

Perceptron

Sriram Sankararaman

The instructor gratefully acknowledges Fei Sha, Ameet Talwalkar, Eric Eaton, and Jessica Wu whose slides are heavily used, and the many others who made their course material freely available online.

Key issues in machine learning

- Modeling

- ▶ How to formulate the problem ?

- Representation

- ▶ What is the input/output space ?
- ▶ What is the model/ hypothesis space?

- Algorithms

- ▶ How to find the best hypothesis?

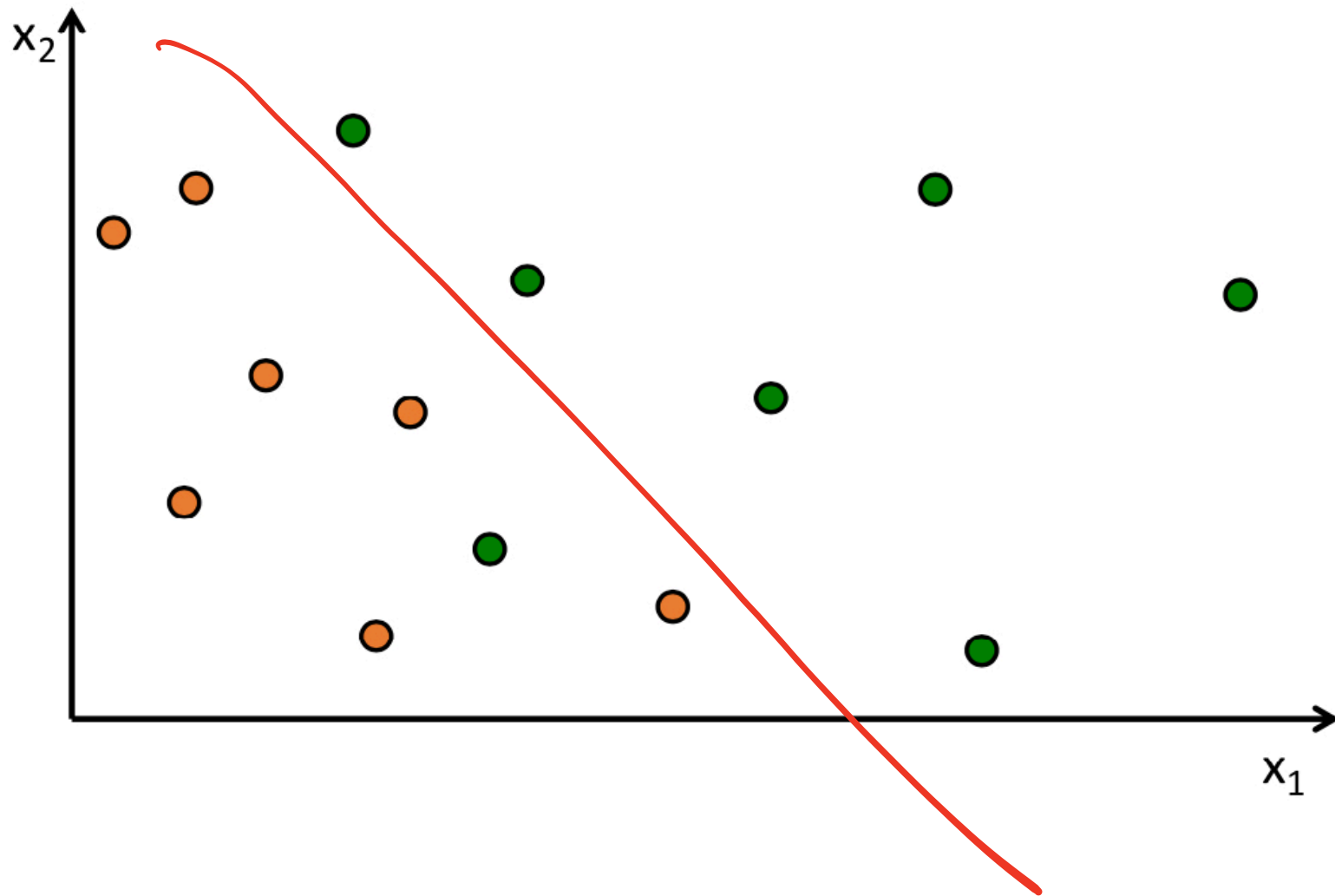
Supervised learning
 $h(\underline{x}) \rightarrow y$

Decision Trees
Nearest neighbors

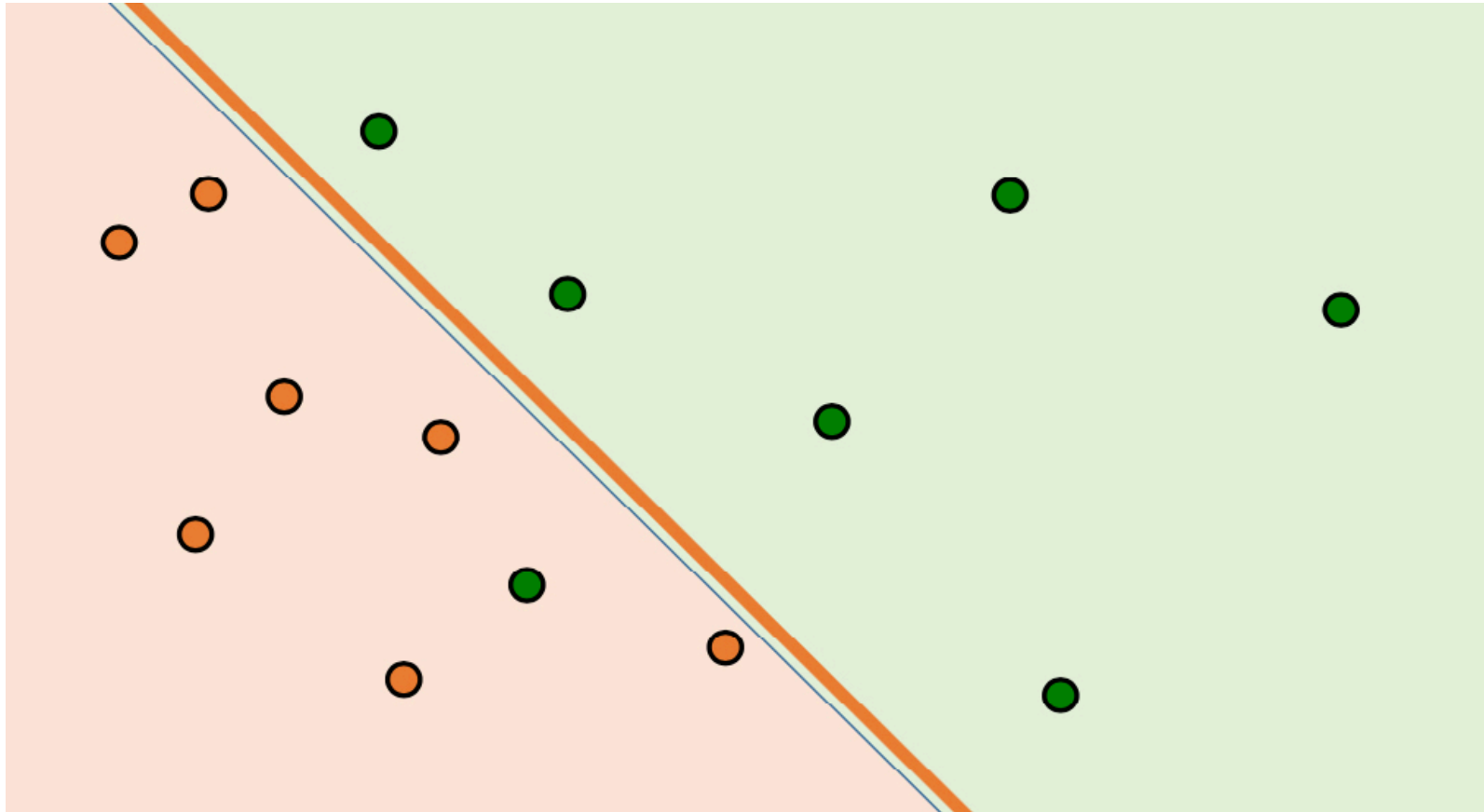
Outline

- 1 Perceptron
 - Setup for binary classification
- 2 Perceptron learning
- 3 Convergence of the Perceptron Learning Algorithm
- 4 Variants of perceptron
- 5 What we have learned

Training data for binary classification



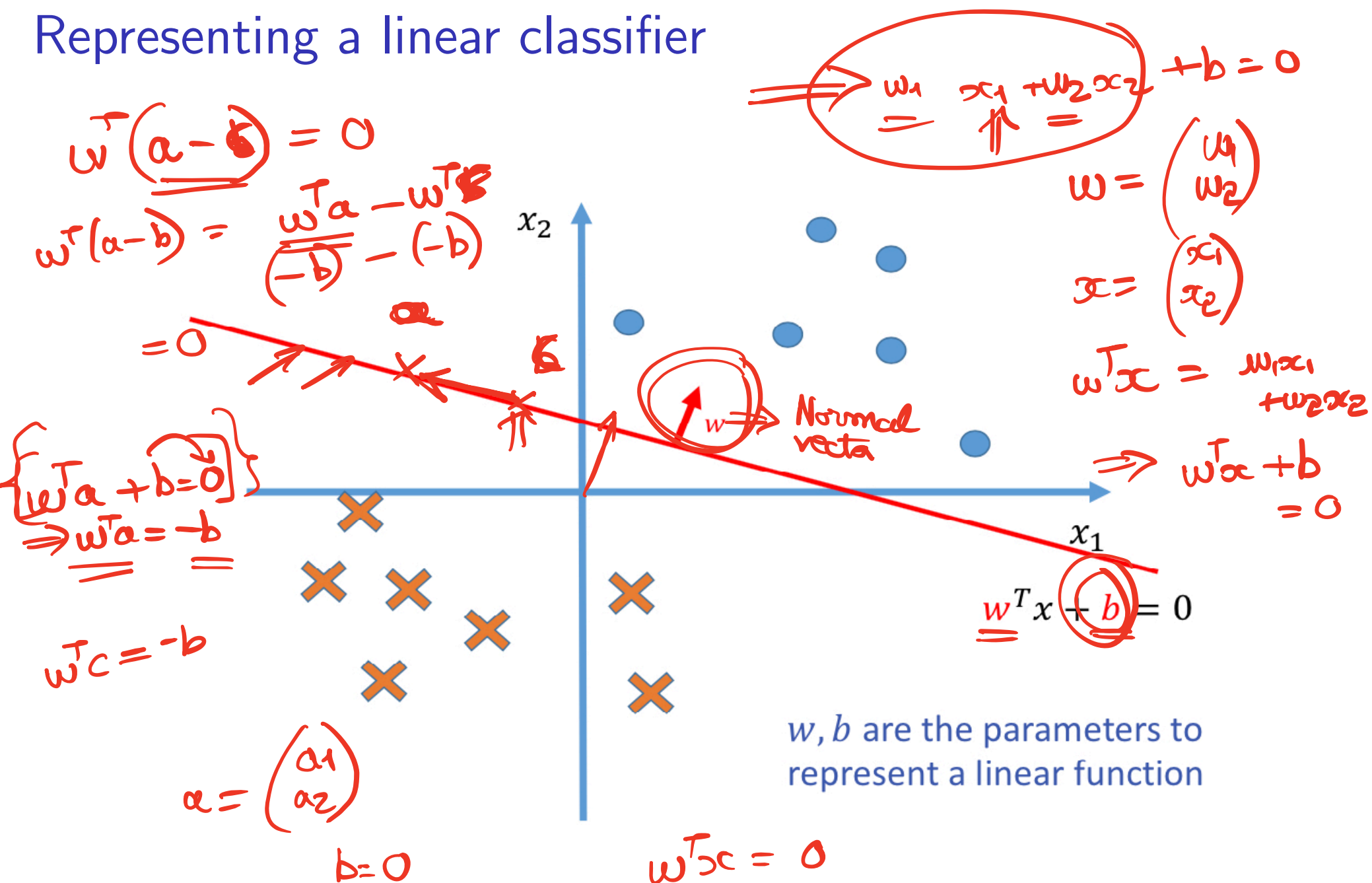
Linear classifier



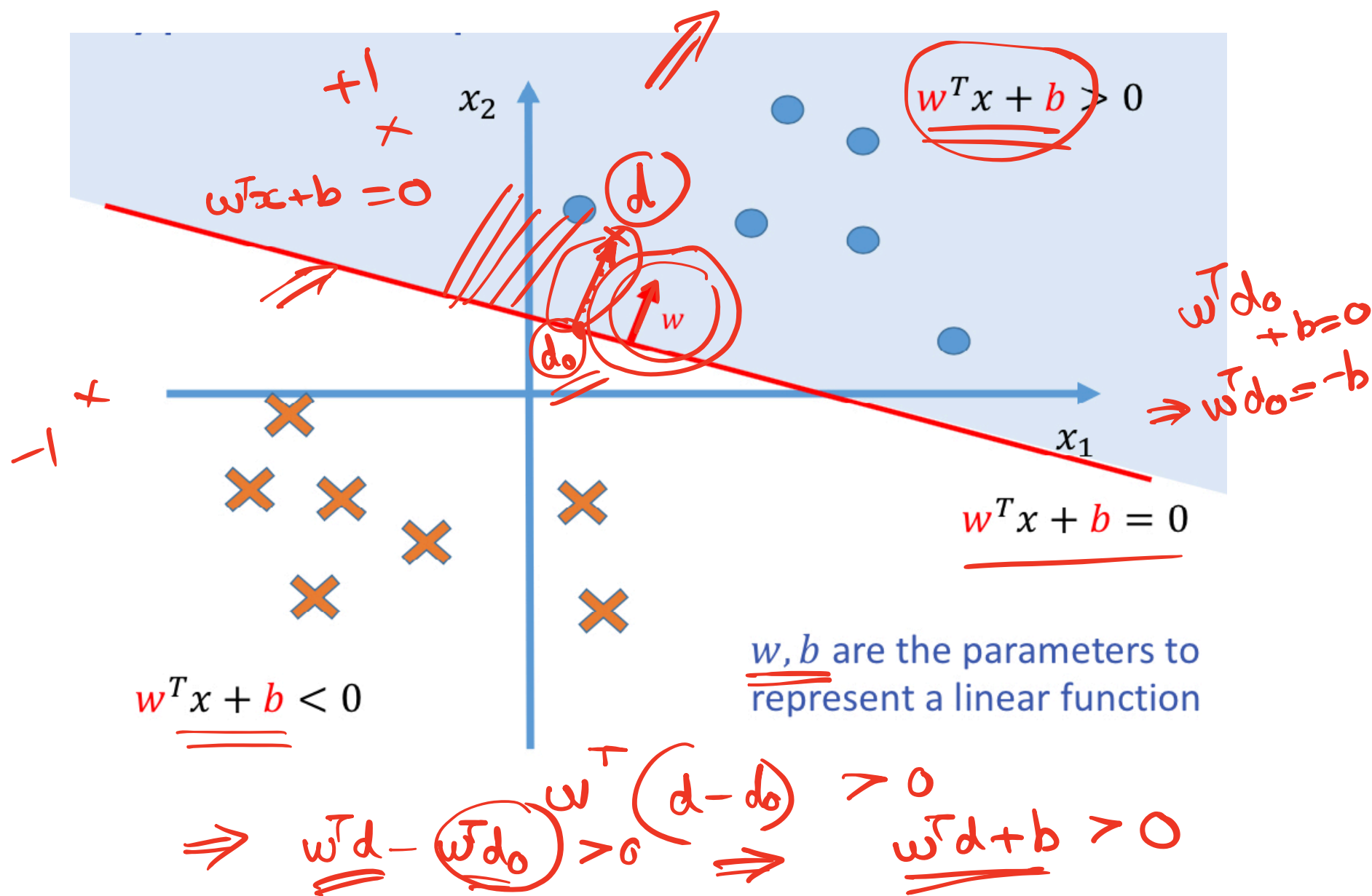
Prediction using a linear classifier



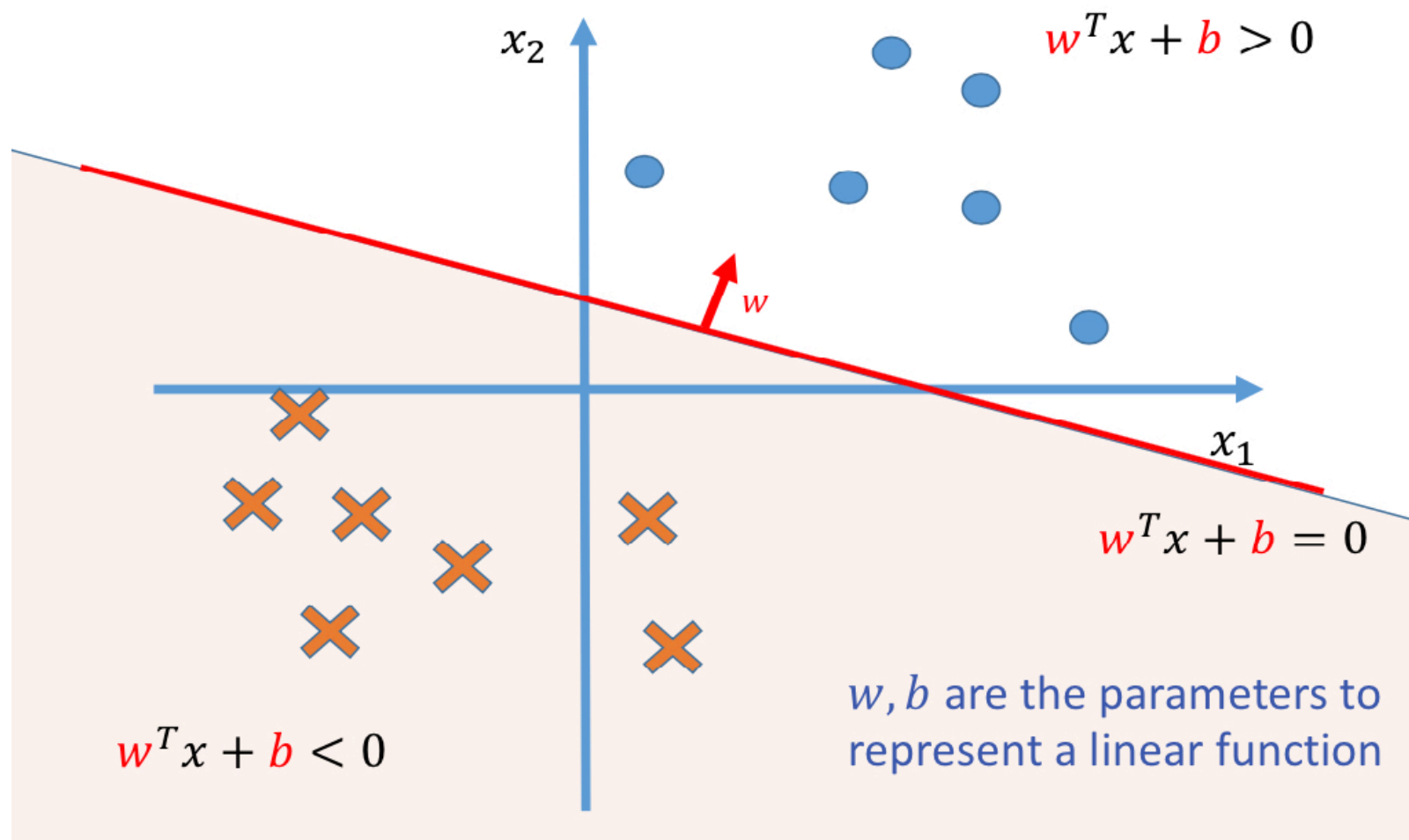
Representing a linear classifier



Representing a linear classifier



Classification using a linear classifier



Perceptron learning

$$\text{sign}(x) = \begin{cases} +1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \\ \text{not determined} & \text{if } x = 0 \end{cases}$$
$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_D \end{pmatrix}$$

Binary classification

- Instance (feature vectors): $x \in \mathbb{R}^D$

- Label: $y \in \{-1, +1\}$

- Model/Hypotheses:

$$H = \{h | h : \mathbb{X} \rightarrow \mathbb{Y}, h(x) = \text{sign}(\sum_{d=1}^D w_d x_d + b)\}.$$

- Learning goal: $\hat{y} = h(x)$

- ▶ Learn w_1, \dots, w_D, b .
- ▶ Parameters: w_1, \dots, w_D, b .
- ▶ w : weights, b : bias

$$(w_1 x_1 + w_2 x_2 + \dots + w_D x_D + b)$$

Perceptron predict

- Input: $x \in \mathbb{R}^D$, $w \in \mathbb{R}^D$, $b \in \mathbb{R}$.

$$\textcircled{a} = \sum_{d=1}^D \textcircled{w_d x_d} + b = \underline{\underline{w^T x + b}}$$
$$\underline{\underline{\hat{y}}} = \underline{\underline{\text{sign}(a)}} \in \{+1, -1\}$$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_D \end{pmatrix}$$

$$(w_1 x_1 + w_2 x_2 + \dots + w_D x_D + b)$$

- Output: \hat{y} .
- $\sum_{d=1}^D w_d x_d + b = \underline{\underline{w^T x + b}} = 0$: hyperplane in D dimensions with parameters (w, b) .
- w : weights, b : bias
- a : activation
- $\text{sign}(\sum_{d=1}^D w_d x_d + b)$: Linear Threshold Unit (LTU)

Hyperplanes through the origin

Consider \underline{x} that satisfies $g(\underline{x}) = \underline{w}^T \underline{x} + b = 0$. These \underline{x} define a hyperplane in D dimensions.

We can always write this as a hyperplane passing through the origin in $D + 1$ dimensions.

$$\begin{aligned} \underline{\tilde{x}} &\equiv \begin{pmatrix} 1 \\ \underline{x_1} \\ \vdots \\ \underline{x_D} \end{pmatrix} & \underline{\tilde{w}} &\equiv \begin{pmatrix} \underline{b} \\ \underline{w_1} \\ \vdots \\ \underline{w_D} \end{pmatrix} \\ \underline{\tilde{g}}(\underline{\tilde{x}}) &= \underline{\tilde{w}}^T \underline{\tilde{x}} = 0 \\ &= \sum_{d=1}^D \underline{w_d x_d} + \underline{b} \\ &= g(\underline{x}) = 0 \end{aligned}$$

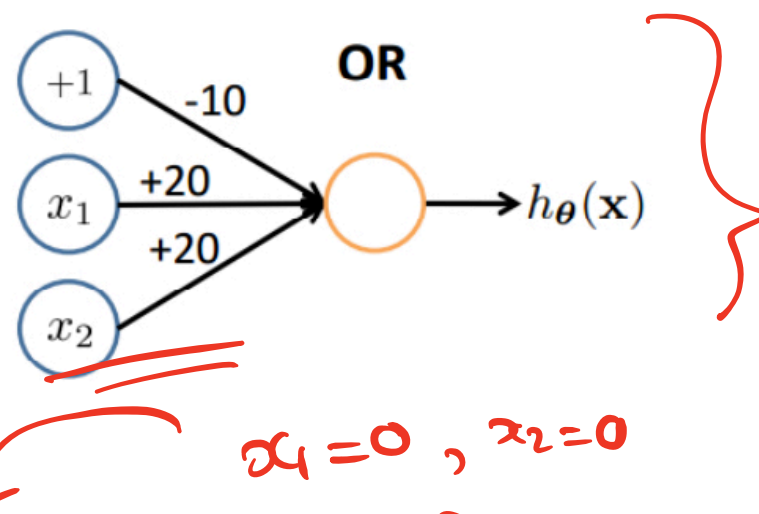
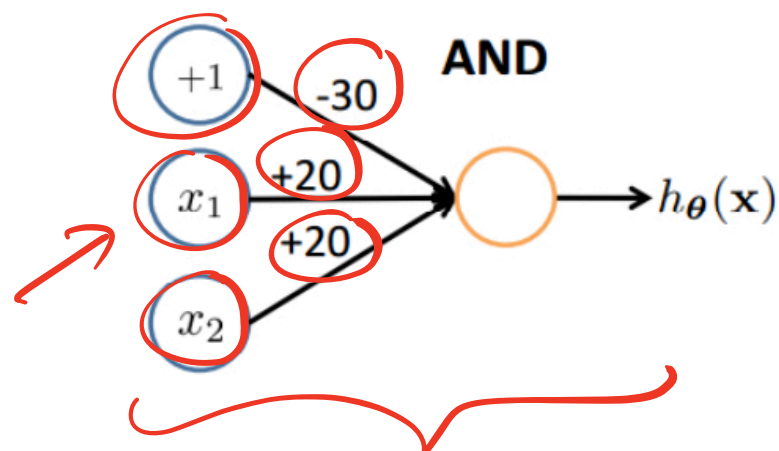
For simplicity, I may write $\underline{\tilde{w}}$ and $\underline{\tilde{x}}$ as w and x when there is no confusion

Representing Boolean functions

AND

x_1	x_2	y
0	0	0
0	1	0
1	0	0
1	1	1

$\left. \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \right\} -1$
 $\left. \begin{matrix} 0 \\ 0 \\ 1 \end{matrix} \right\} -1$
 $\left. \begin{matrix} 0 \\ 0 \\ 1 \end{matrix} \right\} -1$
 $+1$



$a = 20x_1 + 20x_2 - 30$
 $y = \text{sign}(a)$
 $x_1=1, x_2=1$
 $a = 20 + 20 - 30 = 10$
 $y = +1$

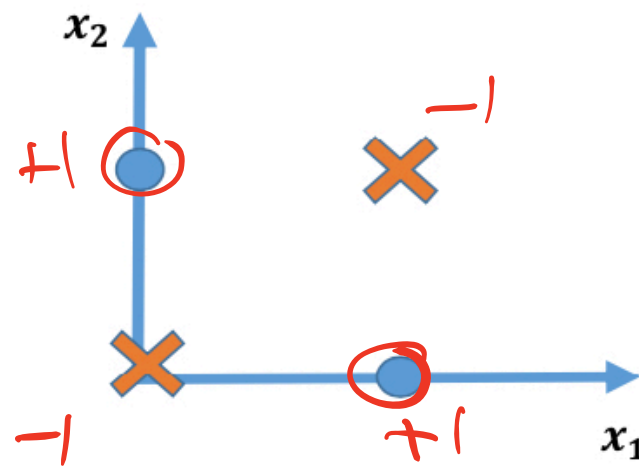
$x_1=0, x_2=1$
 $a = 20 - 30 = -10$
 $y = -1$

$x_1=0, x_2=0$
 $a = -30$
 $y = -1$

Representing Boolean functions

Can linear model represent XOR?

x_1	x_2	y
0	0	0
1	0	1
0	1	1
1	1	0



Learning a linear classifier

Several algorithms

- Perceptron
- Logistic regression
- (Linear) Support Vector Machines

Based on different assumptions

Outline

- 1 Perceptron
- 2 Perceptron learning
- 3 Convergence of the Perceptron Learning Algorithm
- 4 Variants of perceptron
- 5 What we have learned

Perceptron learning

Learning by making mistakes

mistake
+
correction
=
learning

Perceptron learning

If we have only one training example $(\underline{x_n}, \underline{y_n})$.

Assume $\underline{b = 0}$. (w)

How can we change \underline{w} such that

$$\underline{y_n = \text{sign}(\underline{w^T x_n})}$$

Two cases

- If $\underline{y_n = \text{sign}(w^T x_n)}$, do nothing.
- If $\underline{y_n \neq \text{sign}(w^T x_n)}$,

$$\underline{w^{\text{NEW}}} \leftarrow \underline{w} + \underline{y_n x_n}$$

Perceptron learning

If we have only one training example (x_n, y_n) .

Assume $b = 0$.

How can we change w such that

$$y_n = \text{sign}(w^T x_n)$$

Another way of saying the same thing

- $a = w^T x_n$

- If $y_n a > 0$, do nothing.

- If $y_n a \leq 0$,

$$\begin{array}{ll} y_n = +1 & a > 0 \\ y_n = -1 & a < 0 \end{array} \Rightarrow y_n a > 0$$

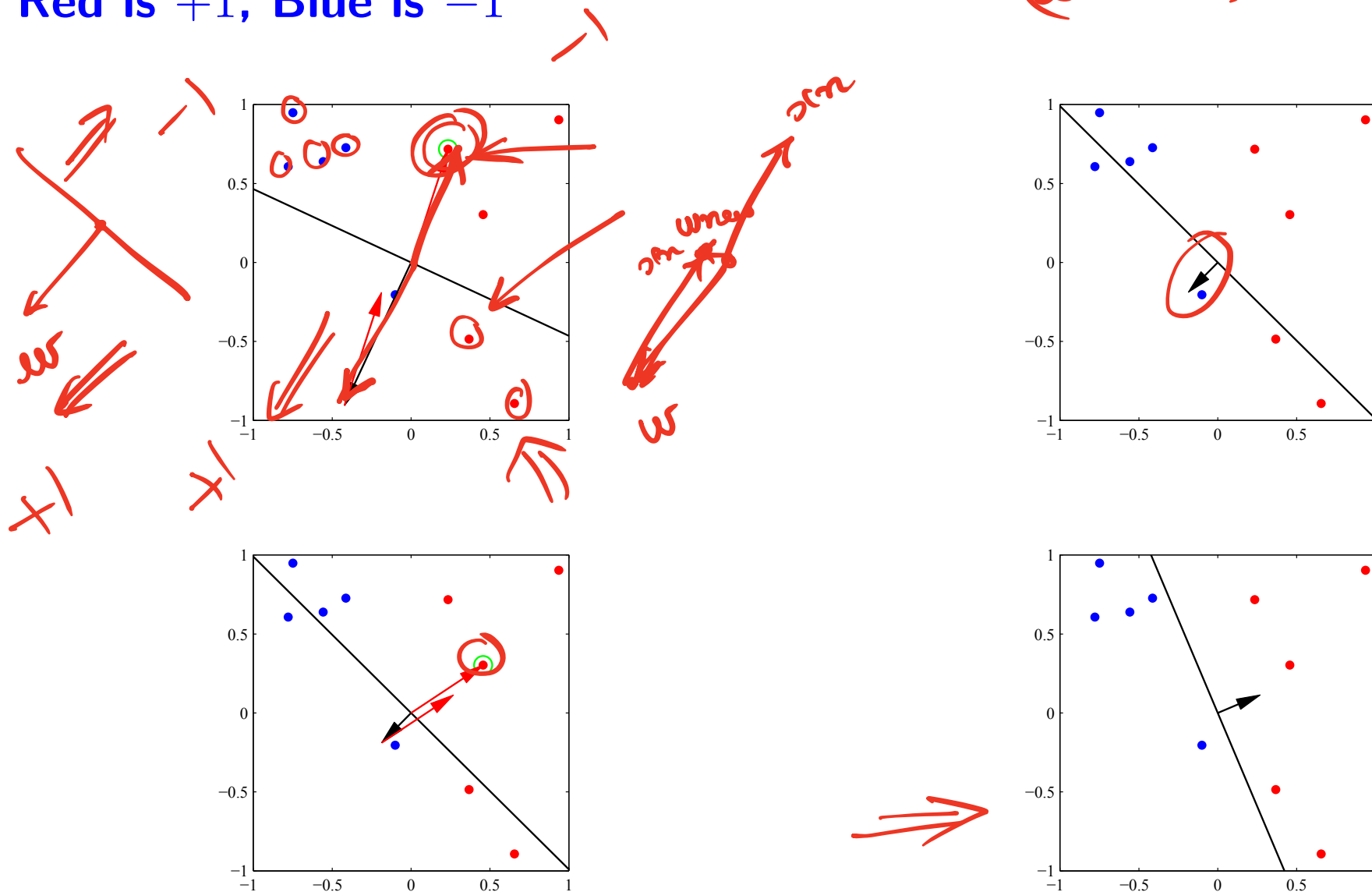
$$w^{\text{NEW}} \leftarrow w + y_n x_n$$

Example of perceptron update

$$w_{\text{new}} \leftarrow w + y_n x_n$$

$(w + x_n)$ $y_n = +1$

Red is +1, Blue is -1



Why would it work?

$$a = \mathbf{w}^T \mathbf{x}_n$$

If $y_n a \leq 0$, then

$$\underline{y_n(\mathbf{w}^T \mathbf{x}_n) \leq 0}$$

Why would it work?

$$y_n \in \{+1, -1\}$$

If $y_n a \leq 0$, then

$$\underline{y_n(\mathbf{w}^T \mathbf{x}_n) \leq 0}$$

$$y_n^2 \mathbf{x}_n^T \mathbf{x}_n = \mathbf{x}_n^T \mathbf{x}_n \neq 0$$

What would happen if we change to new $\mathbf{w}^{\text{NEW}} = \mathbf{w} + y_n \mathbf{x}_n$?

$$\begin{aligned} y_n[(\mathbf{w} + y_n \mathbf{x}_n)^T \mathbf{x}_n] &= \underline{y_n \mathbf{w}^T \mathbf{x}_n} + \underline{y_n^2 \mathbf{x}_n^T \mathbf{x}_n} \\ y_n(\underline{\mathbf{w}_{\text{new}}^T \mathbf{x}_n}) &= \underline{y_n} \left(\underline{(\mathbf{w} + y_n \mathbf{x}_n)^T \mathbf{x}_n} \right) \\ &= y_n \left(\mathbf{w}^T \mathbf{x}_n + \underline{(y_n \mathbf{x}_n)^T \mathbf{x}_n} \right) \\ &= y_n \left(\mathbf{w}^T \mathbf{x}_n + y_n \mathbf{x}_n^T \mathbf{x}_n \right) \\ &= y_n \mathbf{w}^T \mathbf{x}_n + \underline{y_n y_n \mathbf{x}_n^T \mathbf{x}_n} \end{aligned}$$

Why would it work?

If $y_n a \leq 0$, then

$$y_n(\mathbf{w}^T \mathbf{x}_n) \leq 0$$

What would happen if we change to new $\mathbf{w}^{\text{NEW}} = \mathbf{w} + y_n \mathbf{x}_n$?

$$y_n[(\mathbf{w} + y_n \mathbf{x}_n)^T \mathbf{x}_n] = y_n \mathbf{w}^T \mathbf{x}_n + y_n^2 \mathbf{x}_n^T \mathbf{x}_n$$

We are adding a positive number, so it is possible that

$$\underline{y_n(\mathbf{w}^{\text{NEW}}^T \mathbf{x}_n) > 0}$$

i.e., we are more likely to classify correctly

Perceptron learning

) Not linearly separable

Iteratively solving one case at a time

- REPEAT
- Pick a data point x_n
- Compute $a = w^T x_n$ using the current w
- If $ay_n > 0$, do nothing. Else,

$$\underline{w \leftarrow w + y_n x_n}$$

- UNTIL converged.

Perceptron training/learning




data = N **samples/instances**: $= \{(\underline{x_1}, \underline{y_1}), \dots, (\underline{x_N}, \underline{y_N})\}$

Algorithm 1 PerceptronTrain (*data*, *maxIter*)

```
1:  $w \leftarrow 0$ 
2: for iter = 1 .. MaxIter do
3:   for  $(x, y) \in data$  do
4:      $a \leftarrow w^T x$ 
5:     if  $ay \leq 0$  then
6:        $w \leftarrow w + yx$ 
7:     end if
8:   end for
9: end for
10: return  $w$ 
```

Prediction: $sign(w^T x)$.

Design decisions

- *MaxIter*: Hyperparameter
 - How to loop over the data?
 - ▶ Constant. 
 - ▶ Permuting once 
 - ▶ Permuting in each iteration
- 

Properties of perceptron learning

- This is an **online** algorithm – looks at one instance at a time.
- Does the algorithm terminate (**convergence**)?

Properties of perceptron learning

- This is an **online** algorithm – looks at one instance at a time.
- Does the algorithm terminate (**convergence**)?
 - ▶ If training data is **not linearly separable**, the algorithm does not converge.
 - ▶ If the training data is linearly separable, the algorithm stops in a finite number of steps (**converges**).

Properties of perceptron learning

- This is an **online** algorithm – looks at one instance at a time.
- Does the algorithm terminate (**convergence**)?
 - ▶ If training data is **not linearly separable**, the algorithm does not converge.
 - ▶ If the training data is linearly separable, the algorithm stops in a finite number of steps (**converges**).
- How long to convergence ?
 - ▶ Depends on the difficulty of the problem (**margin**).



Outline

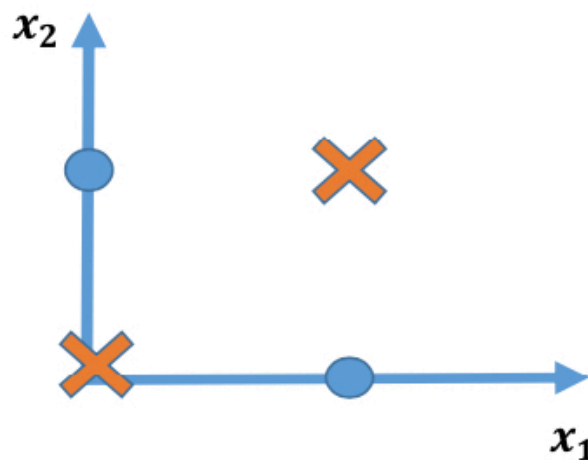
- 1 Perceptron
- 2 Perceptron learning
- 3 Convergence of the Perceptron Learning Algorithm
- 4 Variants of perceptron
- 5 What we have learned

Perceptron learnability

Perceptron cannot learn what it cannot represent

- Only linearly separable functions (Minsky and Papaert 1969).
- Parity function (XOR) cannot be learned.

x_1	x_2	y
0	0	0
1	0	1
0	1	1
1	1	0



Convergence

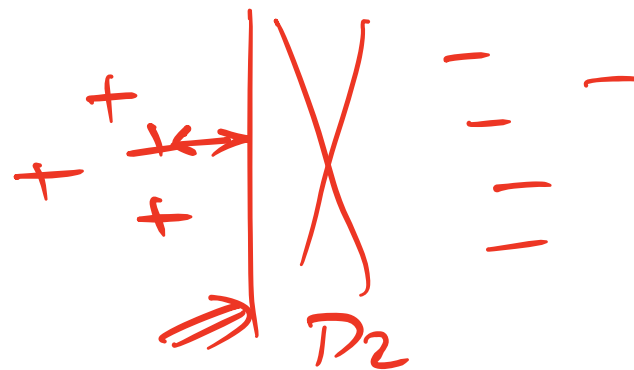
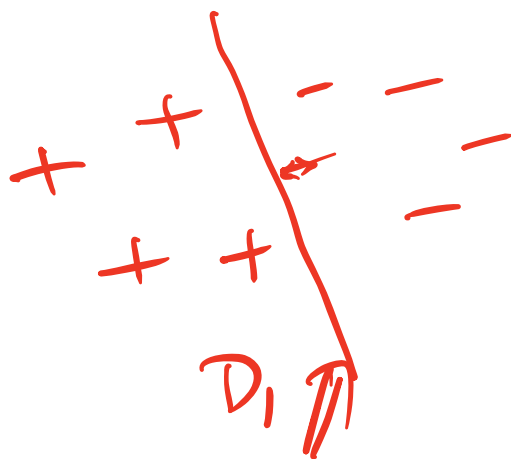
Convergence theorem

- If the data is linearly separable, the perceptron algorithm will converge after making mistakes that depend on the difficulty of the problem (margin).

Cycling theorem

- If the training data is not linearly separable, then the learning algorithm will eventually repeat the same set of weights and enter an infinite loop

Margin

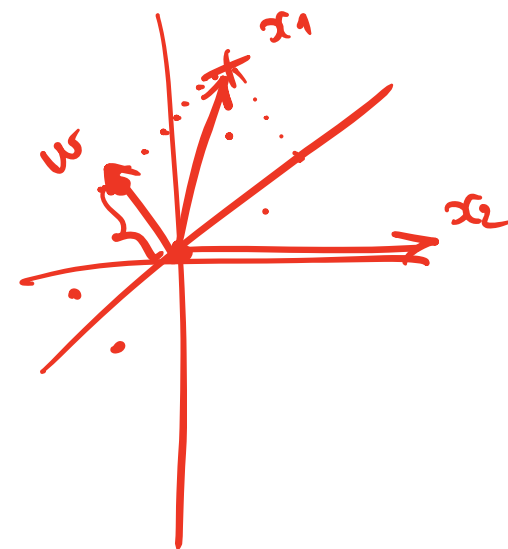


- The margin of a separating hyperplane for a dataset is the distance between the hyperplane and the data point nearest to it.
- The margin of a data set is the maximum margin possible for that dataset using any weight vector.

Margin

$$\mathcal{D} = \left\{ \begin{pmatrix} x_1, y_1 \\ \vdots \\ x_N, y_N \end{pmatrix} \right\}$$

$$y_n w^T x_n$$



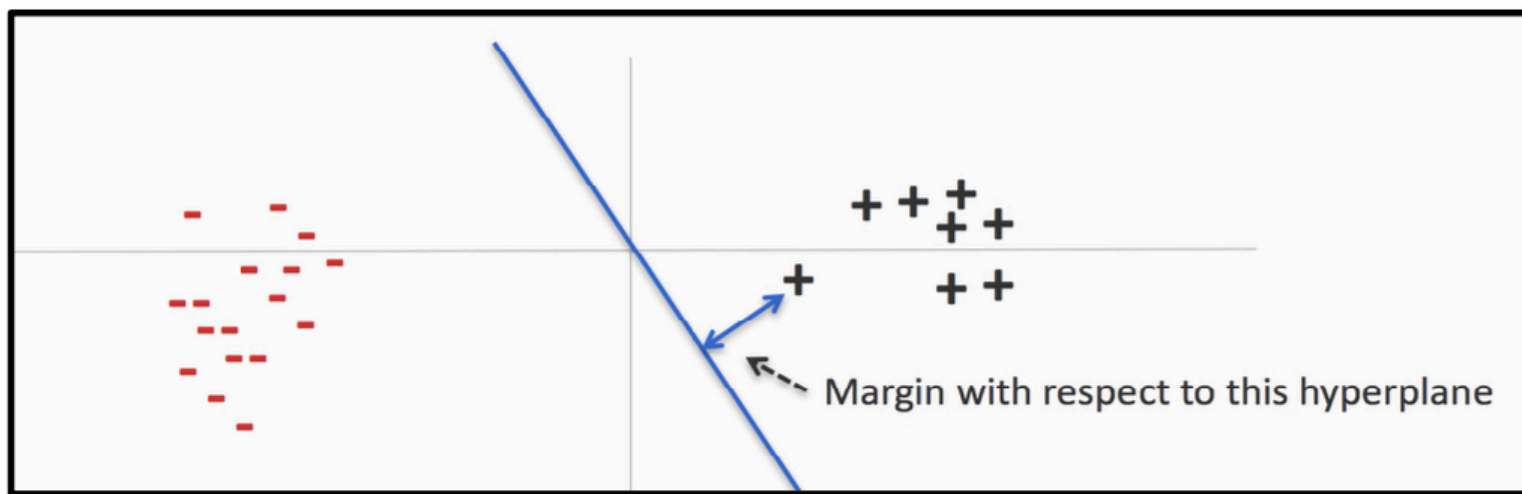
$$\text{Margin}(\mathcal{D}, \underline{w}) = \begin{cases} \min_{(x,y) \in \mathcal{D}} \underbrace{y_n w^T x_n}_{\text{for a separating hyperplane } \underline{w}} & \text{for a separating hyperplane } \underline{w} \\ -\infty & \text{else} \end{cases}$$

$$\text{Margin}(\mathcal{D}) = \underline{\underline{\sup}}_{\underline{w}} \text{Margin}(\mathcal{D}, \underline{w})$$

$$\text{sup} = \text{supremum} \quad x_1^T w$$

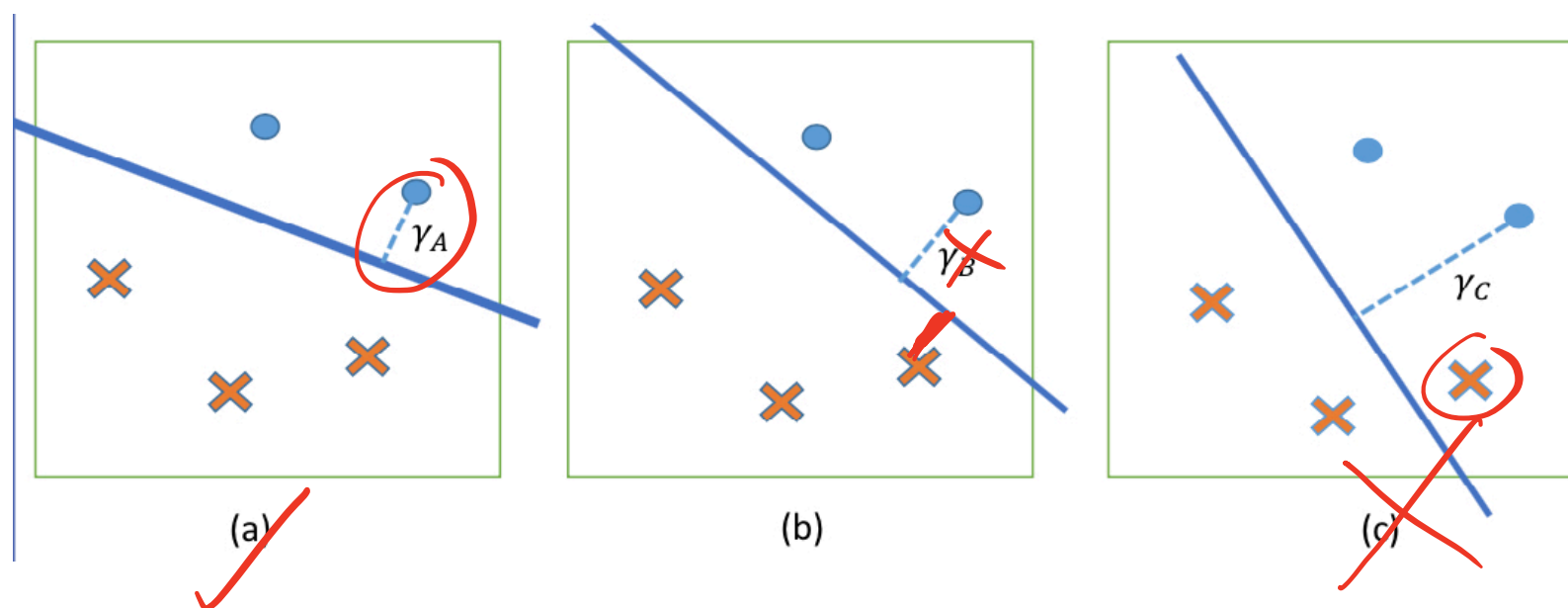
$$w^T x = x^T w$$

Margin



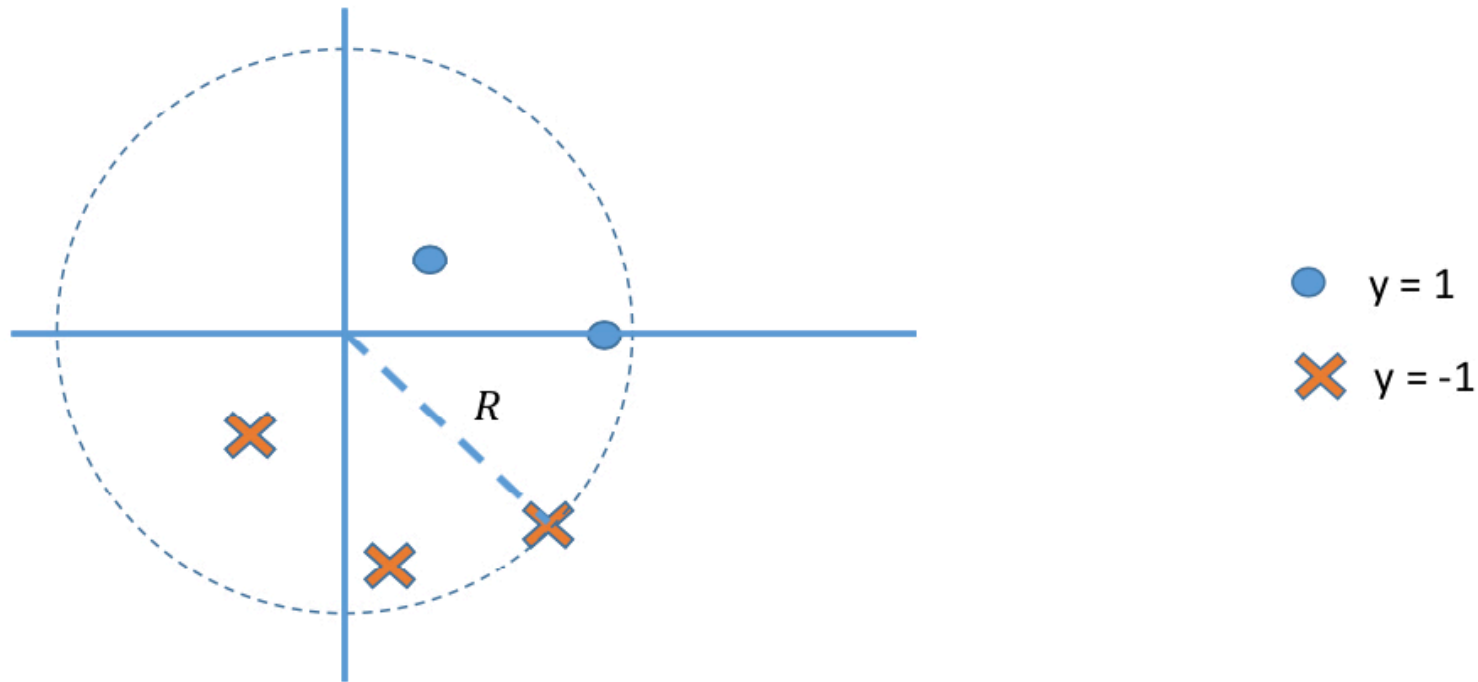
Margin

Which γ is the margin of the data?



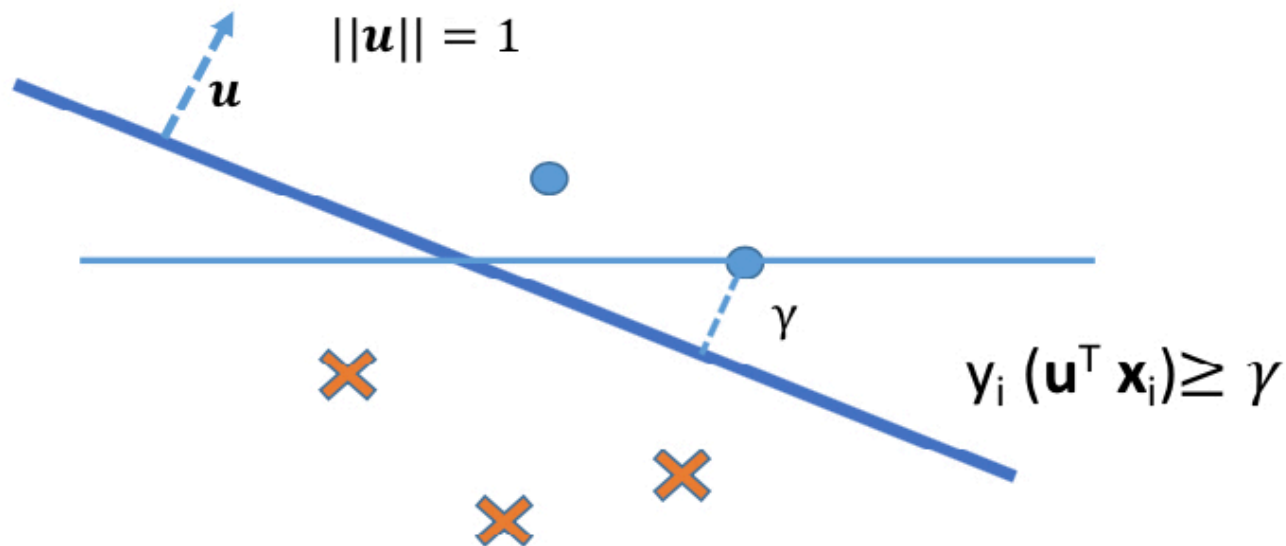
The Mistake Bound Theorem (Novikoff 1962, Block 1962)

- Let $\{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_N, y_N)\}$ be a sequence of training examples such that $\|\mathbf{x}_n\|_2 \leq R$ and label $y_n \in \{-1, +1\}$.



The Mistake Bound Theorem (Novikoff 1962, Block 1962)

- Let $\{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_N, y_N)\}$ be a sequence of training examples such that $\|\mathbf{x}_n\|_2 \leq R$ and label $y_n \in \{-1, +1\}$.
- Suppose there exists a unit vector $\mathbf{u} \in \mathbb{R}^D$ such that for some $\gamma > 0$, we have $y_n \mathbf{u}^T \mathbf{x}_n \geq \gamma$.



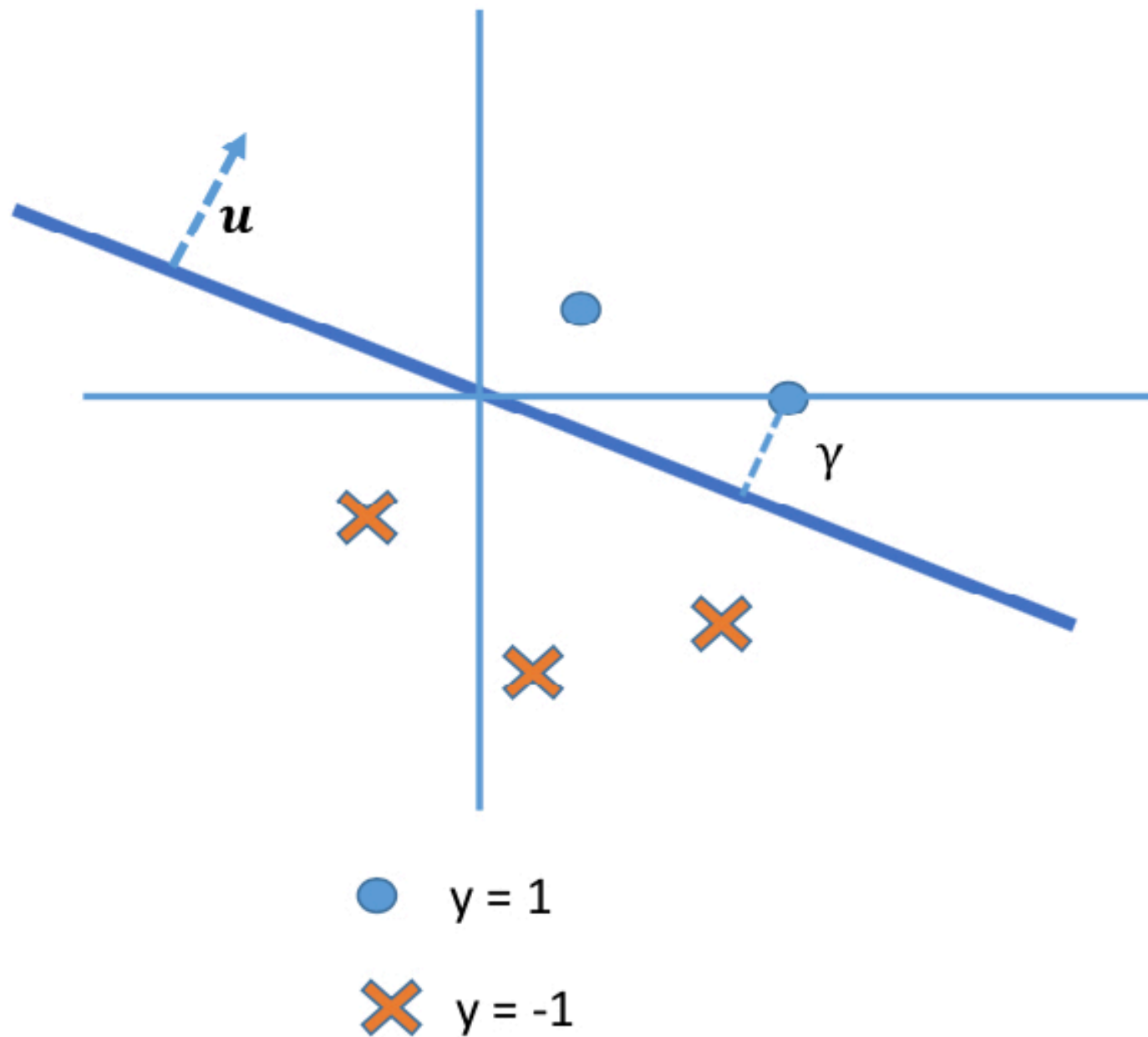
The Mistake Bound Theorem (Novikoff 1962, Block 1962)

- Let $\{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_N, y_N)\}$ be a sequence of training examples such that $\|\mathbf{x}_n\|_2 \leq R$ and label $y_n \in \{-1, +1\}$.
- Suppose there exists a unit vector $\mathbf{u} \in \mathbb{R}^D$ such that for some $\gamma > 0$, we have $y_n \mathbf{u}^T \mathbf{x}_n \geq \gamma$.
- Then the Perceptron algorithm will make at most $\frac{R^2}{\gamma^2}$ mistakes on the training sequence.

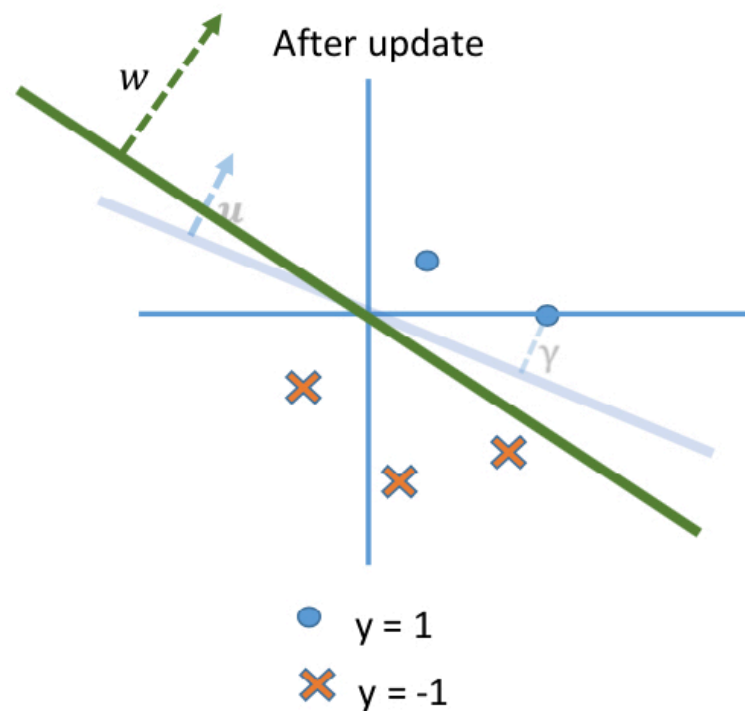
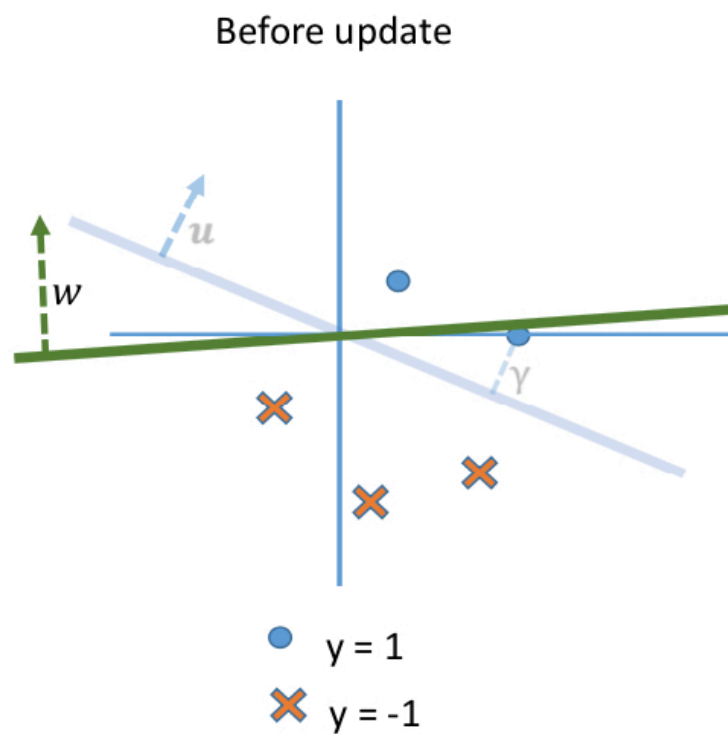
The Mistake Bound Theorem (Novikoff 1962, Block 1962)

- If the data is separable....
- then the perceptron algorithm will find a separating hyperplane after making a finite number of mistakes.

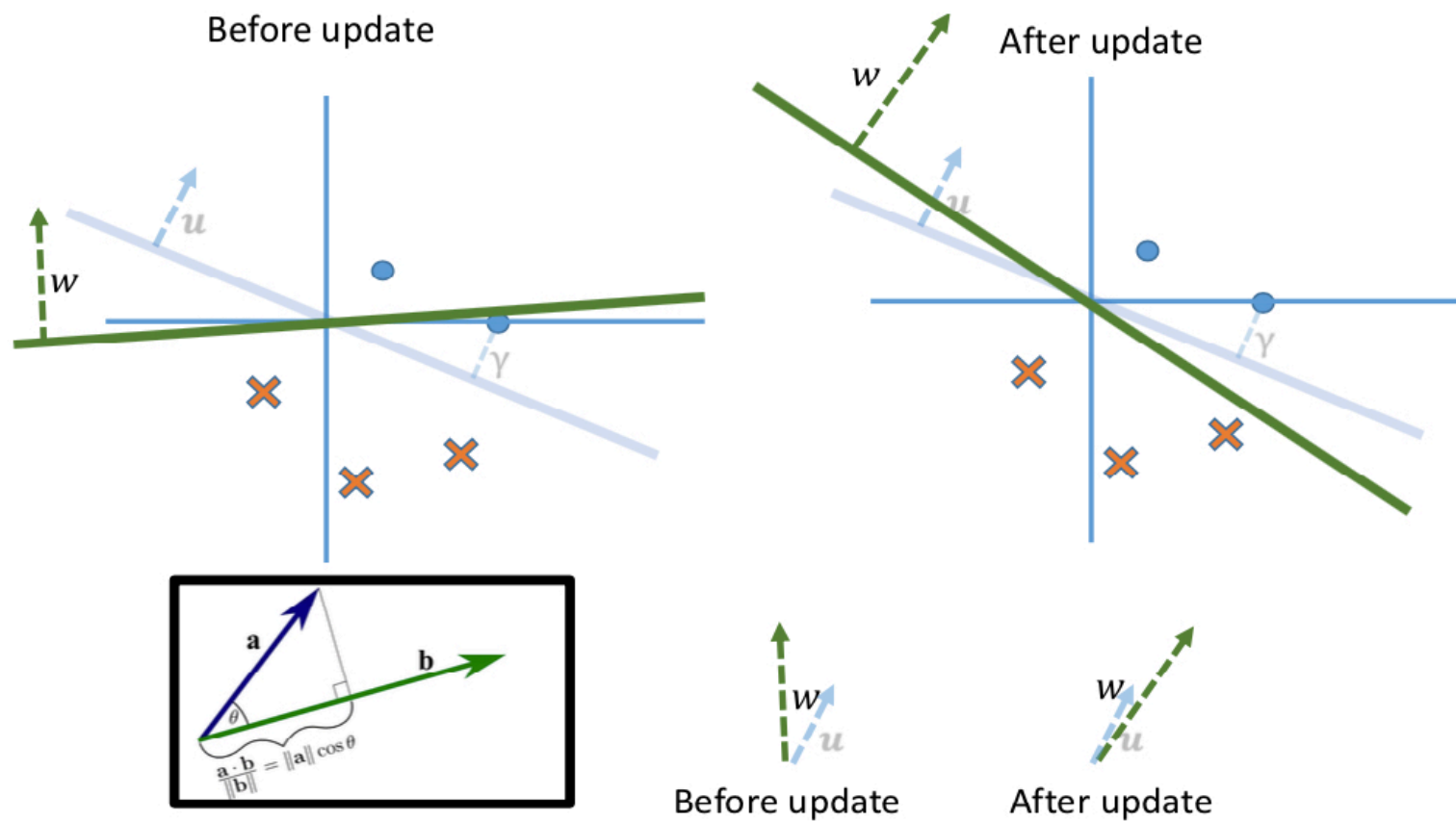
Intuition



Intuition

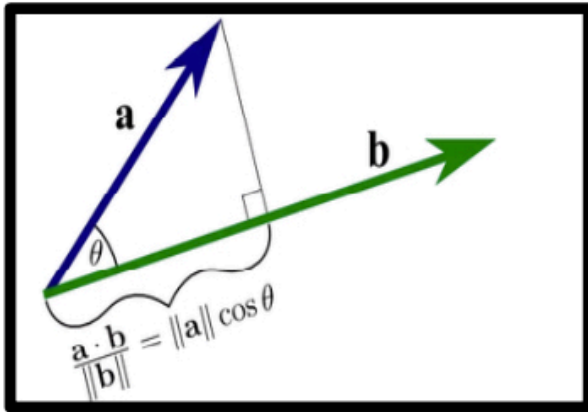


Intuition

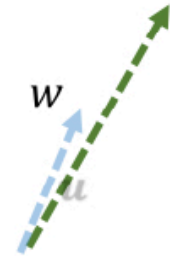


Intuition

- After update, $\mathbf{u}^\top \mathbf{w}_{t+1}$ is larger than $\mathbf{u}^\top \mathbf{w}_t$.
 - ▶ After t mistakes, $\mathbf{u}^\top \mathbf{w}_t \geq t\gamma$.
- The size of $\|\mathbf{w}_{t+1}\|$ may increase but not too much.
 - ▶ After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$.



Before update



After update

Proof (Preliminaries)

Setting

- Initial weight vector $\mathbf{w}_0 = \mathbf{0}$.
- All training examples are contained in a ball of size R .
 $\|\mathbf{x}_n\| \leq R$.
- The training data is separable by a margin γ using a unit vector \mathbf{u} .
 $y_n \mathbf{u}^T \mathbf{x}_n \geq \gamma$.

Proof (1/3)

Claim 1: After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.

$$\begin{aligned}\mathbf{u}^T \mathbf{w}_{t+1} &= \mathbf{u}^T (\mathbf{w}_t + y_n \mathbf{x}_n) \\ &\geq \mathbf{u}^T \mathbf{w}_t + \gamma\end{aligned}$$

Because $\mathbf{w}_0 = 0$, simple induction gives us: $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.

$$\begin{aligned}a &\leftarrow \mathbf{w}^T \mathbf{x} \\ \text{if } ay \leq 0 &\text{ then} \\ \mathbf{w} &\leftarrow \mathbf{w} + y\mathbf{x}\end{aligned}$$

Proof (1/3)

Claim 1: After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.

$$\begin{aligned}\mathbf{u}^T \mathbf{w}_{t+1} &= \mathbf{u}^T (\mathbf{w}_t + y_n \mathbf{x}_n) \\ &\geq \mathbf{u}^T \mathbf{w}_t + \gamma\end{aligned}$$

Because $\mathbf{w}_0 = 0$, simple induction gives us: $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.

```
a ← wTx
if ay ≤ 0 then
  w ← w + yx
```

The inner product between the true underlying model and the current model is non-decreasing after each update. **This could be because the directions of \mathbf{w} and \mathbf{u} align or because the length of \mathbf{w} increases.**

Proof (2/3)

Claim 2: After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$\begin{aligned}\|\mathbf{w}_{t+1}\|^2 &= \|\mathbf{w}_t + y_n \mathbf{x}_n\|^2 \\ &= \|\mathbf{w}_t\|^2 + 2\mathbf{w}_t^T(y_n \mathbf{x}_n) + \|y_n \mathbf{x}_n\|^2\end{aligned}$$

Proof (2/3)

Claim 2: After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$\begin{aligned}\|\mathbf{w}_{t+1}\|^2 &= \|\mathbf{w}_t + y_n \mathbf{x}_n\|^2 \\ &= \|\mathbf{w}_t\|^2 + 2\mathbf{w}_t^T (y_n \mathbf{x}_n) + \|y_n \mathbf{x}_n\|^2 \\ &= \|\mathbf{w}_t\|^2 + 2y_n (\mathbf{w}_t^T \mathbf{x}_n) + y_n^2 \|\mathbf{x}_n\|^2\end{aligned}$$

```
a ← wTx
if ay ≤ 0 then
  w ← w + yx
```

Proof (2/3)

Claim 2: After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$\begin{aligned}\|\mathbf{w}_{t+1}\|^2 &= \|\mathbf{w}_t + y_n \mathbf{x}_n\|^2 \\ &= \|\mathbf{w}_t\|^2 + 2\mathbf{w}_t^T(y_n \mathbf{x}_n) + \|y_n \mathbf{x}_n\|^2 \\ &\leq \|\mathbf{w}_t\|^2 + R^2\end{aligned}$$

Because $\mathbf{w}_0 = 0$, simple induction gives us: $\|\mathbf{w}_t\|^2 \leq tR^2$.

Proof (3/3)

What we know

- ① After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.
- ② After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

The inner product between the true underlying model and the current model is non-decreasing after each update. This could be because the directions of \mathbf{w} and \mathbf{u} align or because the length of \mathbf{w} increases.

But the length of \mathbf{w} does not increase too much!.

Proof (3/3)

What we know

- ① After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.
- ② After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$R\sqrt{t} \geq \|\mathbf{w}_t\|$$

Proof (3/3)

What we know

- ① After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.
- ② After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$R\sqrt{t} \geq \|\mathbf{w}_t\| \geq \mathbf{u}^T \mathbf{w}_t$$

Proof (3/3)

What we know

- ① After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.
- ② After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$R\sqrt{t} \geq \|\mathbf{w}_t\| \geq \mathbf{u}^T \mathbf{w}_t \geq t\gamma$$

Proof (3/3)

What we know

- ① After t mistakes, $\mathbf{u}^T \mathbf{w}_t \geq t\gamma$.
- ② After t mistakes, $\|\mathbf{w}_t\|^2 \leq tR^2$

$$R\sqrt{t} \geq \|\mathbf{w}_t\| \geq \mathbf{u}^T \mathbf{w}_t \geq t\gamma$$

Number of mistakes $t \leq \frac{R^2}{\gamma^2}$.

Bounds the total number of mistakes!

Beyond the separable case

- Good news
 - ▶ Perceptron makes no assumptions about the data, could be even adversarial.
 - ▶ After a fixed number of mistakes, you are done. Do not need to see any more data.
- Bad news
 - ▶ Real world data is often not linearly separable.

Outline

- 1 Perceptron
- 2 Perceptron learning
- 3 Convergence of the Perceptron Learning Algorithm
- 4 Variants of perceptron**
- 5 What we have learned

Voting and averaging

- Vanilla perceptron returns final weight vector.
- Might lose good weight vectors that were learned during training.
- Aggregating the models (or weight vectors) seen during training may give better results (especially when data is not separable).

Voted perceptron

- Remember every weight vector in your sequence of updates.
- At final prediction time, each weight vector gets to vote on the label.
- The number of votes it gets is the number of iterations it survived before being updated
- Comes with strong theoretical guarantees about generalization, impractical because of storage issues

Averaged perceptron

- Instead of using all weight vectors, use the average weight vector (i.e. longer surviving weight vectors get more say)
- More practical alternative and widely used

Averaged Perceptron training/learning

$data = N$ **samples/instances:** $= \{(x_1, y_1), \dots, (x_N, y_N)\}$

Algorithm 2 AveragedPerceptronTrain ($data, maxIter$)

```
1:  $w \leftarrow 0$ .  $\mu \leftarrow 0$ .
2: for  $iter = 1 \dots MaxIter$  do
3:   for  $(x, y) \in data$  do
4:      $a \leftarrow w^T x$ 
5:     if  $ay \leq 0$  then
6:        $w \leftarrow w + yx$ 
7:     end if
8:      $\mu \leftarrow \mu + w$ 
9:   end for
10: end for
11: return  $\mu$ 
```

Prediction: $sign(\mu^T x)$.

Perceptron

- Extensions
 - ▶ Voting
 - ▶ Averaging
- Limitations
 - ▶ Linear separability
- Interpreting the importance of features
 - ▶ The values of weight w_d tells us the importance of feature x_d .

Outline

- 1 Perceptron
- 2 Perceptron learning
- 3 Convergence of the Perceptron Learning Algorithm
- 4 Variants of perceptron
- 5 What we have learned

Summary

- You should now be able to understand the differences between decision trees, perceptrons and nearest neighbors.
- Given data, use training, development and test splits (or cross-validation).
- Use training and development to tune hyperparameters that trades off overfitting and underfitting.
- Use test to get an estimate of generalization or accuracy on unseen data.