + 2\,|\langle x, y\rangle| \\
&\leq \|x\|^2 + \|y\|^2 + 2\|x\| \cdot \|y\| \;\square
\end{aligned}$$

Def.

(a) Two vectors x and y are orthogonal if $\langle x, y\rangle = 0$. Notation: $x \perp y$

(b) A set of vectors S is orthogonal if

$$\forall x,y \in S, x \neq y \Rightarrow \langle x, y\rangle = 0 \text{ (i.e. } x \perp y)$$

(c) If in addition, $\|x\| = 1$ for all $x \in S$, then S is an orthonormal set.

Remark: $x \neq 0$, $\frac{x}{\|x\|}$ has norm 1.

$$\left\| \frac{x}{\|x\|} \right\| = \left| \frac{1}{\|x\|} \right| \cdot \|x\| = \frac{1}{\|x\|} \cdot \|x\| = 1$$

Pythagorean Theorem: If $x \perp y$, then

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2$$

.

Proof: From the proof of the triangle inequality,

$$\begin{aligned} \|x + y\|^2 &= \|x\|^2 + \|y\|^2 + 2\langle x, y \rangle \\ &= \|x\|^2 + \|y\|^2 \text{ (because } \langle x, y \rangle = 0) \ \square \end{aligned}$$

Pre-projection Theorem: Let $\mathcal{X}$ be a finite-dimensional (real) inner product space, M be a subspace of $\mathcal{X}$, and x be an arbitrary point in $\mathcal{X}$.

(a) If $\exists m_0 \in M$ such that

$$\|x - m_0\| \leq \|x - m\| \quad \forall m \in M$$

then m_0 is unique.

(b) A necessary and sufficient condition that m_0 is a minimizing vector in M is that the vector $x - m_0$ is orthogonal to M.

Remarks:

(a') If $\exists m_0 \in M$ such that $\|x - m_0\| = d(x, M) = \inf_{m \in M} \|x - m\|$, then m_0 is unique. (equivalent to (a))

(b') $\|x - m_0\| = d(x, M) \Leftrightarrow x - m_0 \perp M$. (equivalent to (b))

Proof:
Claim 1: If $m_0 \in M$ satisfies $\|x - m_0\| = d(x, M)$, then $x - m_0 \perp M$.
Proof: (By contrapositive) Assume $x - m_0 \not\perp M$, we will find $m_1 \in M$ such that $\|x - m_1\| < \|x - m_0\|$.
Suppose $x - m_0 \not\perp M$. Hence, $\exists m \in M$ such that $\langle x - m_0, m \rangle \neq 0$. We know $m \neq 0$, and hence we define $\tilde{m} = \frac{m}{\|m\|} \in M$.
Define $\delta := \langle x - m_0, \tilde{m} \rangle \neq 0$.

$$
\begin{aligned}
m_1 &= m_0 + \delta \tilde{m} \\
\therefore m_1 &\in M \\
\|x - m_1\|^2 &= \|x - m_0 - \delta \tilde{m}\|^2 \\
&= \langle x - m_0 - \delta \tilde{m}, x - m_0 - \delta \tilde{m} \rangle \\
&= \langle x - m_0, x - m_0 \rangle - \delta \underbrace{\langle x - m_0, \tilde{m} \rangle}_{\delta} - \delta \underbrace{\langle \tilde{m}, x - m_0 \rangle}_{\delta} + \delta^2 \underbrace{\langle \tilde{m}, \tilde{m} \rangle}_{=1} \\
&= \|x - m_0\|^2 - \delta^2
\end{aligned}
$$

$\therefore \|x - m_1\|^2 < \|x - m_0\|^2$ $\square$

Claim 2: If $x - m_0 \perp M$, then $\|x - m_0\| = d(x, M)$ and m_0 is unique.
Proof: Recall the Pythagorean Theorem:

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 \text{ when } x \perp y$$

Let $m \in M$ be arbitrary and suppose $x - m_0 \perp M$.
Then,

$$
\begin{aligned}
\|x - m\|^2 &= \|x - m_0 + \underbrace{m_0 - m}_{\in M}\|^2 \\
&= \|x - m_0\|^2 + \|m_0 - m\|^2 \quad (x - m_0 \perp M)
\end{aligned}
$$

$\therefore \inf_{m \in M} \|x - m\| = \|x - m_0\|$ and the unique minimizer is m_0. $\square$

How to Construct Orthogonal Sets
Gram-Schmidt Process: Let $\{y^1, \ldots, y^n\}$ be a linearly independent set of vectors. We will produce $\{v^1, \ldots, v^n\}$ orthogonal, such that

$$\forall 1 \leq k \leq n, \ \ \text{span}\{y^1, \ldots, y^k\} = \text{span}\{v^1, \ldots, v^k\}.$$

Step 1: $v^1 = y^1$
Remark: $v^1 \neq 0$ because $\{y^1, \ldots, y^n\}$ linearly independent.

Step 2: $v^2 = y^2 - a_{21}v^1$ and choose a_{21} such that $v^1 \perp v^2$.

$$0 = \langle v^2, v^1 \rangle = \langle y^2 - a_{21}v^1, v^1 \rangle = \langle y^2, v^1 \rangle - a_{21}\langle v^1, v^1 \rangle$$

$$\therefore a_{21} = \frac{\langle y^2, v^1 \rangle}{\|v^1\|^2} \quad (\|v^1\| \neq 0 \text{ because } v^1 \neq 0)$$

Claim: $\text{span}\{y^1, y^2\} = \text{span}\{v^1, v^2\}$.
Proof: Know $\text{span}\{y^1\} = \text{span}\{v^1\}$.
To show: $y^2 \in \text{span}\{v^1, v^2\}$ and $v^2 \in \text{span}\{y^1, y^2\}$.

Rob 501 Fall 2014
Lecture 09
Typeset by: Pengcheng Zhao
Proofread by: Xiangyu Ni
Revised by Ni on 1 November 2015

Orthogonal Bases (Continued)

Gram-Schmidt Process: Let $\{y^1, \cdots, y^n\}$ be a linearly independent set of vectors. We will produce $\{v^1, \cdots, v^n\}$ orthogonal such that, $\forall 1 \leq k \leq n$, $\text{span}\{v^1, \cdots, v^k\} = \text{span}\{y^1, \cdots, y^k\}$.

<u>Step 1</u>

$$v^1 = y^1$$

<u>Step 2</u>

$$v^2 = y^2 - a_{21}v^1$$

$$\langle v^2, v^1 \rangle = 0 \Leftrightarrow a_{21} = \frac{\langle y^2, v^1 \rangle}{\|v^1\|^2}$$

<u>Step 3</u>

$$v^3 = y^3 - a_{31}v^1 - a_{32}v^2$$

Choose coefficients such that $\langle v^3, v^1 \rangle = 0$ and $\langle v^3, v^2 \rangle = 0$,

$$0 = \langle v^3, v^1 \rangle = \langle y^3, v^1 \rangle - a_{31}\langle v^1, v^1 \rangle - a_{32}\underbrace{\langle v^2, v^1 \rangle}_{=0}$$

$$0 = \langle v^3, v^2 \rangle = \langle y^3, v^2 \rangle - a_{31}\underbrace{\langle v^1, v^2 \rangle}_{=0} - a_{32}\langle v^2, v^2 \rangle$$

$$\therefore \quad a_{31} = \frac{\langle y^3, v^1 \rangle}{\|v^1\|^2} \qquad a_{32} = \frac{\langle y^3, v^2 \rangle}{\|v^2\|^2}$$

Therefore, we can conclude that $v_k = y_k - \sum_{j=1}^{k-1} \frac{\langle y_k, v_j \rangle}{\|v_j\|^2} v_j$.

Proof of G-S Process: Need to show $\text{span}\{v^1, \cdots, v^k\} = \text{span}\{y^1, \cdots, y^k\}$

$$\Leftrightarrow \begin{cases} \{v^1, \cdots, v^k\} \subseteq \text{span}\{y^1, \cdots, y^k\} \Leftrightarrow v^k \in \text{span}\{y^1, \cdots, y^k\} \\ \{y^1, \cdots, y^k\} \subseteq \text{span}\{v^1, \cdots, v^k\} \Leftrightarrow y^k \in \text{span}\{v^1, \cdots, v^k\} \end{cases}.$$

Intermediate Facts

Proposition: Let$(\mathcal{X}, \mathcal{F})$ be an n-dimensional vector space and let $\{v^1, \cdots, v^k\}$ be a linearly independent set with $0 < k < n$. Then, $\exists v^{k+1}$ such that $\{v^1, \cdots, v^k, v^{k+1}\}$ is linearly independent.

Proof: (By contradiction)
Suppose no such v^{k+1} exists. Hence, $\forall x \in \mathcal{X}$, $x \in \text{span}\{v^1, \cdots, v^k\}$.
$\therefore \mathcal{X} \subset \text{span}\{v^1, \cdots, v^k\}$.
$\therefore \dim(\mathcal{X}) \leq \dim(\text{span}\{v^1, \cdots, v^k\})$.
$\therefore n \leq k$, which contradicts $k < n$. $\square$

Corollary: In a finite dimensional vector space, any linearly independent set can be completed to a basis. More precisely, let $\{v^1, \cdots, v^k\}$ be linearly independent, $n = \dim(\mathcal{X}), k < n$.
Then, $\exists v^{k+1}, \cdots, v^n$ such that $\{v^1, \cdots, v^k, v^{k+1}, \cdots, v^n\}$ is a basis for $\mathcal{X}$.

Proof: Previous proposition+Induction

Def. Let $(\mathcal{X}, \mathcal{F}, \langle \cdot, \cdot \rangle)$ be an inner product space, and $S \subseteq \mathcal{X}$ a subset. (Doesn't have to be a subspace.)

$$S^\perp := \{x \in \mathcal{X} | x \perp S\} = \{x \in \mathcal{X} | \langle x, y \rangle = 0 \text{ for all } y \in S\}$$

is called the orthogonal complement of S.

Exercise: $S^\perp$ is always a subspace.

Proposition: Let $(\mathcal{X}, \mathcal{F}, \langle \cdot, \cdot \rangle)$ be a finite dimensional inner product space,

M a subspace of $\mathcal{X}$. Then,

$$\mathcal{X} = M \oplus M^{\perp}.$$

<u>Proof:</u> If $x \in M \cap M^{\perp}$, $\langle x, x \rangle = 0 \Leftrightarrow x = 0$.
Hence, $M \cap M^{\perp} = \{0\}$.

Let $\{y^1, \cdots, y^k\}$ be a basis of M. Complete it to be a basis for $\mathcal{X}$:

$$\{y^1, y^2, \cdots, y^k, y^{k+1}, \cdots, y^n\}$$

Apply G.S. to produce orthogonal vectors $\{v^1, \cdots, v^k, v^{k+1}, \cdots, v^n\}$ such that $\text{span}\{v^1, \cdots, v^k\} = \text{span}\{y^1, \cdots, y^k\} = M$.
An easy calculation gives

$$M^{\perp} = \text{span}\{v^{k+1}, \cdots, v^n\}$$

<u>Why?</u>

$$\begin{aligned}
x &= \alpha_1 v^1 + \cdots + \alpha_k v^k + \alpha_{k+1} v^{k+1} + \cdots + \alpha_n v^n \\
x &\perp M \Leftrightarrow \langle x, v^i \rangle = 0, \quad 1 \le i \le k \\
\langle x, v^i \rangle &= \alpha_1 \underbrace{\langle v^1, v^i \rangle}_{=0} + \cdots + \alpha_i \langle v^i, v^i \rangle + \cdots + \alpha_n \underbrace{\langle v^n, v^i \rangle}_{=0} \\
&= \alpha_i \langle v^i, v^i \rangle \\
&= \alpha_i \|v^i\|^2 \\
\therefore x &= \alpha_{k+1} v^{k+1} + \cdots + \alpha_n v^n \Leftrightarrow x \in \text{span}\{v^{k+1}, \cdots, v^n\}. \\
\therefore x &\in M^{\perp} \Leftrightarrow x \in \text{span}\{v^{k+1}, \cdots, v^n\}.
\end{aligned}$$

Projection Theorem

Theorem: (Classical Projection Theorem)
Let $\mathcal{X}$ be a finite dimensional inner product space and M a subspace of $\mathcal{X}$. Then, $\forall x \in \mathcal{X}, \exists$ unique $m_0 \in M$ such that

$$\|x - m_0\| = d(x, M) = \inf_{m \in M} \|x - m\|.$$

Moreover, m_0 is characterized by $x - m_0 \perp M$.

Proof: To show: m_0 exists. Uniqueness and orthogonality were shown in the Pre-projection Theorem.
From G.S., we learnt that $\mathcal{X} = M \oplus M^\perp$.
Hence, we can write

$$x = m_0 + \tilde{m}$$

where

$$m_0 \in M \quad \text{and} \quad \tilde{m} \in M^\perp$$

Hence,

$$x - m_0 = \tilde{m} \in M \Rightarrow x - m_0 \perp M. \ \Box$$

Rob 501 Handout: Grizzle
Lecture 10
Orthogonal Projection and Normal Equations

Projection Theorem (Continued)

Orthogonal Projection Operator

Let $\mathcal{X}$ be a finite dimensional (real) inner product space and M a subspace of $\mathcal{X}$. For $x \in \mathcal{X}$ and $m_0 \in M$. The Projection Theorem shows the TFAE:

(a) $x - m_0 \perp M$.

(b) $\exists \tilde{m} = M^\perp$ such that $x = m_0 + \tilde{m}$.

(c) $\|x - m_0\| = d(x, M) = \inf\limits_{m \in M} \|x - m\|$.

Def. P: $\mathcal{X} \to M$ by $P(x) = m_0$, where m_0 satisfies any of (a),(b) or (c), is called the orthogonal projection of $\mathcal{X}$ onto M.

Exercise1: P: $\mathcal{X} \to M$ is a linear operator.

Exercise2: P: Let $\{v^1, \cdots, v^k\}$ be an orthonormal basis for M.Then

$$P(x) = \sum_{i=1}^{k} \langle x, v^i \rangle v^i.$$

Normal Equations
Let $\mathcal{X}$ be a finite dimensional (real) inner product space and $M = \text{span}\{y^1, \cdots, y^k\}$, with $\{y^1, \cdots, y^k\}$ linearly independent. Given $x \in \mathcal{X}$, seek $\hat{x} \in M$ such that

$$\|x - \hat{x}\| = d(x, M) = \inf_{m \in M} \|x - m\| = \min_{m \in M} \|x - m\|$$

where we can write "min" because the Projection Theorem assures the existence of a minimizing vector $\hat{x} \in M$.

Notation: $\hat{x} = \operatorname{argmin} d(x, M)$

Remark: One solution is Gram Schmidt and the orthogonal projection operator. We provide an alternative way to compute the answer.

By the Projection Theorem, $\hat{x}$ exists and is characterized by $x - \hat{x} \perp M$. Write

$$\hat{x} = \alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k$$

and impose $x - \hat{x} \perp M \Leftrightarrow x - \hat{x} \perp y^i,\ 1 \leq i \leq k$.

Then, $\langle x - \hat{x}, y^i \rangle = 0, \quad \forall 1 \leq i \leq k$ yields

$$\begin{aligned} &\langle \hat{x}, y^i \rangle = \langle x, y^i \rangle \quad i = 1, 2, \cdots, k \\ \Leftrightarrow &\langle \alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k, y^i \rangle = \langle x, y^i \rangle \quad i = 1, 2, \cdots, k. \end{aligned}$$

We now write this out in matrix form.
$\underline{i = 1}$

$$\alpha_1 \langle y^1, y^1 \rangle + \alpha_2 \langle y^2, y^1 \rangle + \cdots + \alpha_k \langle y^k, y^1 \rangle = \langle x, y^1 \rangle$$

$\underline{i = 2}$

$$\alpha_1 \langle y^1, y^2 \rangle + \alpha_2 \langle y^2, y^2 \rangle + \cdots + \alpha_k \langle y^k, y^2 \rangle = \langle x, y^2 \rangle$$

$$\vdots$$

$\underline{i = k}$

$$\alpha_1 \langle y^1, y^k \rangle + \alpha_2 \langle y^2, y^k \rangle + \cdots + \alpha_k \langle y^k, y^k \rangle = \langle x, y^k \rangle$$

These are called the Normal Equations.

Def. $G = G(y^1, \cdots, y^k) = \begin{bmatrix} \langle y^1, y^1 \rangle & \langle y^1, y^2 \rangle & \cdots & \langle y^1, y^k \rangle \\ \langle y^2, y^1 \rangle & \langle y^2, y^2 \rangle & \cdots & \langle y^2, y^k \rangle \\ \vdots & \vdots & & \vdots \\ \langle y^k, y^1 \rangle & \langle y^k, y^2 \rangle & \cdots & \langle y^k, y^k \rangle \end{bmatrix}$

$G_{ij} = \langle y^i, y^j \rangle$ is called the Gram matrix.

Remark: Because we are assuming $\mathcal{F} = \mathbb{R}$, $\langle y^i, y^j \rangle = \langle y^j, y^i \rangle$, and we therefore have $G = G^T$.

Let $\alpha = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{bmatrix}$, we have

$$G^T \alpha = \beta \text{ (normal equation in the matrix form)}$$

where

$$\beta_i = \langle x, y^i \rangle, \quad \beta = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_k \end{bmatrix}.$$

Def. $g(y^1, y^2, \cdots, y^k)$ =det $G(y^1, \cdots, y^k)$ is the determinant of the Gram Matrix.

Prop. $g(y^1, y^2, \cdots, y^k) \neq 0 \Leftrightarrow \{y^1, \cdots, y^k\}$ is linearly independent.

The proof is given at the end of the handout.

Summary: Here is the solution of our best approximation problem by the normal equations. Assume the set $\{y^1, \cdots, y^k\}$ is linearly independent and $M := \text{span}\{y^1, \cdots, y^k\}$. Then $\hat{x} = \arg\min d(x, M)$ if, and only if,

$$\hat{x} = \alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k$$

$$G^T \alpha = \beta$$

$$G_{ij} = \langle y^i, y^j \rangle$$

$$\beta_i = \langle x, y^i \rangle.$$

Application: Over determined system of linear equations in $\mathbb{R}^n$

$$A\alpha = b,$$

where $A = n \times m$ real matrix, $n \geq m$, $\mathrm{rank}(A) = m$ (columns of A are linearly independent). From the dimension of A, we have that $\alpha \in \mathbb{R}^m, b \in \mathbb{R}^n$.

<u>Original Problem Formulation:</u>
Seek $\hat{\alpha}$ such that

$$\|A\hat{\alpha} - b\| = \min_{\alpha \in \mathbb{R}^m} \|A\alpha - b\|,$$

where

$$\|x\|^2 = \sum_{i=1}^{n} (x_i)^2.$$

<u>Solution:</u>

$$\mathcal{X} = \mathbb{R}^n, \quad \mathcal{F} = \mathbb{R}, \quad \langle x, y \rangle = x^T y = y^T x = \sum_{i=1}^{n} x_i y_i$$

Therefore,

$$\|x\|^2 = \langle x, x \rangle = \sum_{i=1}^{n} |x_i|^2.$$

Write

$$A = [A_1 | A_2 | \cdots | A_m] \text{ and } \alpha = [\alpha_1, \alpha_2, \cdots, \alpha_m]^\top$$

and we note that

$$A\alpha = \alpha_1 A_1 + \alpha_2 A_2 + \cdots \alpha_m A_m.$$

<u>New Problem Formulation:</u>
Seek

$$\hat{x} = A\hat{\alpha} \in \mathrm{span}\{A_1, A_2, \cdots, A_m\} =: M$$

such that

$$\|\hat{x} - b\| = d(b, M) \Leftrightarrow \hat{x} - b \perp M.$$

From the Projection Theorem and the Normal Equations,

$$\hat{x} = \hat{\alpha}_1 A_1 + \hat{\alpha}_2 A_2 + \cdots \hat{\alpha}_m A_m$$

and $G^\top \hat{\alpha} = \beta$, with

$$G_{ij} = \langle A_i, A_j \rangle = A_i^\top A_j$$
$$\beta_i = \langle b, A_i \rangle = b^\top A_i = A_i^\top b.$$

<u>Aside</u>

$$A^\top = \begin{bmatrix} A_1^\top \\ A_2^\top \\ \vdots \\ A_m^\top \end{bmatrix} \qquad A = [A_1 | \cdots | A_m]$$

$$(A^\top A)_{ij} = A_i^\top A_j$$
$$G = G^\top = A^\top A$$
$$(A^\top b)_i = A_i^\top b$$

Normal Equations are

$$A^\top A \hat{\alpha} = A^\top b.$$

From the Proposition, $G^\top = A^\top A$ is invertible $\Leftrightarrow$ columns of A are linearly independent. Hence,

$$\hat{\alpha} = (A^\top A)^{-1} A^\top b.$$

Prop. $g(y^1, y^2, \cdots, y^k) \neq 0 \Leftrightarrow \{y^1, \cdots, y^k\}$ is linearly independent.

Proof: $g(y^1, y^2, \cdots, y^k) = 0 \leftrightarrow \exists \alpha \neq 0$ such that $G^\top \alpha = 0$.

From our construction of the normal equations, $G^\top \alpha = 0$ if, and only if

$$\langle \alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k, y^i \rangle = 0 \quad i = 1, 2, \cdots, k.$$

This is equivalent to

$$\left(\alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k\right) \perp y^i = 0 \quad i = 1, 2, \cdots, k$$

which is equivalent to

$$\left(\alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k\right) \perp \text{span}\{y^1, \cdots, y^k\} =: M$$

and thus

$$\left(\alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k\right) \in M^\perp.$$

Because $\alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k \in M$, we have that

$$\left(\alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k\right) \in M \cap M^\perp$$

and therefore

$$\alpha_1 y^1 + \alpha_2 y^2 + \cdots + \alpha_k y^k = 0.$$

By the linear independence of $\{y^1, \cdots, y^k\}$, we deduce that

$$\alpha_1 = \alpha_2 = \cdots \alpha_k = 0. \ \square$$

Rob 501 Fall 2014
Lecture 11
Typeset by: Su-Yang Shieh
Proofread by: Zhiyuan Zuo
Updated by Grizzle on 8 October 2015

Symmetric Matrices

Def. An $n \times n$ real matrix A is symmetric if $A^\top = A$.

Claim 1: The eigenvalues of a symmetric matrix are real.

Proof: Let $\lambda \in \mathbb{C}$ be an eigenvalue. To show: $\lambda = \bar{\lambda}$ where $\bar{\lambda}$ is the complex conjugate of λ.
Because $\lambda \in \mathbb{C}$ is an eigenvalue, $\exists v \in \mathbb{C}^n$, $v \neq 0$, such that

$$Av = \lambda v.$$

Take the complex conjugate of both sides, yielding

$$\bar{A}\bar{v} = \bar{\lambda}\bar{v}.$$

Because A is real, we have $\bar{A} = A$ and thus

$$A\bar{v} = \bar{\lambda}\bar{v}.$$

Now, take the transpose of both sides to obtain

$$\bar{v}^\top A^\top = \bar{\lambda}\bar{v}^\top.$$

Because A is symmetric, $A^\top = A$, and hence,

$$\begin{aligned} \bar{v}^\top A &= \bar{\lambda}\bar{v}^\top \\ \Rightarrow \bar{v}^\top A v &= \bar{\lambda}\bar{v}^\top v \\ \Rightarrow \bar{v}^\top \lambda v &= \bar{\lambda}\bar{v}^\top v \\ \therefore \lambda \|v\|^2 &= \bar{\lambda}\|v\|^2 \end{aligned}$$

where $\langle x, y\rangle = x^\top \bar{y}$ and $\|x\|^2 = \langle x, x\rangle = x^\top \bar{x} = \bar{x}^\top x$. Because $\|v\|^2 \neq 0$, we deduce that $\lambda = \bar{\lambda}$, proving the result. $\Box$

Remark: We now know that when A is real and symmetric, an eigenvalue λ is real, and therefore we can assume the corresponding eigenvector is real. Indeed,

$$\underbrace{(A - \lambda I)}_{\text{real}} v = 0.$$

Hence we have $v \in \mathbb{R}^n$ and we can use the real inner product on $\mathbb{R}^n$, namely $\langle x, y\rangle = x^\top y$.

Claim 2: Eigenvectors corresponding to distinct eigenvalues are orthogonal. That is, let $\lambda_1, \lambda_2 \in \mathbb{R}, v^1, v^2 \in \mathbb{R}^n, Av^1 = \lambda_1 v^1, Av^2 = \lambda_2 v^2, v^1 \neq 0, v^2 \neq 0$. Then,

$$\lambda_1 \neq \lambda_2 \Rightarrow \langle v^1, v^2\rangle = 0.$$

<u>Proof:</u> $Av^1 = \lambda_1 v^1$.
Take the transpose of both sides, and use $A = A^\top$. Then,

$$\begin{aligned}
&(v^1)^\top A = \lambda_1 (v^1)^\top \\
&(v^1)^\top A v^2 = \lambda_1 (v^1)^\top v^2 \\
&(v^1)^\top \lambda_2 v^2 = \lambda_1 (v^1)^\top v^2 \\
&(\lambda_1 - \lambda_2)(v^1)^\top v^2 = 0 \\
&\lambda_1 \neq \lambda_2, \Rightarrow (v^1)^\top v^2 = 0. \ \Box
\end{aligned}$$

Def.: A matrix Q is orthogonal if $Q^\top Q = I$. That is, $Q^{-1} = Q^\top$.

Claim 3: Suppose the eigenvalues of A are all distinct. Then there exists an orthogonal matrix Q such that

$$Q^\top A Q = \Lambda = \text{diag}(\lambda_1, \cdots, \lambda_n).$$

<u>Proof:</u> $\lambda_1, \cdots, \lambda_n$ distinct implies that the eigenvectors $v_1, \cdots, v_n$ are orthog-

onal, and thus
$$\langle v^i, v^j \rangle = (v^i)^\top v^j = 0 \quad i \neq j.$$
WLOG (without loss of generality), we can assume:$\|v^i\| = 1$
$$\therefore \|v^i\|^2 = 1 \Leftrightarrow (v^i)^\top v^i = \|v^i\|^2 = 1.$$
We define
$$Q = \left[v^1 | v^2 | \cdots | v^n \right]$$
Then
$$\left[Q^\top Q \right]_{ij} = (v^i)^\top v^j = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$
$$\therefore Q^\top Q = I, \text{ is orthogonal. } \square$$

Fact: [See HW06] Even if the eigenvalues are repeated, $A = A^\top \Rightarrow$ $\exists\, Q$ orthogonal such that $Q^\top A Q = \Lambda = \operatorname{diag}(\lambda_1, \cdots, \lambda_n)$. Symmetric matrices are rather special in that one can ALWAYS find a basis consisting of e-vectors.

Useful Observation: Let A be $m \times n$ real matrix. Then both $A^\top A$ and $AA^\top$ are symmetric, and hence their eigenvalues are real.

Claim 4: Eigenvalues of $A^\top A$ and $AA^\top$ are non-negative.

Proof: We do the proof for $A^\top A$.
Let $A^\top A v = \lambda v$ where $v \in \mathbb{R}^n$, $v \neq 0$, $\lambda \in \mathbb{R}$, $v \in \mathbb{R}^n$. To show: $\lambda \geq 0$.
Multiply both sides by $v^\top$
$$\begin{aligned} v^\top A^\top A v &= v^\top \lambda v \\ \langle Av, Av \rangle &= \lambda \langle v, v \rangle \\ \therefore \|Av\|^2 &= \lambda \|v\|^2 \end{aligned}$$
$\therefore \lambda \geq 0,$ because $\|v\|^2 > 0, \|Av\|^2 \geq 0.$ $\square$

Quadratic Forms

Def. Let M be an $n \times n$ real matrix and $x \in \mathbb{R}^n$. Then $x^\top Mx$ is called a quadratic form.

Def. An $n \times n$ matrix W is skew symmetric if $W = -W^\top$.

Exercise: If W is skew symmetric, then $x^\top Wx = 0$ for all $x \in \mathbb{R}^n$.

Exercise: M a real matrix, $M = \underbrace{\dfrac{M + M^\top}{2}}_{\text{symmetric}} + \underbrace{\dfrac{M - M^\top}{2}}_{\text{skew symmetric}}$.

Def. $\frac{M+M^\top}{2}$ is the symmetric part of M.

Exercise: $x^\top Mx = x^\top \left(\frac{M+M^\top}{2}\right) x$.

Consequence: When working with a quadratic form, always assume M is symmetric.

Def. A real symmetric matric P is positive definite, if, for all $x \in \mathbb{R}^n$, $x \neq 0 \Rightarrow x^\top Px > 0$.

Rob 501 Fall 2014
Lecture 12
Typeset by: Yong Xiao
Proofread by: Pedro Donato

Positive Definite Matrices and Schur Complement

Notation: $P > 0$: P is positive definite. (Does not mean all entries of P are positive)

Theorem: A symmetric matrix P is positive definite if and only if all of its eigenvalues are greater than 0.

Proof:
Claim 1: P is positive definite. $\Rightarrow$ All eigenvalues of P are greater than 0.
Proof: Let $\lambda \in \mathbb{R}$, $Px = \lambda x$, $x \neq 0$. (λ is an eigenvalue of P).
Then, we have:

$$x^\top Px = x^\top \lambda x = \lambda \|x\|^2 > 0$$

$\therefore \|x\| > 0 \Rightarrow \lambda > 0$. $\square$

Claim 2: All eigenvalues of P are greater than 0. $\Rightarrow$ P is positive definite.
Proof: To show $x \neq 0 \Rightarrow x^\top Px > 0$.
Without loss of generality, assume $\|x\| = 1$,

$$\therefore x^\top x = 1.$$

$$x^\top Px \geq \min_{x \in \mathbb{R}^n,\ \|x\|=1} x^\top Px = \lambda_{min}(P)$$

where $\lambda_{min}(P)$ is the smallest eigenvalue of P.
Meanwhile, $\lambda_{min}(P) > 0$ because all eigenvalues of P are positive and there is only a finite number of them.

$$\therefore x^\top Px \geq \lambda_{min}(P) > 0. \ \square$$

Exercise: Show

$$P = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix} > 0$$

Definition: $P = P^\top$ is <u>positive semidefinite</u> if $x^\top P x \geq 0$ for all $x \neq 0$.

Theorem: P is <u>positive semidefinite</u> if and only if all eigenvalues of P are non-negative. (Notation: $P \geq 0$ or $P \succcurlyeq 0$.)

Definition: N is a <u>square root of a symmetric matrix</u> P if $N^\top N = P$.
<u>Note:</u> $N^\top N = \left(N^\top N\right)^\top \Rightarrow N^\top N$ is always symmetric.

Theorem: $P \geq 0 \Leftrightarrow \exists N$ such that $N^\top N = P$.
<u>Proof:</u>

1. Suppose $N^\top N = P$, and let $x \in \mathbb{R}^n$.

$$x^\top P x = x^\top N^\top N x = (Nx)^\top (Nx) = \|Nx\|^2 \geq 0.$$

2. Now suppose $P \geq 0$. To show $\exists N$ such that $N^\top N = P$.
   Since P is symmetric, there exists an orthogonal matrix O such that

$$P = O^\top \Lambda O$$

   where $\Lambda = \text{diag}\,(\lambda_1, \lambda_2, \cdots, \lambda_n)$.
   Since $P \geq 0$, $\lambda_i \geq 0$ for all $i = 1, 2, \ldots, n$.
   Define $\Lambda^{1/2} := diag(\sqrt{\lambda_1}, \sqrt{\lambda_2}, \ldots, \sqrt{\lambda_n})$,

$$\Lambda = (\Lambda^{1/2})^\top \Lambda^{1/2} = \Lambda^{1/2}\Lambda^{1/2}.$$

   Let $N = \Lambda^{1/2} O$, then

$$N^\top N = O^\top \left(\Lambda^{1/2}\right)^\top \Lambda^{1/2} O = O^\top \Lambda O = P.$$

$$\therefore N^\top N = P. \ \square$$

Exercise: For a symmetric matrix P, $x, y \in \mathbb{R}^n$, prove $(x+y)^\top P(x+y) = x^\top Px + y^\top Py + 2x^\top Py$. (Because $y^\top Px$ is scalar)

Theorem: (Schur Complement) Suppose that $A = n \times n$ is symmetric and invertible, $B = n \times m$, $C = m \times m$ is symmetric and invertible, and

$$M = \begin{bmatrix} A & B \\ B^\top & C \end{bmatrix}$$

symmetric.

Then the following are equivalent:

1. $M > 0$.
2. $A > 0$, and $C - B^\top A^{-1} B > 0$.
3. $C > 0$, and $A - BC^{-1}B^\top > 0$.

Definition: $C - B^\top A^{-1} B$ is the Schur Complement of A in M.

Definition: $A - BC^{-1}B^\top$ is the Schur Complement of C in M.

Proof: We will show 1. $\Leftrightarrow$ 2.. The proof of 1. $\Leftrightarrow$ 3. is identical.

Firstly, let's show 1. $\Rightarrow$ 2..
Suppose $M > 0$, then for all $x \in \mathbb{R}^n$, $x \neq 0$,

$$\begin{bmatrix} x \\ 0 \end{bmatrix}^\top M \begin{bmatrix} x \\ 0 \end{bmatrix} > 0$$

$$0 < \begin{bmatrix} x \\ 0 \end{bmatrix}^\top \begin{bmatrix} A & B \\ B^\top & C \end{bmatrix} \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} x^\top & 0 \end{bmatrix} \begin{bmatrix} Ax \\ B^\top x \end{bmatrix} = x^\top Ax.$$

$\therefore A$ is positive definite.
We will make a nice choice of $\begin{bmatrix} x \\ y \end{bmatrix}$ to show $C - B^\top A^{-1} B > 0$.

We want $Ax + By = 0$, thus let $x = -A^{-1}By$, $y \neq 0$.

$$\begin{aligned}
0 < \begin{bmatrix} x \\ y \end{bmatrix}^\top \begin{bmatrix} A & B \\ B^\top & C \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} -A^{-1}By \\ y \end{bmatrix}^\top \begin{bmatrix} A & B \\ B^\top & C \end{bmatrix} \begin{bmatrix} -A^{-1}By \\ y \end{bmatrix} \\
&= \begin{bmatrix} -y^\top B^\top A^{-1} & y^\top \end{bmatrix} \begin{bmatrix} 0 \\ -B^\top A^{-1}By + Cy \end{bmatrix} \\
&= y^\top Cy - y^\top B^\top A^{-1}By \\
&= y^\top (C - B^\top A^{-1}B)y.
\end{aligned}$$

$\therefore C - B^\top A^{-1}B > 0$.

Secondly, let's show 2. $\Rightarrow$ 1..
Suppose $A > 0$, $C - B^\top A^{-1}B > 0$. To show $M > 0$.
(Equivalently, to show: for an arbitrary $\begin{bmatrix} x \\ y \end{bmatrix}$, $\begin{bmatrix} x \\ y \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} x \\ y \end{bmatrix}^\top M \begin{bmatrix} x \\ y \end{bmatrix} > 0$)

For an arbitrary $\begin{bmatrix} x \\ y \end{bmatrix}$, define $\bar{x} = x + A^{-1}By$.
Note that $\begin{bmatrix} x \\ y \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Leftrightarrow \begin{bmatrix} \bar{x} \\ y \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

$$\begin{aligned}
\begin{bmatrix} x \\ y \end{bmatrix}^\top M \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} \bar{x} - A^{-1}By \\ y \end{bmatrix}^\top M \begin{bmatrix} \bar{x} - A^{-1}By \\ y \end{bmatrix} \\
&= \begin{bmatrix} \bar{x} \\ 0 \end{bmatrix}^\top M \begin{bmatrix} \bar{x} \\ 0 \end{bmatrix} + \begin{bmatrix} -A^{-1}By \\ y \end{bmatrix}^\top M \begin{bmatrix} -A^{-1}By \\ y \end{bmatrix} + 2 \begin{bmatrix} \bar{x} \\ 0 \end{bmatrix}^\top M \begin{bmatrix} -A^{-1}By \\ y \end{bmatrix} \\
&= \bar{x}^\top A\bar{x} + y^\top (C - B^\top A^{-1}B)y + 0 > 0. \ \square
\end{aligned}$$

Rob 501 Fall 2014
Lecture 13
Typeset by: Ming-Yuan Yu
Proofread by: Ilsun Song

Weighted Least Squares

Let Q be an $n \times n$ positive definite matrix ($Q > 0$)
and let the inner product on $\mathbb{R}^n$ be

$$\langle x, y\rangle = x^\top Q y.$$

We re-do $A\alpha = b$, where $A = n \times m, n \geq m, rank(A) = m, \alpha \in \mathbb{R}^m,$ and $b \in \mathbb{R}^n$. We want to seek $\hat{\alpha}$ such that

$$\|A\hat{\alpha} - b\| = \min_{\alpha \in \mathbb{R}^m} \|A\alpha - b\|$$

where $\|x\| = \langle x, x\rangle^{\frac{1}{2}} = (x^\top Q x)^{\frac{1}{2}}$ and $Q > 0$.

<u>Solution:</u> $\mathcal{X} = \mathbb{R}^n, \mathcal{F} = \mathbb{R}, \langle x, y\rangle = x^\top Q y$
Write $A = \left[\ A_1 \,\middle|\, A_2 \,\middle|\, \cdots \,\middle|\, A_m\ \right]$

<u>Normal Equations:</u>

$$\begin{aligned}
\hat{x} &= \hat{\alpha}_1 A_1 + \hat{\alpha}_2 A_2 + \cdots + \hat{\alpha}_m A_m \\
G^\top \hat{\alpha} &= \beta, \text{ with } G = G^\top \\
[G^\top]_{ij} &= [G]_{ij} = \langle A_i, A_j\rangle = A_i^\top Q A_j = [A^\top Q A]_{ij} \\
\beta_i &= \langle b, A_i\rangle = b^\top Q A_i = A_i^\top Q b = [A^\top Q b]_i.
\end{aligned}$$

$\therefore A^\top Q A \hat{\alpha} = A^\top Q b.$

Since $A^\top Q A$ is invertible by $rank(A) = m$, we can conclude that

$$\underline{\hat{\alpha} = (A^\top Q A)^{-1} A^\top Q b}.$$

Recursive Least Squares

Model:

$$y_i = C_i x + e_i, \; i = 1, 2, 3, \cdots$$

$$\begin{aligned} C_i &\in \mathbb{R}^{m\times n} \\ i &= \text{time index} \\ x &= \text{an unknown } \underline{\text{constant}} \text{ vector} \in \mathbb{R}^n \\ y_i &= \text{measurements} \in \mathbb{R}^m \\ e_i &= \text{model "mismatch"} \in \mathbb{R}^m \end{aligned}$$

Objective 1: Compute a least squared error estimate of x at time k, using all available data at time k, $(y_1, \cdots, y_k)$!

Objective 2: Discover a computationally attractive form for the answer.

Solution:

$$\begin{aligned} \hat{x}_k :&= \underset{x\in\mathbb{R}^n}{\text{argmin}} \left(\sum_{i=1}^{k} (y_i - C_i x)^\top S_i (y_i - C_i x) \right) \\ &= \underset{x\in\mathbb{R}^n}{\text{argmin}} \left(\sum_{i=1}^{k} e_i^\top S_i e_i \right) \end{aligned}$$

where $S_i = m \times m$ positive definite matrix. ($S_i > 0$ for all time index i)

Batch Solution:

$$Y_k = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix}, A_k = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_k \end{bmatrix}, E_k = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix}$$

$$R_k = \begin{bmatrix} S_1 & & & \mathbf{0} \\ & S_2 & & \\ & & \ddots & \\ \mathbf{0} & & & S_k \end{bmatrix} = diag(S_1, S_2, \cdots, S_k) > 0$$

$Y_k = A_k x + E_k$, [model for $1 \le i \le k$]
$\|Y_k - A_k x\|^2 = \|E_k\|^2 := E_k^\top R_k E_k$

Since $\hat{x}_k$ is the value minimizing the error $\|E_k\|$, which is the unexplained part of the model,

$$\hat{x}_k = \underset{x \in \mathbb{R}^n}{\operatorname{argmin}} \|E_k\| = \underset{x \in \mathbb{R}^n}{\operatorname{argmin}} \|Y_k - A_k x\|,$$

which satisfies the Normal Equations $(A_k^\top R_k A_k)\hat{x}_k = A_k^\top R_k Y_k$.

$\therefore \underline{\hat{x}_k = (A_k^\top R_k A_k)^{-1} A_k^\top R_k Y_k}$, which is called a Batch Solution.

Drawback: $A_k = km \times n$ matrix, and grows at each step!

Solution: Find a recursive means to compute $\hat{x}_{k+1}$ in terms of $\hat{x}_k$ and the new measurement y_{k+1}!

Normal equations at time k, $(A_k^\top R_k A_k)\hat{x}_k = A_k^\top R_k Y_k$, is equivalent to

$$\left(\sum_{i=1}^{k} C_i^\top S_i C_i \right) \hat{x}_k = \sum_{i=1}^{k} C_i^\top S_i y_i.$$

We define

$$Q_k = \sum_{i=1}^{k} C_i^\top S_i C_i$$

so that

$$Q_{k+1} = Q_k + C_{k+1}^\top S_{k+1} C_{k+1}.$$

At time $k+1$,

$$\underbrace{(\sum_{i=1}^{k+1} C_i^\top S_i C_i)}_{Q_{k+1}} \hat{x}_{k+1} = \sum_{i=1}^{k+1} C_i^\top S_i y_i$$

or

$$Q_{k+1}\hat{x}_{k+1} = \underbrace{\sum_{i=1}^{k} C_i^\top S_i y_i}_{Q_k\hat{x}_k} + C_{k+1}^\top S_{k+1} y_{k+1}.$$

$\therefore Q_{k+1}\hat{x}_{k+1} = Q_k\hat{x}_k + C_{k+1}^\top S_{k+1} y_{k+1}$

Good start on recursion! Estimate at time $k+1$ expressed as a linear combination of the estimate at time k and the latest measurement at time $k+1$.

Continuing,

$$\hat{x}_{k+1} = Q_{k+1}^{-1}\left[Q_k\hat{x}_k + C_{k+1}^\top S_{k+1} y_{k+1}\right].$$

Because

$$Q_k = Q_{k+1} - C_{k+1}^\top S_{k+1} C_{k+1},$$

we have

$$\hat{x}_{k+1} = \hat{x}_k + \underbrace{Q_{k+1}^{-1} C_{k+1}^\top S_{k+1}}_{\text{Kalman gain}} \underbrace{(y_{k+1} - C_{k+1}\hat{x}_k)}_{\text{Innovations}}.$$

Innovations $y_{k+1} - C_{k+1}\hat{x}_k$ = measurement at time $k+1$ minus the "predicted" value of the measurement = "new information".

In a real-time implementation, computing the inverse of Q_{k+1} can be time consuming. An attractive alternative can be obtained by applying the Matrix Inversion Lemma:

$$(A + BCD)^{-1} = A^{-1} - A^{-1}B\left(DA^{-1}B + C^{-1}\right)^{-1} DA^{-1}$$

Now, following the substitution rule as shown below,

$$A \leftrightarrow Q_k \quad B \leftrightarrow C_{k+1}^\top \quad C \leftrightarrow S_{k+1} \quad D \leftrightarrow C_{k+1},$$

we can obtain that

$$\begin{aligned} Q_{k+1}^{-1} &= \left(Q_k + C_k^\top S_{k+1} C_{k+1}\right)^{-1} \\ &= Q_k^{-1} - Q_k^{-1} C_{k+1}^\top \left[C_{k+1} Q_k^{-1} C_{k+1}^\top + S_{k+1}^{-1}\right]^{-1} C_{k+1} Q_k^{-1}, \end{aligned}$$

which is a recursion for Q_k^{-1}!

Upon defining

$$P_k = Q_k^{-1},$$

we have

$$P_{k+1} = P_k - P_k C_{k+1}^\top \left[C_{k+1} P_k C_{k+1}^\top + S_{k+1}^{-1}\right]^{-1} C_{k+1} P_k$$

We note that we are now inverting a matrix that is $m \times m$, instead of one that is $n \times n$. Typically, $n > m$, sometimes by a lot!

Rob 501 Fall 2014
Lecture 14
Typeset by: Bo Lin
Proofread by: Hiroshi Yamasaki
Revised: 28 October 2015

Weighted Least Square

We suppose the inner product on $\mathbb{R}^n$ is defined by $< x, y >= x^\top Sy$, where S is an $n \times n$ positive definite matrix. We denote the corresponding norm by $\|x\|_S := (x^\top Sx)^{1/2}$.

Overdetermined Equation:
Let $Ax = b$, where $x \in \mathbb{R}^n$, $b \in \mathbb{R}^m$, $A = m \times n$, $n < m$, and $\text{rank}(A) = n$. Then, we conclude that $\hat{x} = \left(A^\top SA\right)^{-1} A^\top Sb$, where $\hat{x} = \underset{Ax=b}{\text{argmin}}\|x\|_S$.

Underdetermined Equation:
Let $Ax = b$, where $x \in \mathbb{R}^n$, $b \in \mathbb{R}^m$, $A = m \times n$, $n > m$, and $\text{rank}(A) = m$. In other words, we are assuming the rows of A are linearly independent instead of the columns of A are linearly independent.

Def. If $\forall b_0 \in \mathbb{R}^m, \exists x_0 \in \mathbb{R}^n$, such that $b_0 = Ax_0$, $b = Ax$ is consistent.

Fact: If $\text{rank}(A) =$ the number of rows, then the equation $b = Ax$ is consistent.

Fact: Suppose x_0 is such that $b_0 = Ax_0$, and $V = \{x \in \mathbb{R}^n | y = Ax\}$ is the set of solutions. Then, $V = x_0 + \mathcal{N}(A)$, where $\mathcal{N}(A) = \{x \in \mathbb{R}^n | Ax = 0\}$ is the null space of A. Therefore, V is the translate of a subspace. We can also say that V is an "affine" space.

Theorem: If the rows of A are linearly independent, then

$$\hat{x} := \underset{x \in V}{\text{argmin}}\|x\|_S = \underset{Ax=b}{\text{argmin}}\|x\|_S = \underset{Ax=b}{\text{argmin}}(x^\top Sx)^{\frac{1}{2}}$$

exists, is unique, and is given by

$$\hat{x} = S^{-1}A^\top \left(AS^{-1}A^\top\right)^{-1} b.$$

Best Linear Unbiased Estimator (BLUE)

Let $y = Cx + \epsilon$, $y \in \mathbb{R}^m$, $x \in \mathbb{R}^n$, $E\{\epsilon\} = 0$, $\mathrm{cov}\{\epsilon, \epsilon\} = E\{\epsilon\epsilon^\top\} = Q > 0$. We assume no stochastic (random) model for the unknown x. We also assume that columns of C are linearly independent.
Seek: $\hat{x} = Ky$ that minimizes $E\{\|\hat{x} - x\|^2\} = E\{\sum\limits_{i=1}^{n} |\hat{x}_i - x_i|^2\}$ where $\|\cdot\|$ is the standard Euclidean norm on $\mathbb{R}^n$.

<u>Aside:</u>

$$\begin{aligned}(v+w)^\top(v+w) &= v^\top v + w^\top w + v^\top w + w^\top v \\ &= \|v\|^2 + \|w\|^2 + 2v^\top w \text{ (Because } v^\top w \text{ is a scalar.)}\end{aligned}$$

$$\begin{aligned}\therefore E\{\|\hat{x} - x\|^2\} &= E\{\|Ky - x\|^2\} \\ &= E\{\|KCx + K\epsilon - x\|^2\} \\ &= E\{(KCx - x + K\epsilon)^\top(KCx - x + K\epsilon)\} \\ &= E\{(KCx - x)^\top(KCx - x) + 2(K\epsilon)^\top(KCx - x) + \epsilon^\top K^\top K\epsilon\}\end{aligned}$$

From $E\{\epsilon\} = 0$ and x is deterministic, we have

$$2E\{(K\epsilon)^\top(KCx - x)\} = 0.$$

Moreover, by using the properties of the trace, we have

$$\epsilon^\top K^\top K\epsilon = \mathrm{tr}\left(\epsilon^\top K^\top K\epsilon\right) = \mathrm{tr}\left(K\epsilon\epsilon^\top K^\top\right).$$

$$\begin{aligned}\therefore E\{\|x - \hat{x}\|^2\} &= \|KCx - x\|^2 + \mathrm{tr}\, E\{K\epsilon\epsilon^\top K^\top\} \\ &= \|KCx - x\|^2 + \mathrm{tr}(KQK^\top).\end{aligned}$$

<u>Difficulty:</u> Optimal K depends on the unknown x through $\|KCx - x\|^2$!

<u>Observation:</u> If $KC = I$, then the problematic term disappears, i.e.,

$$\|KCx - x\|^2 = 0.$$

<u>Interpretation:</u> Estimator is <u>unbiased</u>.

$$\begin{aligned} E\{\hat{x}\} &= E\{Ky\} \\ &= E\{KCx + K\epsilon\} \\ &= KCx \\ &= x. \qquad \text{(if } KC = I\text{)} \end{aligned}$$

<u>New Problem:</u>

$$\hat{K} = \operatorname{argmin}\{\operatorname{tr}(KQK^\top)\} \text{ subject to } KC = I.$$

<u>New Observation:</u>

Write $K = \begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{bmatrix}$ (partition K by rows).

Then, $K^\top = \left[k_1^\top | k_2^\top | \cdots | k_n^\top\right]$

$$\begin{aligned} \operatorname{tr}\left(\begin{bmatrix} \underline{k_1} \\ \vdots \\ \overline{k_n} \end{bmatrix} Q \left[k_1^\top | \cdots | k_n^\top\right] \right) &= \sum_{i=1}^n k_i Q k_i^\top \\ &= \sum_{i=1}^n \|k_i^\top\|_Q^2 \end{aligned}$$

$$\begin{aligned} KC = I &\Leftrightarrow C^\top K^\top = I_{n\times n} \\ &\Leftrightarrow C^\top \left[k_1^\top | \cdots | k_n^\top\right] = \left[e_1 | \cdots | e_n\right] \\ &\Leftrightarrow C^\top k_i^\top = e_i \quad 1 \le i \le n. \end{aligned}$$

$\therefore$ We have n-separate optimization problems involving the column vectors $k_i^\top$.

$$\hat{k_i}^\top = \operatorname{argmin} \|k_i^\top\|_Q^2 \text{ subject to } C^\top k_i^\top = e_i.$$

From our formula for under determined equations, we have
$\therefore \hat{k}_i^\top = Q^{-1}C(C^\top Q^{-1}C)^{-1}e_i$, which yields
$\therefore \hat{K}^\top = [\hat{k}_1^\top|\cdots|\hat{k}_n^\top] = Q^{-1}C(C^\top Q^{-1}C)^{-1}$.
Therefore,

$$\underline{\hat{K} = (C^\top Q^{-1}C)^{-1}C^\top Q^{-1}}$$

Theorem: Let $x \in \mathbb{R}^n$, $y \in \mathbb{R}^m$, $y = Cx + \epsilon$, $E\{\epsilon\} = 0$, $E\{\epsilon\epsilon^\top\} =: Q > 0$, and $\mathrm{rank}(C) = n$. The Best Linear Unbiased Estimator (BLUE) is $\hat{x} = \hat{K}y$ where

$$\hat{K} = \left(C^\top Q^{-1}C\right)^{-1} C^\top Q^{-1}.$$

Moreover, the covariance of the error is

$$E\{(\hat{x} - x)(\hat{x} - x)^\top\} = \left(C^\top Q^{-1}C\right)^{-1}.$$

Remark: Error covariance computation is an exercise. Solution (from previous calculations)

$$\begin{aligned} E\{(\hat{x} - x)(\hat{x} - x)^\top\} &= KQK^\top \\ &= \left(C^\top Q^{-1}C\right)^{-1} C^\top Q^{-1}QQ^{-1}C\left(C^\top Q^{-1}C\right)^{-1} \\ &= \left(C^\top Q^{-1}C\right)^{-1}\left[C^\top Q^{-1}C\right]\left(C^\top Q^{-1}C\right)^{-1} \\ &= \left(C^\top Q^{-1}C\right)^{-1} \end{aligned}$$

<u>Indeed</u>

$$\begin{aligned} \hat{x} - x &= Ky - x \\ &= KCx + K\epsilon - x \\ &= K\epsilon \text{ (because } KC = I) \\ \therefore E\{(\hat{x} - x)(\hat{x} - x)^\top\} &= E\{(K\epsilon)(K\epsilon)^\top\} \\ &= E\{K\epsilon\epsilon^\top K^\top\} \\ &= KQK^\top \end{aligned}$$

Remarks:

- Comparing Weighted Least Squares to BLUE, we see that they are identical when the weighting matrix is taken as the inverse of the covariance matrix of the noise term: $S = Q^{-1}$.
- Another way to say this, if you solve a least squares problem with weight matrix S, you are implicitly assuming that your uncertainty in the measurements has zero mean and a covariance matrix of $Q = S^{-1}$.
- If you know the uncertainty has zero mean and a covariance matrix of Q, using $S = Q^{-1}$ makes a lot of sense! For simplicity, assume that Q is diagonal. A large entry of Q means high variance, which means the measurement is highly uncertain. Hence, the corresponding component of y should not be weighted very much in the optimization problem....and indeed, taking $S = Q^{-1}$ does just that because, the weight term S is small for large terms in Q.
- The inverse of the covariance matrix is sometimes called the *information* matrix. Hence, there is low information when the variance (or covariance) is large!
- Wow! We do all this abstract math, and the answer makes sense!

Rob 501 Fall 2014
Lecture 15
Typeset by: Connie Qiu
Proofread by: Bo Lin
Revised by Grizzle on 29 October 2015

Minimum Variance Estimator

$$y = Cx + \epsilon, y \in \mathbb{R}^m, x \in \mathbb{R}^n, \text{and } \epsilon \in \mathbb{R}^m.$$

Stochastic assumptions:

$E\{x\} = 0, E\{\epsilon\} = 0$ (means).

$E\{\epsilon\epsilon^\top\} = Q, E\{xx^\top\} = P, E\{\epsilon x^\top\} = 0$ (covariances).

Remark: $E\{\epsilon x^\top\} = 0$ implies that the states and noise are uncorrelated. Recall that uncorrelated does NOT imply independence, except for Gaussian random variables.

Assumptions: $Q \geq 0, P \geq 0, CPC^\top + Q > 0$. (will see why later)

Objective: minimize the variance

$$E\{\|\hat{x} - x\|^2\} = E\{\sum_{i=1}^{n}(\hat{x}_i - x_i)^2\} = \sum_{i=1}^{n} E\{(\hat{x}_i - x_i)^2\}.$$

We see that there are n separate optimization problems.

Remark: suppose $\hat{x} = Ky$. It is automatically unbiased, because

$$E\{\hat{x}\} = E\{Ky\} = E\{KCx + K\epsilon\} = KCE\{x\} + KE\{\epsilon\} = 0 = E\{x\}$$

Problem Formulation: We will pose this as a minimum norm problem in a vector space of random variables.

$$\mathcal{F} = \mathbb{R},$$

$$\mathcal{X} = span\{x_1, x_2, \ldots, x_n, \epsilon_1, \epsilon_2, \ldots, \epsilon_m\},$$

where

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \quad \text{and} \quad \epsilon = \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_m \end{bmatrix}.$$

For $z_1, z_2 \in \mathcal{X}$, we define their inner product by:

$$< z_1, z_2 >= E\{z_1 z_2\}$$

$M = span\{y_1, y_2, \ldots, y_m\} \subset \mathcal{X}$ (measurements),

$y_i = C_i x + \epsilon_i = \sum\limits_{j=1}^{n} C_{ij} x_j + \epsilon_i, 1 \le i \le m$, ($i$-th row of y)

$\hat{x}_i = \arg\min\limits_{m \in M} \|x_i - m\| = d(x, M)$.

Fact: $\{y_1, y_2, \ldots, y_m\}$ is linearly independent if, and only if, $CPC^\top + Q$ is positive definite. This is proven below when we compute the Gram matrix. (Recall, $\{y_1, y_2, \ldots, y_m\}$ linearly independent if, and only if G is full rank, where $G_{ij} :=< y_i, y_j >$.)

Solution via the Normal Equations

By the normal equations,

$$\hat{x}_i = \hat{\alpha}_1 y_1 + \hat{\alpha}_2 y_2 + \cdots + \hat{\alpha}_m y_m$$

where $G^\top \hat{\alpha} = \beta$.

$$\begin{aligned}
G_{ij} = < y_i, y_j >= E\{y_i y_j\} &= E\{[C_i x + \epsilon_i][C_j x + \epsilon_j]\} \\
&= E\{[C_i x + \epsilon_i][C_j x + \epsilon_j]^\top\} \\
&= E\{[C_i x + \epsilon_i][x^\top {C_j}^\top + \epsilon_j]\} \\
&= E\{C_i x x^\top C_j^\top\} + E\{C_i x \epsilon_j\} + E\{\epsilon_i x^\top C_j^\top\} + E\{\epsilon_i \epsilon_j\} \\
&= C_i E\{x x^\top\} C_j^\top + E\{\epsilon_i \epsilon_j\} \\
&= C_i P C_j^\top + Q_{ij} \\
&= [CPC^\top + Q]_{ij}
\end{aligned}$$

where we have used the fact that x and ϵ are uncorrelated. We conclude that

$$G = CPC^\top + Q.$$

We now turn to computing β. Let's note that x_i, the i-th component of x is equal to $x^\top e_i$, where e_i is the standard basis vector in $\mathbb{R}^n$.

$$\begin{aligned}
\beta_j = < x_i, y_j > &= E\{x_i y_j\} \\
&= E\{x_i [C_j x + \epsilon_j]\} \\
&= E\{x_i C_j x\} + E\{x_i \epsilon_j\} \\
&= C_j E\{x x_i\} \\
&= C_j E\{x x^\top e_i\} \\
&= C_j E\{x x^\top\} e_i \\
&= C_j P e_i \\
&= C_j P_i
\end{aligned}$$

where $P = [P_1 | P_2 | \ldots | P_n]$.

Putting all this together, we have

$$
\begin{aligned}
G^\top \hat{\alpha} &= \beta \\
&\Updownarrow \\
[CPC^\top + Q]\hat{\alpha} &= CP_i \\
&\Updownarrow \\
\hat{\alpha} &= [CPC^\top + Q]^{-1} CP_i
\end{aligned}
$$

$\hat{x}_i = \hat{\alpha}_1 y_1 + \hat{\alpha}_2 y_2 + \cdots + \hat{\alpha}_m y_m = \hat{\alpha}^\top y =$ (row vector $\times$ column vector.)

$$
\hat{\alpha} = \begin{bmatrix} \hat{\alpha}_1 \\ \vdots \\ \hat{\alpha}_m \end{bmatrix}.
$$

We now seek to identify the gain matrix K so that

$$
\hat{x} = Ky \Leftrightarrow \hat{x}_i = K_i y, \text{where} \;\; K = \begin{bmatrix} K_1 \\ \hline K_2 \\ \hline \vdots \\ \hline K_n \end{bmatrix};
$$

that is, K_i is the i-th row of K.

$$
\begin{aligned}
K_i^\top = \hat{\alpha} &= [CPC^\top + Q]^{-1} CP_i \\
[K_1^\top | \dots | K_n^\top] &= [CPC^\top + Q]^{-1} CP \\
K &= PC^\top [CPC^\top + Q]^{-1}
\end{aligned}
$$

$$
\boxed{\hat{x} = Ky = PC^\top [CPC^\top + Q]^{-1} y}
$$

Remarks:

1. Exercise: $E\{(\hat{x}-x)(\hat{x}-x)^\top\} = P - PC^\top[CPC^\top + Q]^{-1}CP$
2. The term $PC^\top[CPC^\top + Q]^{-1}CP$ represents the "value" of the measurements. It is the reduction in the variance of x given the measurement y.
3. If $Q > 0$ and $P > 0$, then from the Matrix Inversion Lemma

   $$\boxed{\hat{x} = Ky = [C^\top Q^{-1}C + P^{-1}]^{-1}C^\top Q^{-1}y.}$$

   This form of the equation is useful for comparing BLUE vs MVE
4. <u>BLUE vs MVE</u>

   - **BLUE:** $\hat{x} = [C^\top Q^{-1}C]^{-1}C^\top Q^{-1}y$
   - **MVE:** $\hat{x} = [C^\top Q^{-1}C + P^{-1}]^{-1}C^\top Q^{-1}y$
   - Hence, BLUE = MVE when $P^{-1} = 0$.
   - $P^{-1} = 0$ roughly means $P = \infty I$, that is infinite covariance in x, which in turn means *no idea* about how x is distributed!
   - For BLUE to exist, we need $\dim(y) \geq \dim(x)$
   - For MVE to exist, we can have $\dim(y) < \dim(x)$ as long as

     $$(CPC^\top + Q) > 0$$

Solution to Exercise

We seek $E\{(\hat{x}-x)(\hat{x}-x)^\top\}$ To get started, let's note that

$$\hat{x}-x = Ky - x = KCx + K\epsilon - x = (KC-I)x + K\epsilon$$

and thus

$$(\hat{x}-x)(\hat{x}-x)^\top = (KC-I)xx^\top(KC-I)^\top + K\epsilon\epsilon^\top K^\top - 2(KC-I)x\epsilon^\top K^\top$$

Taking expectations, and recalling that x and ϵ are uncorrelated, we have

$$\begin{aligned} E\{(\hat{x}-x)(\hat{x}-x)^\top\} &= (KC-I)P(KC-I)^\top + KQK^\top \\ &= KCPC^\top K^\top + P - 2PC^\top K^\top + KQK^\top \\ &= P + K[CPC^\top + Q]K^\top - 2PC^\top K^\top \end{aligned}$$

substituting with $K = PC^\top[CPC^\top + Q]^{-1}$ and simplifying yields the result.

Solution to MIL

We will show that if $Q > 0$ and $P > 0$, then

$$PC^\top[CPC^\top + Q]^{-1} = [C^\top Q^{-1}C + P^{-1}]^{-1}C^\top Q^{-1}$$

MIL: Suppose that A, B, C and D are compatible[1] matrices. If A, C, and $(C^{-1} + DA^{-1}B)$ are each square and invertible, then $A + BCD$ is invertible and

$$(A + BCD)^{-1} = A^{-1} - A^{-1}B(C^{-1} + DA^{-1}B)^{-1}DA^{-1}$$

We apply the MIL to $[C^\top Q^{-1}C + P^{-1}]^{-1}$, where we identify $A = P^{-1}, B = C^\top, C = Q^{-1}, D = C$. This yields

$$[C^\top Q^{-1}C + P^{-1}]^{-1} = P - PC^\top[Q + CPC^\top]^{-1}CP$$

Hence

$$\begin{aligned}
[C^\top Q^{-1}C + P^{-1}]^{-1}C^\top Q^{-1} &= PC^\top Q^{-1} - PC^\top[Q + CPC^\top]^{-1}CPC^\top Q^{-1} \\
&= PC^\top \left[I - [Q + CPC^\top]^{-1}CPC^\top\right] Q^{-1} \\
&= PC^\top \left[[Q+CPC^\top]^{-1}[Q+CPC^\top] - [Q+CPC^\top]^{-1}CPC^\top\right] Q^{-1} \\
&= PC^\top[Q + CPC^\top]^{-1} \left[[Q + CPC^\top] - CPC^\top\right] Q^{-1} \\
&= PC^\top[Q + CPC^\top]^{-1} \left[Q + CPC^\top - CPC^\top\right] Q^{-1} \\
&= PC^\top[Q + CPC^\top]^{-1} [Q]\, Q^{-1} \\
&= PC^\top[Q + CPC^\top]^{-1}
\end{aligned}$$

[1] The sizes are such the matrix products and sum in $A + BCD$ make sense.

Rob 501 Fall 2014
Lecture 16
Typeset by: Kurt Lundeen
Proofread by: Connie Qiu
Revised by Ni on 6 November 2015

Matrix Factorizations

QR Decomposition or Factorization: Let A be a real $m \times n$ matrix with linearly independent columns (rank of $A = n = \#$ columns). Then there exist an $m \times n$ matrix Q with orthonormal columns and an upper triangular $n \times n$ matrix R such that

$$A = QR.$$

Notes:

1) $Q^\top Q = I_{n\times n}$

2) $[R]_{ij} = 0, \text{for } i < j,\ R = \begin{bmatrix} r_{11} & \cdots & \cdots & r_{1n} \\ \vdots & r_{22} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & r_{nn} \end{bmatrix}$

3) Columns of A linearly independent $\Leftrightarrow$ R is invertible

Utility of QR Decomposition:

1) Suppose $Ax = b$ is overdetermined with columns of A linearly independent.

Write $A = QR$ and consider

$$\begin{aligned} A^\top A\hat{x} &= A^\top b \\ A^\top A &= R^\top Q^\top QR = R^\top R \\ A^\top b &= R^\top Q^\top b \\ \therefore \quad R^\top R\hat{x} &= R^\top Q^\top b \\ R\hat{x} &= Q^\top b \qquad \text{(because } R \text{ is invertible)} \end{aligned}$$

$\therefore$ Solve for $\hat{x}$ by back substitution using triangular nature of R.
For example, when $n = 3$

$$\left[\begin{bmatrix} r_{11} & r_{12} & r_{13} \\ 0 & r_{22} & r_{23} \\ 0 & 0 & r_{33} \end{bmatrix}\right] \hat{x} = Q^\top b$$

Then, $\hat{x}_3$ to $\hat{x}_1$ can be obtained easily without using the matrix inversion.

2) Suppose $Ax = b$ is under determined with rows of A linearly independent.
<u>Recall:</u> $\hat{x} = A^\top(AA^\top)^{-1}b$ is x of smallest norm satisfying $Ax = b$.
$A^\top$ has linearly independent columns.
$\therefore A^\top = QR,\ Q^\top Q = I,\ R$ is upper triangular and invertible.

$$\begin{aligned} AA^\top &= R^\top Q^\top QR = R^\top R \\ \hat{x} &= QR(R^\top R)^{-1}b \\ &= QRR^{-1}(R^\top)^{-1}b \\ \hat{x} &= Q(R^\top)^{-1}b \end{aligned}$$

Computation of QR Factorization:

<u>Gram Schmidt with Normalization:</u>

$A = [A_1|A_2|\cdots|A_n], \quad A_i \in \mathbb{R}^m, \quad \langle x, y\rangle = x^\top y.$

For $1 \le k \le n$, $\{A_1,\ A_2,\ \cdots,\ A_n\} \to \{v_1,\ v_2,\ \cdots,\ v_n\}$

by

$$
\begin{aligned}
v^1 &= \frac{A_1}{\|A_1\|};\\
v^2 &= A_2 - \langle A_2, v^1\rangle v^1;\\
v^2 &= \frac{v^2}{\|v^2\|};\\
&\vdots\\
v^k &= A_k - \langle A_k, v^1\rangle v^1 - \langle A_k, v^2\rangle v^2 - \cdots - \langle A_k, v^{k-1}\rangle v^{k-1};\\
v^k &= \frac{v^k}{\|v^k\|};
\end{aligned}
$$

For $k = 1 : n$
    $v^k = A_k$
    For $j = 1 : k-1$
        $v^k = v^k - \langle A_k, v^j\rangle v^j$
    End
    $v^k = \frac{v^k}{\|v^k\|}$
End
$Q = [v^1|v^2|\cdots|v^n]$ has orthonormal columns, and hence $Q^\top Q = I_{n\times n}$ because $[Q^\top Q]_{ij} = \langle v^i, v^j\rangle = \delta_{ij}$.

What about R?
$A_i \in \text{span}\{v^1, \cdots, v^i\}$
$A_i = \langle A_1, v^1\rangle v^1 + \langle A_2, v^2\rangle v^2 + \cdots + \langle A_i, v^i\rangle v^i$
We define $R_i = \begin{bmatrix} \langle A_1, v^1\rangle \\ \vdots \\ \langle A_i, v^i\rangle \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, where the value becomes 0 in R_i from the $(i+1)$-th element to the n-th element.
$\therefore QR_i = A_i \Leftrightarrow QR = A$

Modified Gram Schmidt Algorithm:

We have been using the classical Gram-Schmidt Algorithm. It behaves poorly under round-off error.

Here is a standard example:

$$y^1 = \begin{bmatrix} 1 \\ \varepsilon \\ 0 \\ 0 \end{bmatrix}, y^2 = \begin{bmatrix} 1 \\ 0 \\ \varepsilon \\ 0 \end{bmatrix}, y^3 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \varepsilon \end{bmatrix}, \varepsilon > 0$$

Let $\{e^1, e^2, e^3, e^4\}$ be the standard basis vectors $\left(\text{Yes, } (e^i_j) = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}\right)$

We note that

$$\begin{aligned} y^2 &= y^1 + \varepsilon(e^3 - e^2) \\ y^3 &= y^2 + \varepsilon(e^4 - e^3) \end{aligned}$$

and thus

$$\begin{aligned} \text{span}\{y^1, y^2\} &= \text{span}\{y^1, (e^3 - e^2)\} \\ \text{span}\{y^1, y^2, y^3\} &= \text{span}\{y^1, (e^3 - e^2), (e^4 - e^3)\} \end{aligned}$$

Then, GS applied to $\{y^1, y^2, y^3\}$ and $\{y^1, (e^3 - e^2), (e^4 - e^3)\}$ should produce the same orthonormal vectors.

We go to MATLAB, and for $\varepsilon = 0.1$, we do indeed get the same results. See MATLAB.

But with $\varepsilon = 10^{-8}$,

$$\|Q_1 - Q_2\| = 0.5$$

Initial data $\{y^1, \cdots, y^n\}$ linearly independent.

For $k = 1 : n$

  $v^k = y^k$

end

For $i = 1 : n$

  $v^i = \frac{v^i}{\|v^i\|}$

  For $j = i + 1 : n$

    $v^j = v^j - \langle v^i, v^j \rangle v^i$

end
end

Rob 501 Fall 2014
Lecture 17
Typeset by: Joshua Mangelson
Proofread by: Katie Skinner
Revised by Ni on Nov. 20, 2015

Singular Value Decomposition

We will use the SVD (Singular Value Decomposition) to understand "numerical" rank of a matrix, "numerical linear independence", etc.

Def. Rectangular diagonal matrix: Σ is an $m \times n$ matrix.

a) $m > n \quad \Sigma = \begin{bmatrix} S \\ 0 \end{bmatrix}$, S is an $n \times n$ diagonal matrix

b) $m < n \quad \Sigma = \begin{bmatrix} S & 0 \end{bmatrix}$, S is an $m \times m$ diagonal matrix

Diagonal of Σ is equal to diagonal of S.
Another way to say Rectangular Diagonal Matrix is $[\Sigma]_{ij} = 0$ for $i \neq j$.

SVD Theorem: Any $m \times n$ $\mathbb{R}$ matrix A can be factorized as $A = Q_1 \Sigma Q_2^\top$, where Q_1 is an $m \times m$ orthogonal matrix, Q_2 is an $n \times n$ orthogonal matrix, Σ is an $m \times n$ rectangular diagonal matrix, and diagonal of Σ diag$(\Sigma) = [\sigma_1, \sigma_2, \cdots, \sigma_k]$, which satisfies $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_k \geq 0$, where $k = \min(n, m)$. Moreover, the columns of Q_1 are eigenvectors of $AA^\top$, the columns of Q_2 are eigenvectors of $A^\top A$, and $(\sigma_1^2, \sigma_2^2, \cdots, \sigma_k)^2$ are eigenvalues of $A^\top A$ and $AA^\top$.

Remark: The entries of diag(Σ) are called singular values.

Generalizes decomposition of symmetric matrix.

$$P = O\Lambda O^\top$$

Projection process embedded in SVD: Interpret SVD in the case of over-determined system of equations.

$$Y = Ax, \quad Y \in \mathbb{R}^m, \quad X \in \mathbb{R}^n, \quad A \in \mathbb{R}^{m\times n}$$

where rank$(A) = n$ $(m > n)$, $A = Q_1 \Sigma Q_2^\top$, $\Sigma = \begin{bmatrix} S \\ 0 \end{bmatrix}$, S is an $n \times n$ diagonal matrix.

$$\begin{aligned}
A^\top A &= Q_2 \Sigma^\top Q_1^\top Q_1 \Sigma Q_2^\top \\
&= Q_2 \begin{bmatrix} S & 0 \end{bmatrix} Q_1^\top Q_1 \begin{bmatrix} S \\ 0 \end{bmatrix} Q_2^\top \\
&= Q_2 \begin{bmatrix} S & 0 \end{bmatrix} I \begin{bmatrix} S \\ 0 \end{bmatrix} Q_2^\top \\
&= Q_2 S^2 Q_2^\top \\
A^\top Y &= Q_2 \begin{bmatrix} S & 0 \end{bmatrix} Q_1^\top Y \\
\tilde{Y} &= Q_1^\top Y = \begin{bmatrix} \tilde{Y}_1 \\ \tilde{Y}_2 \end{bmatrix}, \quad \tilde{Y}_1 \in \mathbb{R}^n, \quad \tilde{Y}_2 \in \mathbb{R}^{m\times n} \\
A^\top Y &= Q_2 \begin{bmatrix} S & 0 \end{bmatrix} \tilde{Y} \\
&= Q_2 \begin{bmatrix} S & 0 \end{bmatrix} \begin{bmatrix} \tilde{Y}_1 \\ \tilde{Y}_2 \end{bmatrix} \\
&= Q_2 S \tilde{Y}_1
\end{aligned}$$

Projection! Notice how $\tilde{Y}_2$ gets multiplied by 0, in the last line above. Here we are throwing away the orthogonal parts.

We decomposed Y into part in column span of A, $\tilde{Y}_1$, and a part not in the span $\tilde{Y}_2$.

$$\begin{aligned} & Ax = Y \\ \Rightarrow\ & A^\top A\hat{x} = A^\top Y \\ \Rightarrow\ & Q_2 S^2 Q_2^\top \hat{x} = Q_2 S \tilde{Y}_1 \\ \Rightarrow\ & S^2 Q_2^\top \hat{x} = S\tilde{Y}_1 \text{ (rank}(A) = \#\text{ columns} \Rightarrow S \text{ invertible.)} \\ \Rightarrow\ & S Q_2^\top \hat{x} = \tilde{Y}_1 \end{aligned}$$

$\therefore \hat{x} = Q_2 S^{-1} \tilde{Y}_1$

Remarks:

- Q_2 only rotates, no scaling.
- Only S^{-1} scales.
- If S has small elements, elements of S^{-1} are big. Therefore, $\hat{x}$ is too sensitive to the noise perturbation in measurements.

Hermitian of X: Consider $x \in \mathbb{C}^n$. Then we define the vector "x Hermitian" by $x^H := \bar{x}^\top$. That is, x^H is the complex conjugate transpose of x. Similarly, for a matrix $A \in \mathbb{C}^{m\times n}$, we define $A^H \in \mathbb{C}^{n\times m}$ by $\bar{A}^\top$. We say that a square matrix $A \in \mathbb{C}^{n\times n}$ is a <u>Hermitian matrix</u> if $A = A^H$.

Another common way to write the SVD:

$$A = \begin{cases} U \begin{bmatrix} \Sigma \\ 0 \end{bmatrix} V^H, & m > n \\ U \begin{bmatrix} \Sigma & 0 \end{bmatrix} V^H, & m < n \end{cases}$$

Unitary Matrix: A matrix $U \in \mathbb{C}^{n\times n}$ is <u>unitary</u> if $U^H U = U U^H = I_n$.

Numerical Rank: numerical rank$(A) = \#$ of nonzero singular values larger than a threshold.

Fact: The <u>numerical rank</u> of A is the number of singular values that are larger than a given threshold. Often the threshold is chosen as a percentage of the largest singular value.

Rob 501 Fall 2014
Lecture 18
Lecture: Random Vector
Typeset by: Xianan Huang
Proofread by: Josh Mangelson
Revised by Grizzle 10 Nov 2015

Probability Review

1 Random Variables

I will assume known the definition of a probability space, a set of events, and random variable. My scanned lecture notes are attached at the end of this handout.

Given: $(\Omega, \mathscr{F}, P)$ a probability space

$X : \Omega \to R$ random variable

2 Random Vectors

Def. A random vector is a function $X : \Omega \to \mathbb{R}^p$ where each component of $X = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_p \end{pmatrix}$ is a random variable, that is, $X_i : \Omega \to \mathbb{R}$ for $1 \leq i \leq p$.

Assumption: $\forall x \in \mathbb{R}^p$, the set $\{\omega \in \Omega \mid X(\omega) \leq x\} \in \mathscr{F}$ where the inequality is understood pointwise, that is,

$$\{\omega \in \Omega \mid X(\omega) \leq x\} = \bigcap_{i=1}^{p} \{\omega \in \Omega \mid X_i(\omega) \leq x_i\}$$

Distributions and Densities For a random vector $X : \Omega \to \mathbb{R}^p$, the cumulative probability distribution function is

$$F_X(x) = P(X \leq x) = P(\{\omega \in \Omega \mid X(\omega) \leq x\})$$

The probability density function of a continuous random vector X is

$$f_X(x) = \frac{\partial^p F_X(x)}{\partial x_1 \partial x_2 ... \partial x_p}$$

which is equivalent to

$$F_X(x_1, x_2, ...x_p) = \int_{-\infty}^{x_p} ... \int_{-\infty}^{x_2} \int_{-\infty}^{x_1} f_X(\bar{x}_1, \bar{x}_2 ... \bar{x}_p) d\bar{x}_1 d\bar{x}_2 ... d\bar{x}_p$$

Suppose the vector X is partitioned into two components X_1 and X_2, so that, by abuse notation, we have

$$X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \begin{array}{l} X_1 : \Omega \to R^n \\ X_2 : \Omega \to R^m \end{array}$$

$$X : \Omega \to \mathbb{R}^p \text{ with } p = n + m$$

Def. X_1 and X_2 are independent if the distribution function factors

$$F_X(x) = F_{X_1, X_2}(x_1, x_2) = F_{X_1}(x_1) F_{X_2}(x_2).$$

The same is true for densities.

3 Conditioning

Recall For two events $A, B \in \mathscr{F}, P(B) > 0$

$$P(A \mid B) := \frac{P(A \bigcap B)}{P(B)}$$

Note

$$B \subset A,\ P(A \mid B) = \frac{P(A \bigcap B)}{P(B)} = \frac{P(B)}{P(B)} = 1$$

$$A \subset B,\ P(A \mid B) = \frac{P(A \bigcap B)}{P(B)} = \frac{P(A)}{P(B)} \geq P(A)$$

Def. The conditional distribution of X_1 given $X_2 = x_2$ is

$$F_{X_1|X_2}(x_1 \mid x_2) = \lim_{\varepsilon \to 0} P(X_1 \leq x_1 \mid x_2 - \varepsilon \leq X_2 \leq x_2 + \varepsilon) = \lim_{\varepsilon \to 0} \frac{P(A \bigcap B_\varepsilon)}{P(B_\varepsilon)}$$

where $A = \{\omega \in \Omega \mid X_1(\omega) \leq x_1\}$ and $B_\epsilon = \{\omega \in \Omega \mid x_2 - \varepsilon \leq X_2(\omega) \leq x_2 + \varepsilon\}$

In general, this is unpleasant to compute, but for Gaussian random vectors, the handout "*Useful Facts About Gaussian Random Variables and Vectors*" shows that it is quite easy.

Def. The conditional density is $f_{X_1|X_2}(x_1 \mid x_2) = \frac{f_{X_1 X_2}(x_1, x_2)}{f_{X_2}(x_2)}$. Sometimes we simply write $f(x_1 \mid x_2)$

Very important: X_1 given $X_2 = x_2$ is a random vector. We have produced its distribution and density!

4 Moments

Suppose $g : \mathbb{R}^p \to R$

$$E\{g(X)\} = \int_{\mathbb{R}^p} g(x) f_X(x) dx = \int_{-\infty}^{\infty} ... \int_{-\infty}^{\infty} g(x_1 ... x_p) f_X(x_1 ... x_p) dx_1 ... dx_p$$

Mean or Expected Value

$$\mu = E\{X\} = E\{\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}\} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_p \end{pmatrix}$$

Covariance Matrices

$$cov(X) = cov(X, X) = E\{(X - \mu)(X - \mu)^T\}$$

where

$$(X - \mu) \text{ is } p \times 1,\ (X - \mu)^T \text{ is } 1 \times p,\ (X - \mu)(X - \mu)^T \text{ is } p \times p$$

Exercise cov(X) is positive semidefinite

If we have X decomposed in blocks $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$ $\begin{matrix} X_1 : \Omega \to R^n \\ X_2 : \Omega \to R^m \end{matrix}$ we may compute

$$cov(X_1, X_2) = E\{(X_1 - \mu_1)(X_2 - \mu_2)^T\}$$

where

$$(X_1 - \mu_1) \text{ is } m \times 1,\ (X_2 - \mu_2)^T \text{ is } 1 \times n,\ (X_1 - \mu_1)(X_2 - \mu_2)^T \text{ is } m \times n$$

Def. X_1 and X_2 are uncorrelated if $cov(X_1, X_2) = 0$

Fact: In general, independence $\Rightarrow$ uncorrelated, but the converse is false.

5 Derivation of the conditional density formula from the definition of the conditional distribution:

$$P(A \bigcap B_\varepsilon) = \int_{-\infty}^{x_1} \int_{x_2-\varepsilon}^{x_2+\varepsilon} f_{X_1X_2}(\bar{x}_1, \bar{x}_2) d\bar{x}_2 d\bar{x}_1$$

$$P(B_\varepsilon) = \int_{x_2-\varepsilon}^{x_2+\varepsilon} f_{X_2}(\bar{x}_2) d\bar{x}_2$$

$$F_{X_1|X_2}(x_1 \mid x_2) = \frac{P(A \bigcap B_\varepsilon)}{P(B_\varepsilon)} = \frac{\int_{-\infty}^{x_1} \int_{x_2-\varepsilon}^{x_2+\varepsilon} f_{X_1X_2}(\bar{x}_1, \bar{x}_2) d\bar{x}_2 d\bar{x}_1}{\int_{x_2-\varepsilon}^{x_2+\varepsilon} f_{X_2}(\bar{x}_2) d\bar{x}_2}, \ \varepsilon \text{ small}$$

Density: differentiate w.r.t. x_1

$$f_{X_1|X_2}(x_1 \mid x_2) = \frac{\int_{x_2-\varepsilon}^{x_2+\varepsilon} f_{X_1X_2}(x_1, \bar{x}_2) d\bar{x}_2}{\int_{x_2-\varepsilon}^{x_2+\varepsilon} f_{X_2}(\bar{x}_2) d\bar{x}_2} = \frac{f_{X_1X_2}(x_1, x_2) \cdot 2\varepsilon}{f_{X_2}(x_2) \cdot 2\varepsilon} = \frac{f_{X_1X_2}(x_1, x_2)}{f_{X_2}(x_2)}$$

ROB 501 Fall 2014
Lecture 19
Typeset by:
Proofread by:
There was no lecture on this day.

Rob 501 Fall 2014
Lecture 20
Typeset by: Yevgeniy Yesilevskiy
Revised by Ni on 21 Nov. 2015

Multivariate Random Variables or Vectors

Let $(\Omega,\ \mathscr{F},\ P)$ be a probability space.

$$X = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}$$

where $X_1 \in \mathbb{R}^n$ and $X_2 \in \mathbb{R}^m$, and let $p = n + m$.
Then, the distribution function

$$\begin{aligned} F_{X_1 X_2}(x_1,\ x_2) &= P(X_1 \leq x_1,\ X_2 \leq x_2) \\ &= P(\{\omega \in \Omega | X_1(\omega) \leq x_1,\ X_2(\omega) \leq x_2\}) \end{aligned}$$

Conditioning:

$$\begin{aligned} F_{X_1|X_2}(x_1|x_2) &= P(X_1 \leq x_1 | X_2 = x_2) \\ &= \lim_{\epsilon \to 0} \frac{P(A \cap B_\epsilon)}{P(B_\epsilon)} \end{aligned}$$

where $A = \{\omega | X_1(\omega) \leq x_1\}$, $B_\epsilon = \{\omega | x_2 - \epsilon \leq X_2(\omega) \leq x_2 + \epsilon\}$

Conditional Density:

$$f_{X_1|X_2} = \frac{f_{X_1 X_2}(x_1,\ x_2)}{f_{X_2}(x_2)}$$

Sometimes, it is convenient to write $f(x_1|x_2)$.

Conditional Mean (Expectation):

$$\begin{aligned}\mu(x_2) = E\{X_1|X_2 = x_2\} &= \int_{\mathbb{R}^n} x_1 f(x_1|x_2)dx_1 \\ &= \int_{\mathbb{R}^n} x_1 f_{X_1|X_2}(x_1|x_2)dx_1\end{aligned}$$

Theorem: Let $\hat{x} = \operatorname{argmin}_{z=g(x_2)} E\{\|X_1 - z\|^2|X_2 = x_2\}$, where g varies over all functions $g: \mathbb{R}^m \to \mathbb{R}^n$.
Then, $\hat{x} = \mu(x_2) = E\{X_1|X_2 = x_2\}$.

Remark: $g: \mathbb{R}^m \to \mathbb{R}^n$ includes linear, quadratic, cubic ... terms.

Rob 501 Fall 2014
Lecture 21
Typeset by: Jeff Koller
Proofread by: Yevgeniy Yesilevskiy
Revised by Grizzle on 10 Nov. 2015

Luenberger Observers

Luenberger Observers: It is deterministic estimator. We consider the easiest case

$$x_{k+1} = Ax_k$$
$$y_k = Cx_k$$

where $x \in \mathbb{R}^n$, $y \in \mathbb{R}^p$, $A \in \mathbb{R}^{n\times n}$, and $C \in \mathbb{R}^{p\times n}$.

Question 1: When can we reconstruct the initial condition (x_o) from the measurements $y_0, y_1, y_2, \ldots$

$$\begin{aligned} y_o &= Cx_o \\ y_1 &= Cx_1 = CAx_o \\ y_2 &= Cx_2 = CAx_1 = CA^2x_o \\ &\vdots \\ y_k &= CA^kx_o \end{aligned}$$

Represent the above matrix form:

$$\begin{bmatrix} y_o \\ y_1 \\ \vdots \\ y_k \end{bmatrix} = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^k \end{bmatrix} x_o$$

We note that if rank $\begin{bmatrix} C \\ CA \\ \vdots \\ CA^k \end{bmatrix} = n$, then we can determine x_0 uniquely on the basis of the measurements.

Caley Hamilton Theorem:

$$\text{rank} \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix} = \text{rank} \begin{bmatrix} C \\ CA \\ \vdots \\ CA^k \end{bmatrix} \text{ for all } k \geq n-1$$

Theorem: rank $\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix} = n$ means that we can determine x_o uniquely from the measurements. (This called the Kalman observability rank condition.)

Question 2: Can we process the measurements dynamically (i.e. recursively) and "estimate" x_k?

Full-State Luenberger Observer:

$$\hat{x}_{k+1} = A\hat{x}_k + L(y_k - C\hat{x}_k)$$

We define the error to be $e_k = x_k - \hat{x}_k$. We want conditions such that $e_k \to 0$ as $k \to \infty$. Want $e_k \to 0$ because then $\hat{x}_k \to x_k$!!!

$$\begin{aligned} e_{k+1} &= x_{k+1} - \hat{x}_{k+1} \\ &= Ax_k - [A\hat{x}_k + L(y_k - C\hat{x}_k)] \\ &= A(x_k - \hat{x}_k) - LC(x_k - \hat{x}_k) \\ &= Ae_k - LCe_k \end{aligned}$$

$$\boxed{e_{k+1} = (A - LC)e_k}$$

Theorem: Let $e_0 \in \mathbb{R}^n$ and define $e_{k+1} = (A - LC)e_k$. The the sequence $e_k \to 0$ as $k \to \infty$ for all $e_0 \in \mathbb{R}^n$ if, and only if, $|\lambda_i(A - LC)| < 1$ for $i = 1, \ldots, n$.

Theorem: A sufficient condition for the existence of $L : \mathbb{R}^m \to \mathbb{R}^n$ that places eigenvalues of $(A - LC)$ in the unit circle is:

$$\text{rank} \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix} = n = dim(x)$$

.

Remarks: L = constant similar to K_{ss} = steady-state Kalman Gain

1. Reason to choose one gain over the other: Optimality of the estimate when you know the noise statistics.
2. Kalman Filter works for time varying models A_k, C_k, G_k, etc.

Rob 501 Fall 2014
Lecture 22
Typeset by Ni on 18 Nov. 2015

Real Analysis

Let $(\mathcal{X},\ \mathbb{R},\ \|\cdot\|)$ be a real normed space.
Recall $\|\cdot\|:\ \mathcal{X} \to [0,\ +\infty)$ such that

1. $\|x\| \geq 0$ and $\|x\| = 0 \ \Leftrightarrow\ x = 0$
2. $\|\alpha \cdot x\| = |\alpha| \cdot \|x\|$ for all $\alpha \in \mathbb{R}$, $x \in \mathcal{X}$
3. $\|x + y\| \leq \|x\| + \|y\|$ for all $x,\ y \in \mathcal{X}$.

Recall:
Def.

1. For $x,\ y \in \mathcal{X}$, $d(x,\ y) := \|x - y\|$.
2. For $x \in X$, $S \subset \mathcal{X}$ a subset
$$d(x,\ S) := \inf_{y \in S} \|x - y\|.$$

Def. Let $x_0 \in X$ and $a \in \mathbb{R}$, $a > 0$. The open ball of radius a center at x_0 is
$$B_a(x_0) = \{x \in \mathcal{X} | \|x - x_0\| < a\}.$$

Examples:

1. $\left(\mathbb{R}^2,\ \|\cdot\|_2\right)$: Euclidean norm

2. $\left(\mathbb{R}^2,\ \|\cdot\|_1\right)$: One norm

$$\|(x_1,\ x_2)\|_1 = |x_1| + |x_2|$$

3. $\left(\mathbb{R}^2,\ \|\cdot\|_\infty\right)$: Max norm

$$\|\cdot\|_\infty = \max_{1\le i\le n} |x_i|$$

Lemma: Let $(\mathcal{X},\ \|\cdot\|)$ be a normed space, $x \in \mathcal{X}$, and $S \subset \mathcal{X}$. Then,

$$\begin{aligned} d(x,\ S) = 0 &\Leftrightarrow \forall \epsilon > 0,\ \exists y \in S,\ \|x-y\| < \epsilon \\ &\Leftrightarrow \forall \epsilon > 0,\ B_\epsilon(x) \cap S \neq \varnothing. \end{aligned}$$

Corollary:

$$\begin{aligned} d(x,\ S) > 0 &\Leftrightarrow \exists \epsilon > 0,\ \forall y \in S,\ \|x-y\| \geq \epsilon \\ &\Leftrightarrow \exists \epsilon > 0 \text{ such that } B_\epsilon(x) \cap S = \varnothing \end{aligned}$$

In the following, we assume $(\mathcal{X},\ \|\cdot\|)$ is given.

Def.

1. Let $P \subset \mathcal{X}$, a subset of $\mathcal{X}$. A point $p \in P$ is <u>an interior point of P</u> if $\exists \epsilon > 0$ such that $B_\epsilon(p) \subset P$.

2. $$\begin{aligned} \mathring{P} &= \{p \in P \mid p \text{ is an interior point}\} \\ &= \{p \in P \mid \exists \epsilon > 0 \text{ such that } B_\epsilon(p) \subset P\} \end{aligned}$$

   Remark for later use: $p \in \mathring{P} \Leftrightarrow \exists \epsilon > 0,\ B_\epsilon(p) \subset P \Leftrightarrow \exists \epsilon > 0$ such that $B_\epsilon(p) \cap (\sim P) = \varnothing \Leftrightarrow d(p,\ \sim P) > 0$

   $$\sim P = P^C = \text{complement} = \{x \in \mathcal{X} | x \notin P\}$$

3. P is open if $P = \mathring{P}$. (Every point in P is an interior point.)

Proposition: $x \in \mathring{P} \Leftrightarrow d(x, \sim P) > 0$

Example:

- $P = (0, 1) \subset (\mathbb{R}, \|\cdot\|)$ is open
$$x \in P,\ 0 < x \leq \frac{1}{2},\ \epsilon = \frac{x}{2},\ B_\epsilon(x) \subset P, \text{ and}$$
$$x \in P,\ \frac{1}{2} \leq x < 1,\ \epsilon = 1 - \frac{x}{2},\ B_\epsilon(x) \subset P.$$
- $P = [0, 1) \subset (\mathbb{R}, |\cdot|)$ is not open because $0 \in P$, $\forall \epsilon > 0$, $B_\epsilon(0) \cap (\sim P) \neq \varnothing$ or $0 \in P$, $d(0, \sim P) = 0$.

Def.

1. A point $x \in \mathcal{X}$ is a closure point of P if $\forall \epsilon > 0$, $\exists p \in P$ such that dis$\|x - p\| < \epsilon$, $[d(x, P) = 0]$.
2. $$\underline{\text{Closure of P}} = \overline{P} := \{x \in \mathcal{X} \mid \mathcal{X} \text{ is a closure point}\}$$
$$= \{x \in \mathcal{X} \mid d(x, P) = 0\}$$
3. P is closed if $P = \overline{P}$.

Example:

1. $P = \{x \in [0, 1] \mid x \text{ rational}\} \Rightarrow \overline{P} = [0, 1]$
2. $P = (0, 1) \Rightarrow \overline{P} = [0, 1]$

Proposition:

$$x \in \mathcal{X},\ x \in \overline{P} \Leftrightarrow d(x, P) = 0.$$
$$x \in \mathcal{X},\ x \in \mathring{P} \Leftrightarrow d(x, \sim P) > 0.$$

Proposition:

$$P \text{ is closed} \Leftrightarrow P = \overline{\ P\ }.$$
$$P \text{ is open} \Leftrightarrow P = \mathring{P}.$$

Proposition:

$$P \text{ is closed} \Leftrightarrow \sim P \text{ is open}.$$
$$P \text{ is open} \Leftrightarrow \sim P \text{ is closed}.$$

<u>Proof:</u>

$$\underbrace{\sim P = \sim (\mathring{P})}_{P \text{ is open}} = \{x \in \mathcal{X} \mid d(x,\ \sim P) = 0\} = \underbrace{\overline{\sim P} = \sim P}_{\sim P \text{ is closed}} \ \square$$

Rob 501 Fall 2014
Lecture 23
Typeset by: Ilsun Song
Proof-read by: Yunxiang Xu
Revised by Ni on 21 Nov. 2015

Sequence

Def. A set of vectors indexed by the non-negative integers is called a sequence (x_n) or $\{x_n\}$. Let (x_n) be a sequence and $n_1 < n_2 < n_3 < \cdots$ be an infinite set of strictly increasing integers. Then, (x_{n_i}) is called a subsequence of (x_n).
Example:

$$n_i = 2i + 1 \text{ or } n_i = 2^i$$

Def. A sequence of vectors (x_n) converges to $x \in X$ if, $\forall\ \varepsilon > 0,\ \exists N(\varepsilon) < \infty$ such that, $n \geq N$, then $\|x_n - x\| < \varepsilon$, i.e., $n \geq N \Rightarrow\ x_n \in B_\varepsilon(x)$. One writes

$$\lim_{n\to\infty} x_n = x \text{ or } x_n \to x \text{ or } x_n \xrightarrow[n\to\infty]{} x.$$

Proposition: Suppose $x_n \to x$. Then,

1. $\|x_n\| \to \|x\|$
2. $\sup\limits_n \|x_n\| < \infty$ (The sequence is bounded.)
3. If $x_n \to y$ then y = x. (Limits are unique.)

Aside: Useful inequality (Triangular inequality)
For $\overline{x},\ \overline{y} \in X$,

$$\begin{aligned} &\|\overline{x}\| = \|\overline{x} - \overline{y} + \overline{y}\| \leq \|\overline{x} - \overline{y}\| + \|\overline{y}\| \\ \Rightarrow\ &\|\overline{x}\| - \|\overline{y}\| \leq \|\overline{x} - \overline{y}\| \\ \therefore\ &\big|\|\overline{x}\| - \|\overline{y}\|\big| \leq \|\overline{x} - \overline{y}\| \end{aligned}$$

<u>Proof:</u>

1. $|\|x\| - \|x_n\|| \leq \|x - x_n\| \xrightarrow[n\to\infty]{} 0.$
2. Set $\varepsilon = 1$, $\exists N(1) < \infty$ such that $n \geq N,\ \|x_n - x\| \leq 1.$
   $\therefore \forall\ n \geq N,\ \|x_n\| = \|x_n - x + x\| \leq \|x_n - x\| + \|x\| \leq 1 + \|x\|.$
   $$\sup_k \|x_k\| \leq \max\{\underbrace{\|x_1\|, \|x_2\|, \cdots, \|x_{n-1}\|, 1 + \|x\|}_{\text{finite}}\} < \infty.$$
3. $\|x - y\| = \|x - x_n + x_n - y\| \leq \|x - x_n\| + \|x_n - y\| \xrightarrow[n\to\infty]{} 0.$

Def. $x \in X$, P $\subset$ X a subset. x is a <u>limit point</u> of P if $\exists$ a sequence of elements of P that converges to x. That is, $\exists (x_n),\ x_n \in P,$ and $\lim\limits_{n\to\infty} x_n = x.$

Proposition: x is a limit point of $P \Leftrightarrow x \in \overline{P}$.
<u>Proof:</u>

1. Suppose x is a limit point. Then, $\exists (x_n)$ such that $x_n \in P$ and $x_n \to x$. Because $x_n \to x$, $\forall \varepsilon > 0$, $\exists x_n \in P$ such that $\|x_n - x\| < \varepsilon \Rightarrow d(x,\ P) = 0$ $\Rightarrow x \in \overline{P}$.
2. Suppose $x \in \overline{P}$. Then, $\forall\ \varepsilon > 0$, $\exists\ y \in P$ such that $\|x - y\| < \varepsilon$. Let $\varepsilon = \frac{1}{n}$. Then, $\exists\ x_n \in P$ such that $\|x - x_n\| < \frac{1}{n}$
   $\Rightarrow x_n \to x.$
   $\therefore x$ is a limit point.

Corollary: P is closed $\Leftrightarrow$ it contains its limit points.

Complete Spaces (Banach Spaces)

Def. A sequence (x_n) in $(\mathcal{X},\ \|\cdot\|)$ is a <u>Cauchy sequence</u> if $\forall\ \varepsilon > 0$, $\exists N(\varepsilon) < \infty$, such that $n,\ m \geq N \Rightarrow \|x_n - x_m\| < \varepsilon.$

Notation: $\|x_n - x_m\| \xrightarrow[n,\ m\to\infty]{} 0$

Proposition: If $x_n \to x$, then (x_n) is Cauchy.
Proof: Let $\varepsilon > 0$ and choose $N < \infty$ such that $n \geq N \Rightarrow \|x_n - x\| < \frac{\varepsilon}{2}$. Then,

$$\begin{aligned}\|x_n - x_m\| &= \|x_n - x + x - x_m\| \\ &\leq \|x_n - x\| + \|x - x_m\| \\ &< 0.5\varepsilon + 0.5\varepsilon \\ &< \varepsilon \qquad \text{for all } n,\ m \geq N \ \square\end{aligned}$$

Unfortunately, not all Cauchy sequences are convergent. For a reason we will understand shortly, all counter examples are infinite dimensional.

Example:

$$X = \{f : [0,1] \to \mathbb{R} \mid \text{f continuous}\}$$

where $\|f\|_1 = \int_0^1 |f(\tau)| d\tau$.

Define a sequence as follow

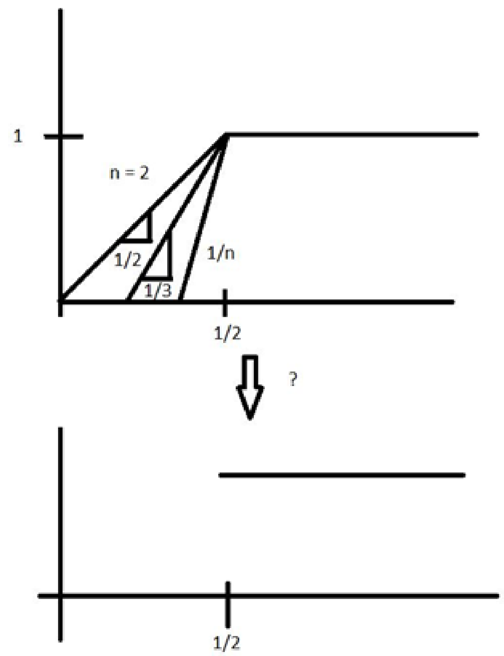
$$f_n(t) = \begin{cases} 0 & 0 \leq t \leq \frac{1}{2} - \frac{1}{n} \\ 1 + n(t - \frac{1}{2}) & \frac{1}{2} - \frac{1}{n} \leq t \leq \frac{1}{2} \\ 1 & t \geq \frac{1}{2} \end{cases}$$

$\|f_n - f_m\|_1 = \frac{1}{2}\ |\frac{1}{n} - \frac{1}{m}| \xrightarrow[n,\ m\to\infty]{} 0$, but there is no continuous $f(t)$, such that $f(t) \to f$.

Def. A normed space $(X, \mathbb{R}, \|\cdot\|)$ is complete if every Cauchy Sequence in X has a limit in X. Such spaces are called Banach spaces.
There are many useful and known Banach spaces.

In EECS562, you will use $(C\,[0,\ T]\,,\ \|\cdot\|_\infty)$.

Def. A subset P of a normed space is complete if every Cauchy Sequence in P has a limit in P.



Remark: P is complete $\Rightarrow$ P is closed.

Theorem:

1. In a normed linear space, any finite dimensional subspace is complete.
2. Any closed subset of a complete set is also complete.
3. $C[a,\ b]$, $\|\cdot\|_\infty$ is complete where $C[a,\ b] = \{f : [a,\ b] \to \mathbb{R} \mid f \text{ continuous}\}$
   Note: $a < b$, both finite.

Rob 501 Fall 2014
Lecture 24
Typeset by: Kevin Chen
Proofread by: Yong Xiao
Revised by Ni on Nov. 21, 2015

Newton-Raphson & Contraction Mapping

Let $h : \mathbb{R}^n \to \mathbb{R}^n$ satisfy, $\forall\ x \in \mathbb{R}^n$, the Jacobian $\frac{\partial h}{\partial x}(x)$ exists , is continuous and is invertible. Moreover, $\frac{\partial h}{\partial x}(x)$ is a continuous function.

Remark: One says h is C^1 when its derivative exits and is continuous.

Problem: For $y \in \mathbb{R}^n$, find a solution to $y = h(x)$, i.e., seek $x^* \in \mathbb{R}^n$ s.t. $h(x^*) = y$.

Approach: Generate a sequence of approximate solutions. Then, refer to the literature to ensure convergence.

Idea: Have x_k, seek x_{k+1} such that $h(x_{k+1}) - y \approx 0$. We write $x_{k+1} = x_k + \Delta x_k$ so that $h(x_k + \Delta x_k) - y \approx 0$. Applying Taylor's Theorem and keeping only the zeroth and first order terms,

$$h(x_k) + \frac{\partial h}{\partial x}(x_k)\,\Delta x_k - y \approx 0$$

$$\frac{\partial h}{\partial x}(x_k)\,\Delta x_k \approx -\left(h(x_k) - y\right)$$

$$\Delta x_k \approx -\left[\frac{\partial h}{\partial x}(x_k)\right]^{-1}\left(h(x_k) - y\right)$$

$$\therefore x_{k+1} = \underbrace{x_k - \left[\frac{\partial h}{\partial x}(x_k)\right]^{-1}\left(h(x_k) - y\right)}_{T(x_k)}$$

As indicated, we define $T(x) = x - \left[\frac{\partial h}{\partial x}(x)\right]^{-1}(h(x) - y)$. Then,

$$\begin{aligned} x^* &= T(x^*) \quad \text{(Fixed Point)} \\ \Leftrightarrow x^* &= -\left[\frac{\partial h}{\partial x}(x^*)\right]^{-1}(h(x^*) - y) \\ \Leftrightarrow 0 &= \left[\frac{\partial h}{\partial x}(x^*)\right]^{-1}(h(x^*) - y) \\ \Leftrightarrow y &= h(x^*) \end{aligned}$$

Let $(\mathcal{X}, \mathbb{R}, \|\cdot\|)$ be a normed space, $S \subset \mathcal{X}$, and $T : S \to S$.

Questions:

1. When does $\exists x^*$ s.t. $T(x^*) = x^*$? (Fixed point)
2. If a fixed point exists, is it unique?
3. When can a fixed point be determined by the Method of Successive Approximations: $x_{n+1} = T(x_n)$?

Def. $T : S \to S$ is a <u>contraction mapping</u> if,

$$\exists\ 0 \leq \alpha < 1 \text{ s.t. } \forall x, y \in S, \|T(x) - T(y)\| \leq \alpha \|x - y\|$$

.

Contraction Mapping Theorem: If T is a contraction mapping on a complete subset S of a normed space $(\mathcal{X}, \mathbb{R}, \|\cdot\|)$, then there exists a unique vector $x^* \in S$ such that $T(x^*) = x^*$. Moreover, for every initial point $x_0 \in S$, the sequence $x_{n+1} = T(x_n), n \geq 0$, is Cauchy, and $x_n \to x^*$.

<u>Proof:</u> For all $n \geq 1$

$$\begin{aligned} \|x_{n+1} - x_n\| &= \|T(x_n) - T(x_{n-1})\| \\ &\leq \alpha \|x_n - x_{n-1}\| \end{aligned}$$

By induction, $\|x_{n+1} - x_n\| \leq \alpha^n \|x_1 - x_0\|$. Consider $\|x_m - x_n\|$, and WLOG, suppose $m = n + p,\ p > 0$. Then,

$$
\begin{aligned}
\|x_m - x_n\| &= \|x_{n+p} - x_n\| \\
&= \|x_{n+p} - x_{n+p-1} + x_{n+p-1} - \cdots + x_{n+1} - x_n\| \\
&\leq \|x_{n+p} - x_{n+p-1}\| + \cdots + \|x_{n+1} - x_n\| \\
&\leq \left(\alpha^{n+p-1} + \alpha^{n+p-2} + \cdots + \alpha^n\right) \|x_1 - x_0\| \\
&= \alpha^n \sum_{i=0}^{p-1} \alpha^i \|x_1 - x_0\| \\
&\leq \alpha^n \sum_{i=0}^{\infty} \alpha^i \|x_1 - x_0\| \\
&= \frac{\alpha^n}{1-\alpha} \|x_1 - x_0\| \xrightarrow[\substack{n\to\infty \\ m\to\infty}]{} 0
\end{aligned}
$$

$\therefore$ (x_n) is Cauchy sequence in S, and by completeness, $\exists x^* \in S$ such that $x_n \to x^*$. $\square$

Claim: $x^* = T(x^*)$

<u>Proof:</u> For every $n \geq 1$,

$$
\begin{aligned}
\|x^* - T(x^*)\| &= \|x^* - x_n + x_n - T(x^*)\| \\
&= \|x^* - x_n + T(x_{n-1}) - T(x^*)\| \\
&\leq \|x^* - x_n\| + \|T(x_{n-1}) - T(x^*)\| \\
&\leq \|x^* - x_n\| + \alpha \|x_{n-1} - x^*\| \xrightarrow[n\to\infty]{} 0. \ \square
\end{aligned}
$$

Claim: x^* is unique.

<u>Proof:</u> Suppose $y^* = T(y^*)$.
Then,

$$
\begin{aligned}
\|x^* - y^*\| &= \|T(x^*) - T(y^*)\| \\
&\leq \alpha \|x^* - y^*\| \text{ and } 0 \leq \alpha < 1
\end{aligned}
$$

The only non-negative real number γ that satisfies $\gamma \leq \gamma\alpha$ for some $0 \leq \alpha < 1$ is $\gamma = 0$. Hence, due to the property of norms, $0 = \|x^* - y^*\| \Leftrightarrow x^* = y^*$. $\square$

Continuous Functions and Compact Sets

Def. Let $(\mathcal{X}, \|\cdot\|)$, and $(\mathcal{Y}, |||\cdot|||)$, be two normed spaces.

(a) $f : \mathcal{X} \to \mathcal{Y}$ is <u>continuous at $x_0 \in \mathcal{X}$</u> if $\forall \varepsilon > 0,\ \exists \delta\left(\varepsilon, x_0\right) > 0$ such that

$$\|x - x_0\| < \delta \Rightarrow |||f\left(x\right))\,||| < \varepsilon$$

, $i.e.$ $\forall \varepsilon > 0,\ \exists \delta > 0,\ s.t.\ x \in B_\delta\left(x_0\right) \Rightarrow f\left(x\right) \in B_\varepsilon\left(f\left(x_0\right)\right)$.

(b) f is <u>continuous</u> if it is continuous at x_0 for all $x_0 \in \mathcal{X}$.

Theorem: Let Let $(\mathcal{X}, \|\cdot\|)$, and $(\mathcal{Y}, |||\cdot|||)$ be two normed spaces. $f : \mathcal{X} \to \mathcal{Y}$ a function.

(a) If f is continuous at x_0 and the sequence (x_n) converges to x_0 (i.e. $x_n \to x_0$). Then, $f\left(x_n\right) \to f\left(x_0\right)$.

(b) If f is not continuous at x_0 (discontinuous), then theres exists a sequence (x_n) such that $x_n \to x_0$, and $f\left(x_n\right) \nrightarrow f\left(x_0\right)$, that is, $f\left(x_n\right)$ does not converge to $f\left(x_0\right)$.

The proof is done in HW 10.

Rob 501 Fall 2014
Lecture 25
Typeset by: Yunxiang Xu
Proofread by: Jakob Hoellerbauer
Revised by Ni on Nov. 29, 2015

Continuous Functions and Compact Sets (Continued)

Def. A set C is bounded if $\exists r < \infty$ such that $C \subset B_r(0)$.

Bolzano-Weierstrass Theorem (Sequential Compactness Theorem): In a finite dimensional normed space $(\mathcal{X}, \mathbb{R}, ||\cdot||)$, the following two properties are equivalent for a set $C \subset \mathcal{X}$.

(a) C is closed and bounded;

(b) For every sequence (x_n) in C (i.e. $x_n \in C$), there exists $x_0 \in C$ and a subsequence (x_{n_i}) of (x_n) such that $x_{n_i} \to x_0$ (Every sequence in C contains a convergent subsequence).
Subsequence: $1 \leqslant n_1 < n_2 < n_3 < \cdots$

Def. C satisfies (a) or (b) is said to be compact.

Example: $C = [0, 1]$ is a compact subet of $\mathbb{R}$. For all (x_n) in C, it will have two following possibilities.

(a) (x_n) has finite number of distinct values and at least one of them has to be used for infinite times.

(b) (x_n) has infinite number of distinct values.

Weierstrass Theorem: If C is compact and $f : C \to \mathbb{R}$ is continous, then f

achieves its extreme values. That is,

$$\exists x^* \in C, \text{ s.t. } f(x^*) = \sup_{x \in C} f(x)$$

and

$$\exists x_* \in C, \text{ s.t. } f(x_*) = \inf_{x \in C} f(x).$$

<u>Proof:</u> Let $f^* := \sup\limits_{x \in C} f(x)$. To show $\exists x^* \in C$, s.t. $f(x^*) = f^*$.

Assume f^* is finite (Can be shown, but we skip it).

$$f^* = \text{supremum} = \text{least upper bound}$$

$\forall \varepsilon > 0, \exists x_\varepsilon \in C$, s.t. $|f^* - f(x_\varepsilon)| < \varepsilon$.

Set $\varepsilon = \frac{1}{n}$, and deduce that $\exists (x_n)$ in C such that $|f^* - f(x_n)| < \frac{1}{n}$
C is compact $\Rightarrow \exists (x_{n_i})$ and $x^* \in C$, s.t. $x_{n_i} \to x^*$.

By f continuous, $f(x_{n_i}) \to f(x^*)$

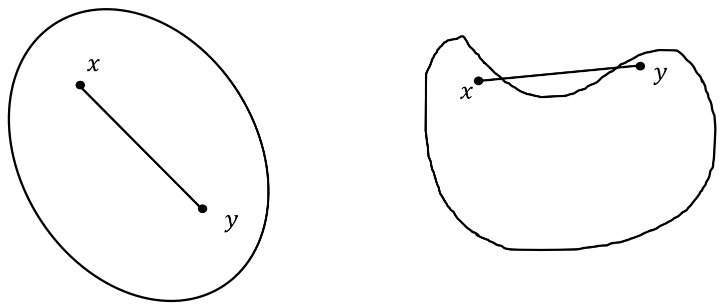
$$\begin{aligned}
|f^* - f(x^*)| &= |f^* - f(x_{n_i}) + f(x_{n_i}) - f(x^*)| \\
&\leqslant |f^* - f(x_{n_i})| + |f(x_{n_i}) - f(x^*)| \\
&\leqslant \frac{1}{n_i} + |f(x_{n_i}) - f(x^*)| \\
&\xrightarrow[i \to \infty]{} 0
\end{aligned}$$

$\therefore f^* = f(x^*)$. $\square$

Convex Sets and Convex Functions

Def. Let$(V, \mathbb{R})$ is a vector space. $C \subset V$ is <u>convex</u> if $\forall x, y \in C, 0 \leqslant \lambda \leqslant 1$.
Then, $\lambda x + (1 - \lambda) y \in C$.

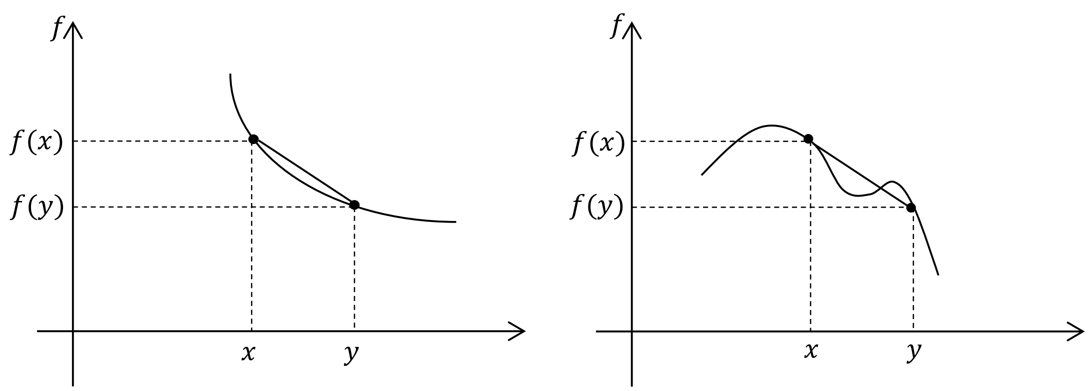
Remark:



(a) $x, y \in C$, then line connecting x and y also lies in C.

(b) Balls are always convex.

Def. Suppose C is convex. Then $f : C \to \mathbb{R}$ is <u>convex</u> if $\forall x, y \in C, 0 \leqslant \lambda \leqslant 1$, $f\left(\lambda x + (1-\lambda)y\right) \leqslant \lambda f(x) + (1-\lambda)f(y)$.



Def. Suppose $(V, \mathbb{R}, ||\cdot||)$ a normed space. $D \subset V$ a subset, and $f : D \to \mathbb{R}$ a function.

(a) $x^* \in D$ is a local minimum of f if $\exists \delta > 0$ s.t.$\forall x \in B_\delta(x^*)$, $f(x^*) \leqslant f(x)$.

(b) $x^* \in D$ is a global minimum if $\forall y \in D$, $f(x^*) \leqslant f(y)$.

Theorem: If D and f are both convex, then any local miniumum is also a global minimum.

Proof: We prove by contrapositive statement.

We show that if x is not a global minimum, then it cannot be a local minimum.
$x \in D$, x is not a global minimum, hence $\exists y \in D$ s.t. $f(y) < f(x)$.

To show: $\forall \delta > 0$. $\exists z \in B_\delta(x)$, s.t. $f(z) < f(x)$.

Claim: $\forall \delta > 0$, $\exists 0 < \lambda < 1$, s.t. $z = (1-\lambda)x + \lambda y \in B_\delta(x)$.

$$\begin{aligned} ||z - x|| &= ||(1-\lambda)x + \lambda y - x|| \\ &= ||\lambda(y-x)|| \\ &= \lambda ||y - x|| \\ &< \delta \end{aligned}$$

$\therefore \lambda < \frac{\delta}{||y-x||}$. It works!

$$\begin{aligned} f(z) &= f((1-\lambda)x + \lambda y) \\ &\leqslant (1-\lambda)f(x) + \lambda f(y) \\ &< (1-\lambda)f(x) + \lambda f(x) \\ &= f(x) \end{aligned}$$

$\therefore f(z) < f(x)$. x is not a local minimum. $\square$

Rob 501 Fall 2014
Lecture 26
Typeset by: Vittorio Bichucher
Proofread by: Mia Stevens
Revised by Ni on Nov. 29, 2015

Convex Sets and Convex Functions (Continued)

Additional Facts:

- All norms $\|\cdot\| : X \to [0, \infty)$ are convex. (proof using triangle inequality)
- For all $1 \leq \beta < \infty$, $\|\cdot\|^\beta$ is convex. (Convex function $\times$ strictly increasing function) Hence, on $\mathbb{R}^n$:
$$\Sigma_{i=1}^n |x_i|^3$$
is convex.
- Let $r > 0$, $\|\cdot\|$ a norm, $B_r(x_0)$ is a convex set.

  Special case: $B_1(0)$ convex set. (unit ball about the origin)
  Let C be an open, bounded and convex set, $0 \in$ C. Then, $\exists \,\|\cdot\| : X \to [0, \infty)$ such that $C = \{x \in X \mid ||x|| < 1\} = B_1(0)$.
- K_1 convex, K_2 convex $\to K_1 \cap K_2$ is convex. (Proved by line inside the set)
- Consider $(\mathbb{R}^n, \mathbb{R})$, A is a real m by n matrix, $b \in \mathbb{R}^m$. Then:
  - $K = \{x \in \mathbb{R}^n | \; Ax \leq b\}$ is also convex. (linear inequality)
  - $K = \{x \in \mathbb{R}^n | \; Ax = b\}$ is convex. (linear equality)
  - $K = \{x \in \mathbb{R}^n | \; A_{eq}x = b_{eq}, \; A_{in}x \leq b_{in}\}$ is convex as well. (intersection property)

Remark: $\tilde{A}x \geq \tilde{b} \Leftrightarrow -\tilde{A}x \leq -\tilde{b}$.

Quadratic Programming

$x \in \mathbb{R}^n$, $Q \geq 0$.
Minimize: $\underbrace{x^T Q x}_{\text{quadratic term}} + \underbrace{fx}_{\text{linear term}}$ subject to $A_{in}x \leq b_{in}$ and $A_{eq}x = b_{eq}$

Note: $f(x)$, Q, A_{in} and A_{eq} are all convex. Also, check if constraints form the empty set.

There are special purposes solvers available! See S. Boyd's website!

Example using robot equation:

$$D(q)\ddot{q} + C(q,\dot{q})\dot{q} + G(q) = Bu$$

where $q \in \mathbb{R}^n$, $u \in \mathbb{R}^m$.

Further, the ground reaction forces can be modeled as:

$$F = \Lambda_0(q,\dot{q}) + \Lambda_1(q)u = \begin{bmatrix} F^h \\ F^v \end{bmatrix}.$$

Suppose the desired feedback signal is $u = \gamma(q,\dot{q})$, but we need to respect bounds on the ground reaction forces

$$F^v \geq 0.2 m_{total} g.$$

Therefore, the normal force should be at least 20% of the total weight

$$|F^h| \leq 0.6 F^v.$$

Therefore, the friction force has a cone shape, and its magnitude is less than

60% of the total vertical force. Putting it all together:

$$\begin{bmatrix} F^v \geq 0.2m_{total}g \\ F^h \leq 0.6F^v \\ -F^h \leq 0.6F^v \end{bmatrix} \Leftrightarrow A_{in}(q)u \leq b_{in}(q,\dot{q}).$$

QP:

$$\begin{gathered} u^* = \text{argmin } \ u^T u + d^T dp \\ A_{in}(q)u \leq b_{in}(q,\dot{q}) \\ u = \gamma(q,\dot{q}) + d^T d \end{gathered}$$

where $d^T d$ is often called the relaxation parameter. Further, p is an weighting factor and it should be $>>>> 1 \cdot 10^4$. Dr. Grizzle finished by showing his handout in linear programming and quadractic programming. And remember Stephen Boyd!