# ***I14: Klasifikátory a jejich učení - nejbližší soused, lineární klasifikátor, Adaboost, SVM, rozhodovací stromy, neuronové sítě. (RPZ)***

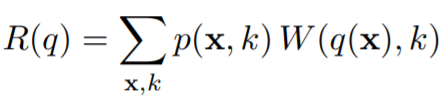
## Klasifikátory a jejich učení

“Objekt zájmu je charakterizován pozorovatelnými vlastnostmi *x* ∈ *X* a svou příslušností ke třídě (nezsjistitelný/skrytý stav) *k* ∈ *K*. (*X* je prostor pozorování a *K* je množina skrytých stavů / tříd)”

Cílem klasifikátoru je najít strategii *q*\*: X → K, která splňuje určité optimální vlastnosti.

Učení klasifikátorů - snižování risku.

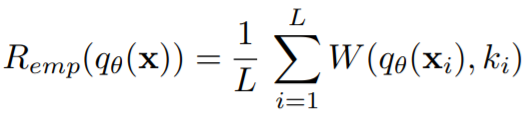
**Pokud známe rozdělení pravděpodobnosti,** chceme snižovat Bayesovský risk:



**Pokud neznáme pravděpodobnosti:**

1. Předpokládáme, že *p*(*x*,*k*) má určitou formu/tvar (např. mix gaussiánů, apod.) s konečným (malým) počtem parametrů *θk*.
2. Chceme odhadnout (určit) tyto parametry z trénovací množiny *T*.

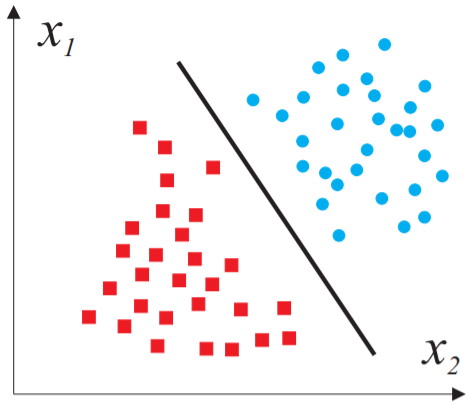
V tomto případě snižujeme empirický risk = Remp = Chyba na trénovací množině

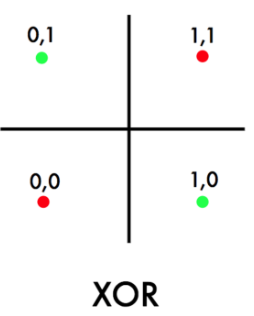
 → 

Minimalizace empirického risku může vést k overfitování.

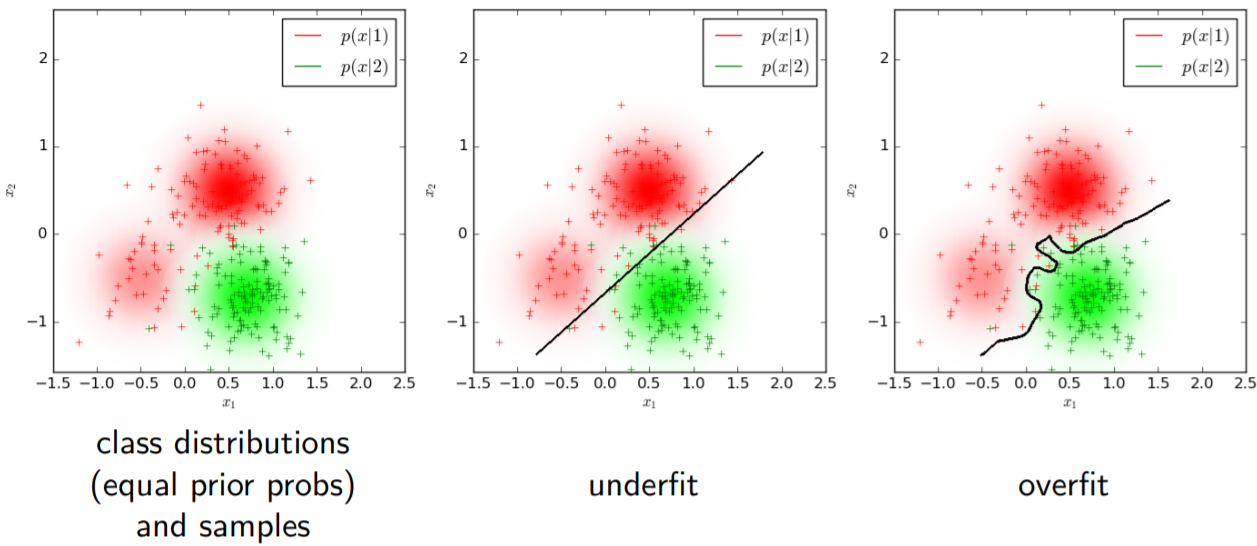
(Problém generalizace je klíčový problém v rozpoznávání patternů. Malý Remp ⇏ malý opravdový risk)

*Další, kdo chce jít do hloubky: Vapnik and Chervonenkis inequality a VC dimenze*

Lineárně separabilní (oddělitelná) data

* lineární klasifikátor je bezchybně oddělí: ––––––––––––––––––->
* XOR problém - lineárně neseparabilní data nejde oddělit lineárním klasifikátorem

Přeučený klasifikátor vede k overfittingu *(tedy když se natrénuje “příliš přesně” podle trénovacích dat)*:



## Lineární klasifikátor

Vhodný pro lineárně oddělitelné množiny (ale vstupní data typicky obsahují chyby/šum a pak tento jednoduchý přístup není použitelný) – předpokládáme, že data jsou lineárně separovatelná (klasifikovatelná).

Lineární klasifikátor ... nadrovina – *g*(***x***) = ***w***T***x*** + *w*0 = 0

*d* ... dimenze vstupního prostoru, ***w*** = (*w*1, ..., *w*d) ... váhový vektor, *w*0 ... práh

rozdělení prostoru na dvě části: jedna strana (*g*(***x***) > 0) a druhá strana (*g*(***x***) < 0)

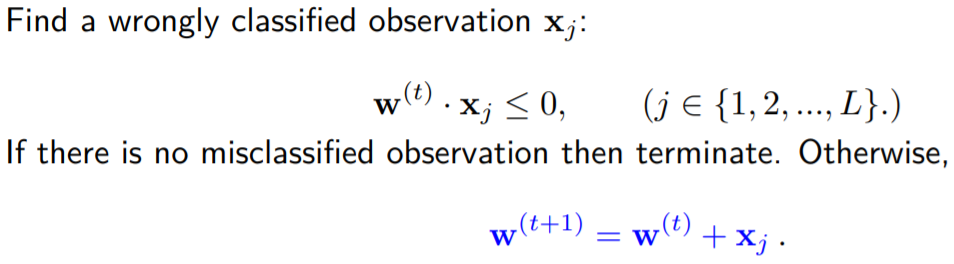
Příklady lineární klasifikace: Perceptron, Logistická regrese, SVM, Bayesovský klasifikátor

**Perceptron** - cílem nalézt parametry *w*0, *w*1, … *w*d

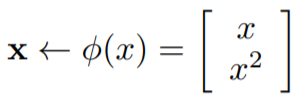
* Pro lineárně separabilní množiny existuje nadrovina ***w***\*T·***x*** = 0:

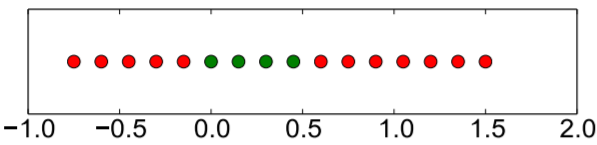
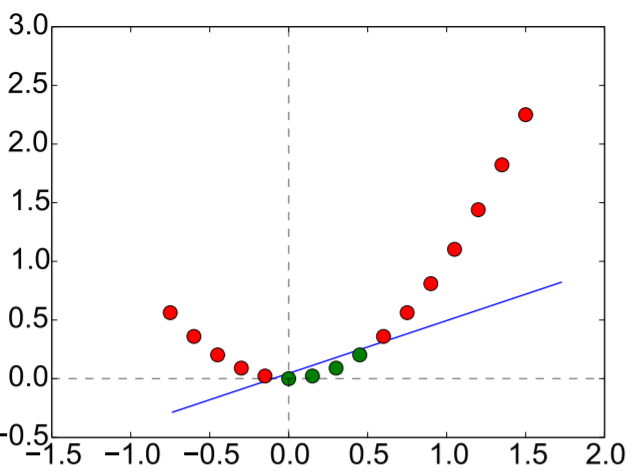
***w***\*T·***x*** > 0 pro každý x z ω1 a ***w***\*T·***x*** < 0 pro každý x z ω2

* Zavádí se rozšířený (d+1)-dimenzionální prostor: ***w***’ ≡ [***w***\*,*w*0], ***x***’ ≡ [***x***,1]  
   → pak ***w***\*T·***x*** + ***w***\*0 = ***w***’T·***x***’
* Perceptronový algoritmus zkonverguje k řešení (nějakému) v konečném počtu kroků pokud jsou data lineárně separabilní, jinak pojede napořád
* Nalezená řešení jsou nejednoznačná → existuje více než jedna dělící nadrovina (nemusí být “nejlepší” - ve smyslu třeba max. šířky marginu (pásu) jako SVM)
* Algoritmus:
  + inicializace: ***x***’ ≡ [***x***,1] → ***x***i = ***x***i\**y*i (*y*i e {-1,1}) , ***w’*** = zeros(D+1)
  + přidáváme do vektoru *w* chybně klasifikovaný bod v dané iteraci

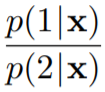


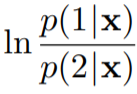
* + Terminace pokud jsou všechny body klasifikovány správně.
* Co když data nejsou **lineárně separabilní?**: dimension lifting

**Dimension lifting** – příklad:: (fi…. mapping function)

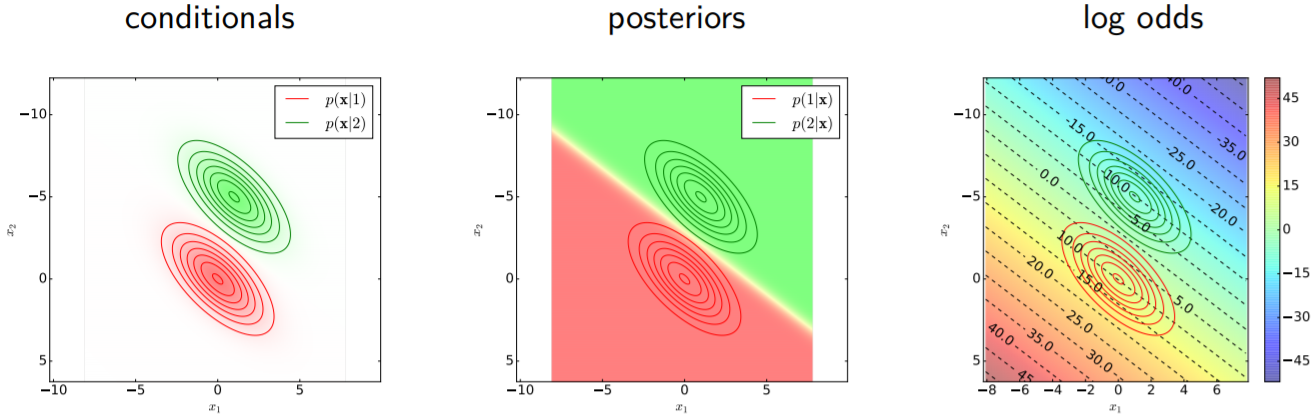
 → 

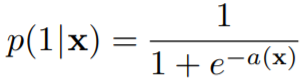
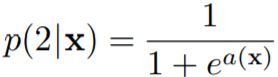
**Logistická regrese** (viz. I13)

Poměr posteriorních pravděpodobností  je nazýván odds ratio.

Zlogaritmováním získáváme log odds:

*Příklad*:



Posteriorní pravděpodobnosti (*posteriors*) lze modelovat takto: , 

  
a obrácené znaménko pro q(x) = 2

Odhad parametrů daného modelu se provádí obvykle metodou maximální věrohodnosti.

Generativní vs. diskriminativní přístup:

## Nejbližší soused (1-NN)

Objekt je jednoduše přiřazován ke svému nejbližšímu sousedu.

Pro n → inf: chyba 1-NN klasifikace </= 2eB

## Metoda nejbližších sousedů = K-NN

* **Vlastnosti**

(+) jednoduchá implementace (naivní řešení - složitost: D\*N)

(+) pro 1-NN: lze najít upper-bound () a lower-bound: єB (єB = Bayes error)

(+) není potřeba předpoklad na distribuci, ze které data pocházejí

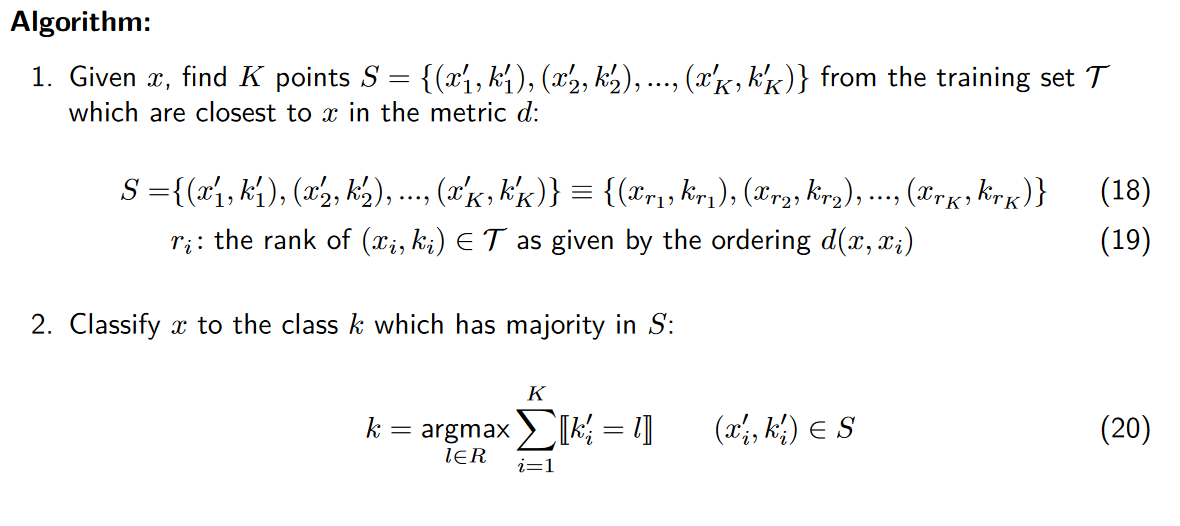
(+) pro libovolný počet tříd

(-) při naivní implementaci pomalé, vysoké nároky na paměť počítače (příp. nutná úprava dat) → lze urychlit *(viz. níže)*: redukcí trn. množiny, pomocí k-D trees *nebo Voronoi*

(-) není jasné jak zkonstruovat metriku *d*  
 (potenciální problém: různý význam různých dimenzí)

(-) vysoké nároky na paměť  
(-) může overfitovat

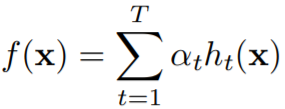
* **Algoritmus**
  + Máme trénovací množinu T = {(xi, ki)}1 <= i <= N. Pro testovací bod y nalezneme k nejbližších trénovacích bodů xi a y ohodnotíme jako té třídy, která má mezi k nejbližšími body většinu.

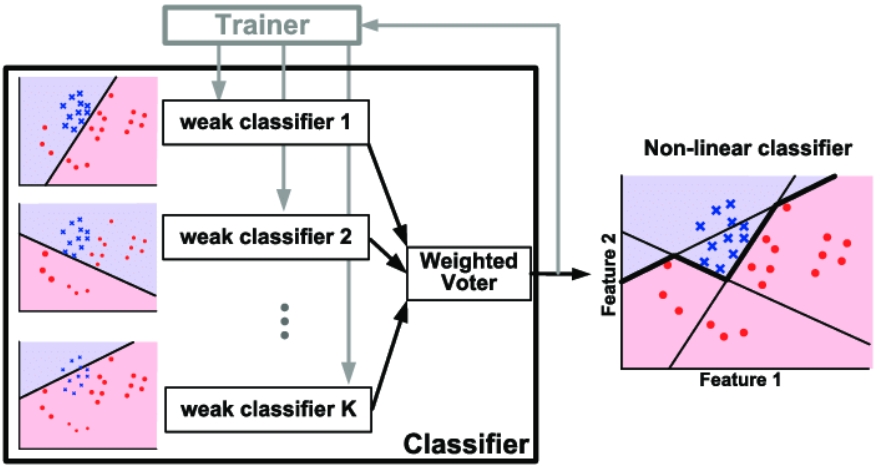


* **Urychlení** klasifikátoru K-NN:
  + redukcí trénovací množiny: snížení N např. z tisíců na desítky
  + pomocí k-D stromů: ty urychlují vyhledávání podle vzdálenosti v geometrickém prostoru pomocí ukládání dat ve stromové struktuře. Při procházení stromu se pro každou větev určí minimální možná vzdálenost nejbližšího bodu ve větvi od posuzovaného bodu. Po prvním projití do listu pak můžeme ořezat větve, které jistě nemají bližší bod. Je to sublineární vyhledávání, ale složitost je funkcí dat, nejde tedy garantovat.
  + pomocí Voronoiových diagramů: při klasifikaci stačí zjistit v jaké buňce bod leží  
    (rychlejší než počítat vzdálenosti)

## Adaboost

Kombinuje vícero klasifikátorů do jednoho silného klasifikátoru. Výstup dílčích slabých klasifikátorů je kombinován do váženého součtu, který představuje konečný výstup silného klasifikátoru.

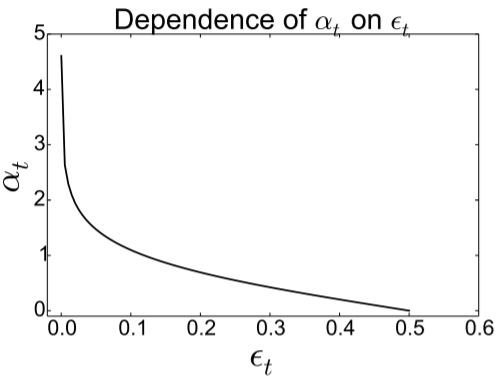
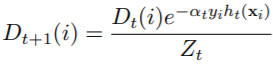
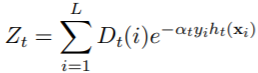
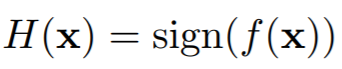
Silný klasifikátor *H*: ,  (*h*t je slabý klasifikátor)

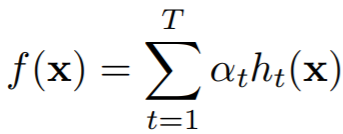
* **Vlastnosti**:

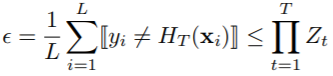
(+) jednoduchá implementace

(+) dobrá generalizace (= chová se dobře k testovacím datům po natrénování, neoverfituje moc)

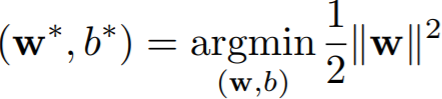
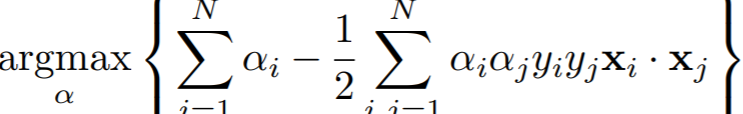
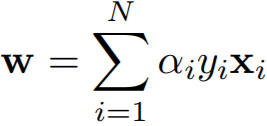
(-) overfitting kvůli noise

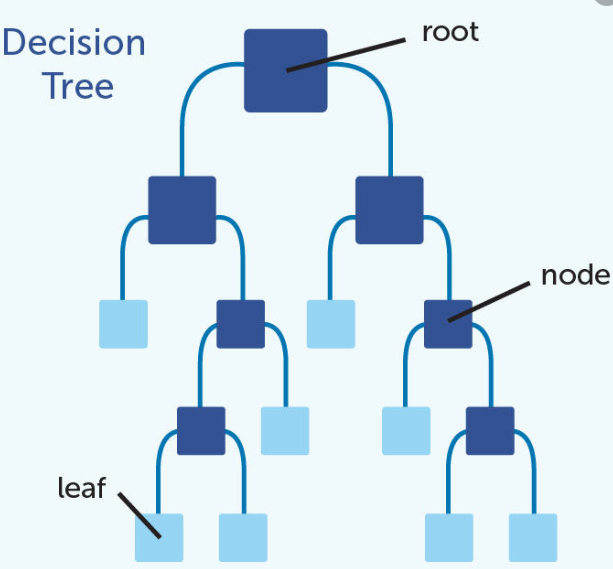
* množina *B* slabých klasifikátorů *h*i(*x*)
* **Algoritmus**:
  + Init: t=1, Dt=1(i)=1/N
  + vyberu ht(x) s nejmenší chybou єt: 
    - divná závorka dá jedničku pokud výraz uvnitř platí, jinak nulu (tj. při chybě → 1)
  + pro vybraný slabý klasifikátor ht mám chybu єt
    - pokud єt = 0,5 ⇒ terminace algoritmu
  + Váha daného slabého klasifikátoru: 
  + Update vah dat: , normalizační faktor Zt: 
    - normalizační faktor lze vypočítat také takto: 
  + Nakonec (po ukončení iterování) – výsledný (silný) klasifikátor: ,



* *Upper bound theorem:* 

## SVM

* lineární klasifikátor; nachází optimální řešení (dělící nadrovina maximalizuje šířku dělícího pásu); lze upravit i pro lin. neseparabilní data; (w, b)\* = argmaxw,b mini d(xi) za podmínky yi(wTxi + b) > 0, kde d(xi) je vzdálenost xi od nadroviny
* T = {xi, yi} (i=1...N), xi ∈ RD, yi ∈ {-1,1}
* primární formulace: , tj. argmax 1/IIwII, w ∈ RD, b ∈ R
* duální f: α\*= (podm: α >= 0, Sumi yiαi = 0)  
  → pomocí QP najdeme glob. optimum
* strategie pak: , (pouze α>0, tj. SV (ostatní mají α=0))
* učení pomocí iteračních metod, funkce je konvexní → dospěje do globálního minima
* Soft margin SVM: pro nesep. data představíme C – ztráta za špatně klasifikovaný bod; ; Primární úloha: (w, b)\* = argminw,b ½||w||2 + C\*Sumi ξi za podmínky yi(wTxi + b) >= 1 - ξi, ξi >= 0; Duální úloha: α\* = argmaxα Sumi αi - ½ Sumi Sumj αiαjyiyjxiTxj za podmínky 0 <= α <= C, Sumi yiαi = 0
* Při použití dimension lifting φ(x): RD -> RM nemusíme používat/znát přímo předpis mapování. Stačí znát kernel funkci K(x, y) = φ(x)Tφ(y). Tou lze nahradit například i mapování do teoreticky nekonečně dimenzionálních prostorů apod. Učení SVM probíhá stejně, pouze duální úloha přijme kernel funkci: α\* = argmaxα Sumi αi - ½ Sumi Sumj αiαjyiyiK(xi, xj) za podmínky 0 <= α <= C, Sumi yiαi = 0
* Klasifikace má dva způsoby:
  + použijeme mapování φ(x): Získáme w = Sumi z SV αiyiφ(xi), b = ysv - wTφ(xsv) a klasifikujeme: q(z) = sign(wTφ(z) + b); To znamená, že musíme znát φ a klasifikace je zpomalena oproti lineární variantě výpočtem φ(z)
  + použijeme kernel K(x, y): b = ysv - Sumi z SV αiyiK(xi, xsv) ; q(z) = sign(b + Sumi z SV αiyiK(xi, z)); To znamená, že si musíme pro klasifikaci pamatovat αi, yi, xi pro support vektory a klasifikace je zpomalena výpočtem Sumi z SV αiyiK(xi, z)
* časová složitost závislá na N (ne na D; při optimalizaci jsou počítány skalár. součiny xiT,xj)
* rychlost učení závisí na inicializaci
* dobře generalizuje, používají pouze skalární součiny dat, tzn. že jsou nezávislé na vstupní dimenzi, umí pracovat i s neseparabilními daty, při klasifikaci stačí znát pouze w a b, lze zobecnit pro oddělení nelineárně separovatelných dat pomocí dimension lifting a kernel triku.
* SVM se složitě zobecňují pro oddělení více tříd a nehodí se do inkrementálního učení.
* *Perceptron vs SVM*
  + Perceptron nalezne nějaké řešení, SVM “dobré” (maximalizující margin)
  + u perceptronu pro separabilní data zaručena konvergence (Novikoff teorém)

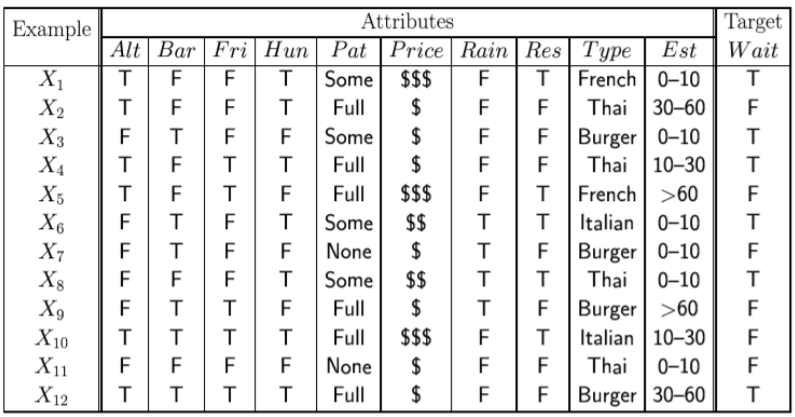


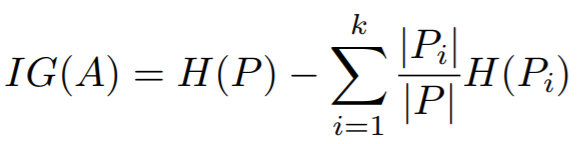
## Rozhodovací stromy (decision trees)

Výhodou je interpretovatelnost (*srovnejme např. s neuronovou sítí, kde takřka nevíme nic, co parametry znamenají*), zde vidíme podle kterých atributů se rozhoduje

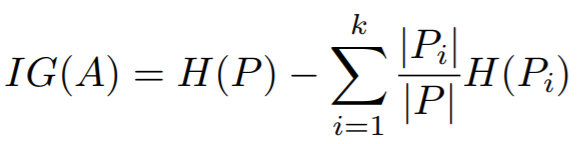
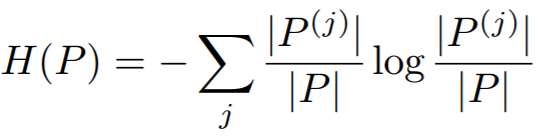
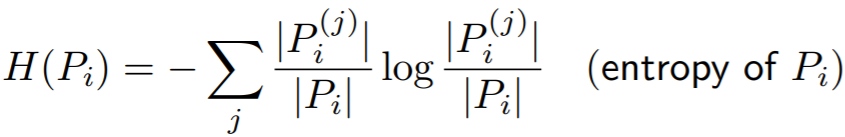
**Příklad – restaurace: *(viz. tabulka níže)***

* Atributy
  + Fri = Je pátek? → T/F
  + Price → $/$$/$$$
  + Rain? → T/F
* atributy mohou být různé datové typy (boolean, integer; diskrétní/spojité)
* Klasifikuje do dvou tříd: True nebo False (Wait nebo neWait)



Information Gain (*IG*) pro daný atribut (*A*): 

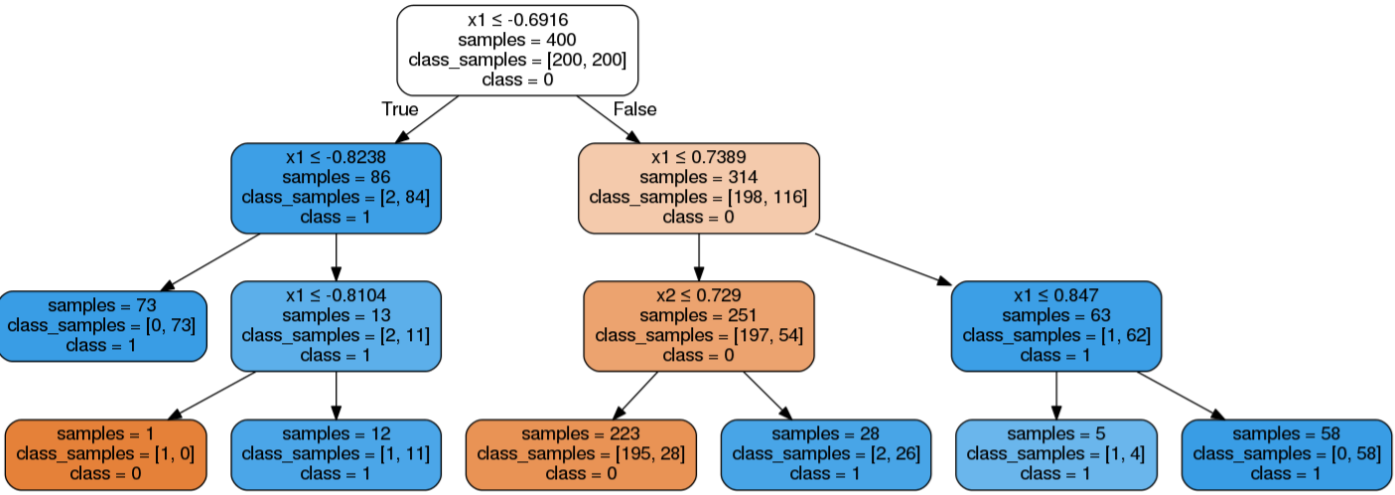
Při trénování (učení) rozhodovacího stromu - trénování na trénovacích datech:

* Spočítám IG pro každý atribut ()
  + Ten atribut, u kterého vyjde nejvyšší, ten použiju.
  + *kde P(j) je počet bodů které spadnou do j-té dané třídy*
  + *entropy of Pi:* 

To odpovídá tomu, že se snažím co nejvíc snižovat entropii.

Entropie:

* *log2; informační entropie [bit]: vysoká = nic nevím, nízká = vím co se stane*



**(+) Výhody**

* Interpretovatelnost
* Rychlost rozhodování
* nepotřeba použít všechny měření - jen ty relevantní
* outliers ošetřeny speciální větví
* pro klasifikační i regresní úlohy

**(–) Nevýhody**

* Neexistuje efektivní způsob trénování (všechny na bázi greedy algoritmu *→ není záruka optimality*)
* Hrozí overfitting *(→ proti tomu se používají randomizované stromy)*

**Top-down** je příkladem greedy algorimtu (“hladový”) → nemusí být “nejlepší”

Na začátku nastavím P=T  
spočítám IG pro každý atribut, zvolím pro dělení ten který mi dá nejvyšší IG  
rekurze pro větve

## Decision trees vs. SVM

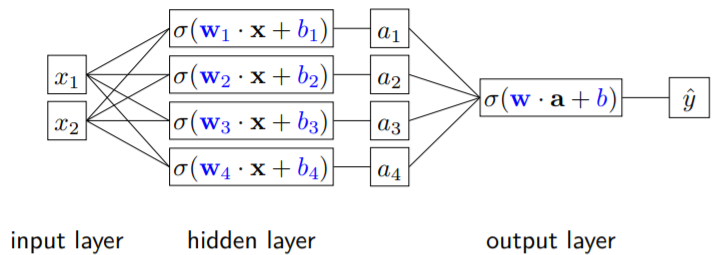
* *DT: žádné záruky na generalizaci/optimalitu řešení X SVM: dobře generalizuje, jelikož minimalizuje VC dimenzi maximalizací margin mezi třídami dat, díky konvexnosti rozhodovací funkce a QP optimalizaci nalezne globální optimum*
* *DT: pro jakékoliv prostory, i nenumerické, s různými hodnotami/měřítky v různých dimenzích, apod. X SVD: jen pro data z RD*
* *trénovací množina může být libovolně velká, při klasifikaci se nevyužívá (klasifikace je sublineární vůči dimenzi dat) X trénovací množina může být libovolně velká, při klasifikaci se nevyužívá, pouze se z její části (tzv. support vektorů) vypočítá lineární klasifikátor q(x) = sign(wTx)*
* *při učení je potřeba uchovávat veškerá data, při klasifikaci pak již DT samotný (posloupnost otázek/rozhodnutí) X při učení stačí uchovávat skalární součiny všech xi, pro klasifikaci stačí uchovávat jediný vektor w z RD*
* *učení je závislé na složitosti stromu, respektive nic jako učení neprobíhá, strom je pouze sestaven, při stavbě stromu lze dodržovat určitá pravidla pro jeho obecně lepší klasifikaci (TDIDT) X učení je závislé na velikosti trénovací množiny a rychlosti konvergence QP optimalizace, která kriticky závisí na počáteční inicializaci*
* *odchýlené hodnoty lze jednoduše odchytávat jako speciální větve stromu X vliv odchýlených hodnot lze regulovat velikostí ztráty za špatně klasifikovaný bod C, ta určuje směr “úzký margin bez špatně klasifikovaných bodů (vyšší C)” vs “širší margin se špatně klasifikovanými body (nižší C)”*

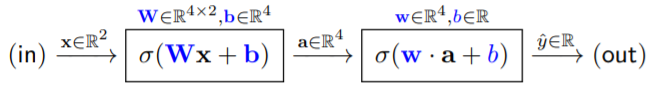
## Neuronové sítě

*Doporučuju:* [*3Blue1Brown - YT*](https://www.youtube.com/playlist?list=PLZHQObOWTQDNU6R1_67000Dx_ZCJB-3pi)

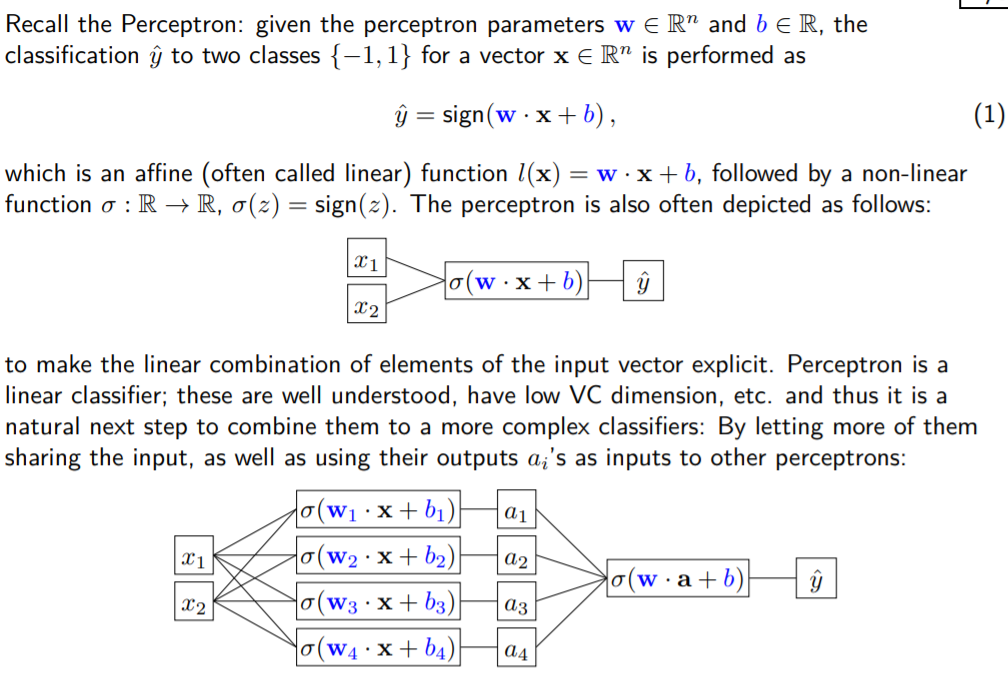
**Vrstvy**

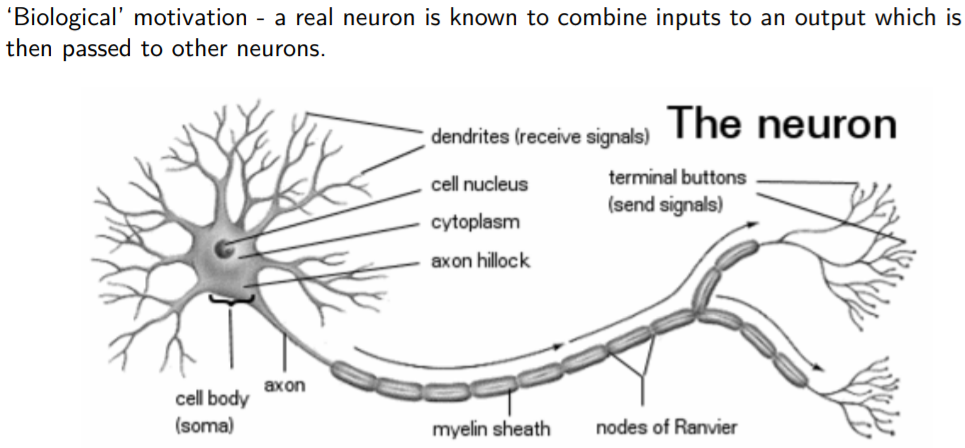
Příklad s jednou skrytou vrstvou: (jinak jich je obvykle více)



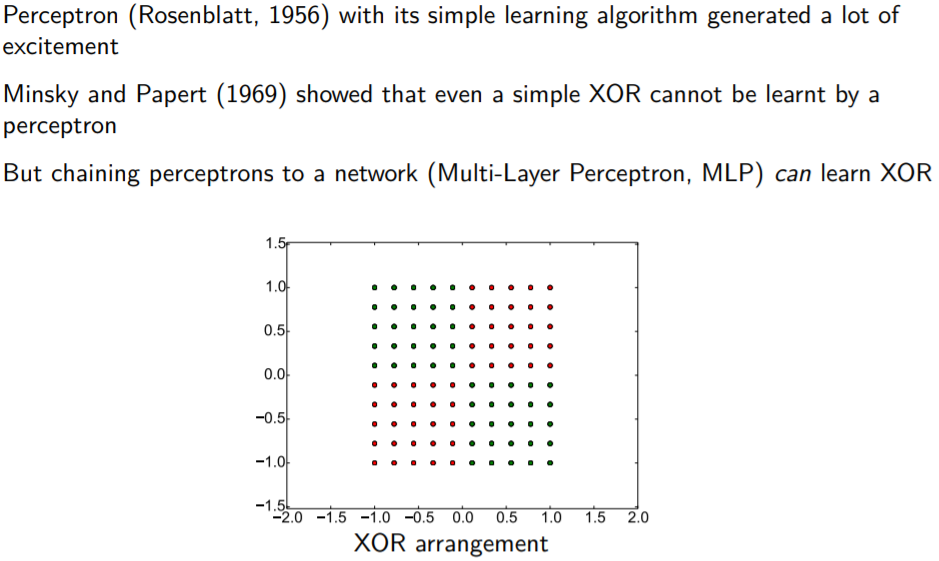
, což je to samé co

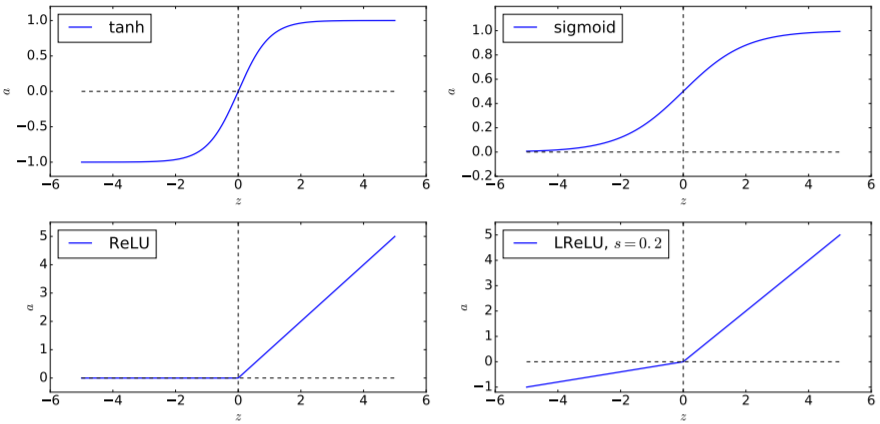
**Motivace**





**Historická poznámka**





U perceptronu byl na konci threshold, ..

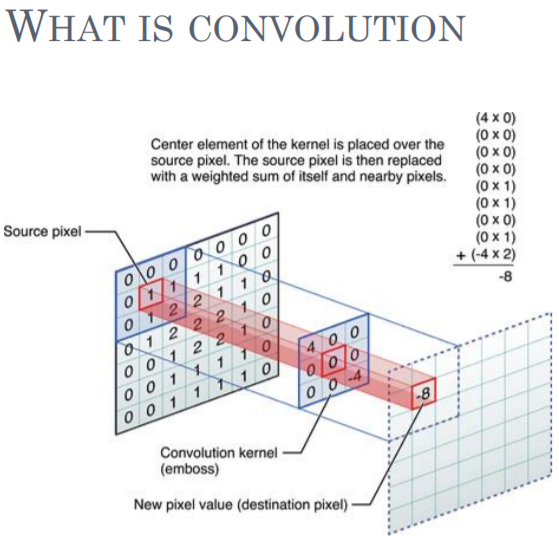
Aktivační funkce mají takovéto tvary:

* sigmoida (logistická *nebo tanh*)
* ReLU (Rectified Linear Unit)
* Leaky ReLU

*Nepoužívá se sign (jako u perceptronu) - ta není diferencovatelná v 0*

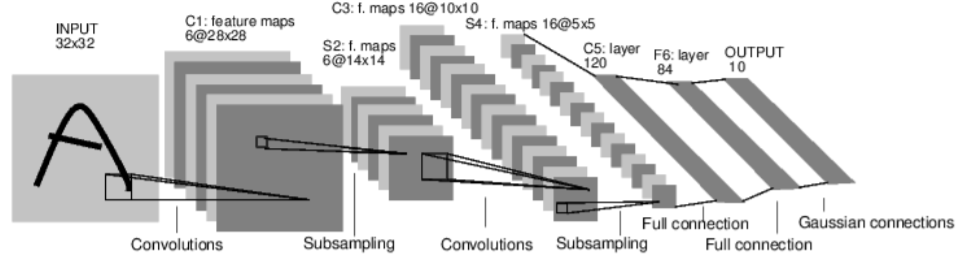
**Gradient a Back propagation:** *3Blue1Brown (LINK nahoře)*

**Neuronové sítě pro Image Recognition (Rozpoznáv**

→ Konvoluční neuronové sítě

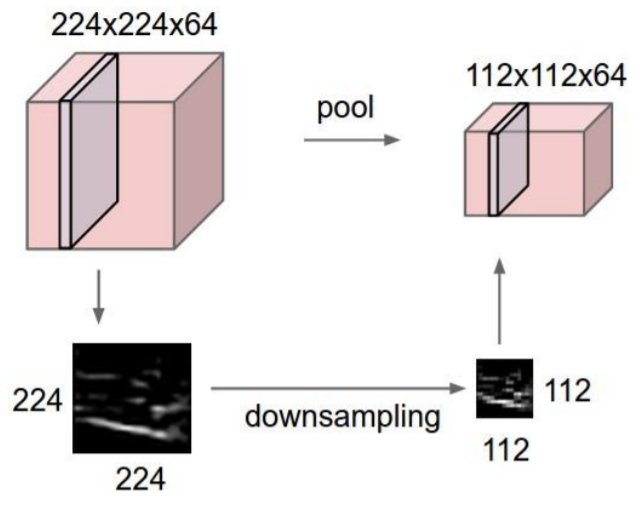
Co je konvoluce? –––––––––––->

Pro ilustraci jak CNN (konvoluční neuronová síť) může vypadat:

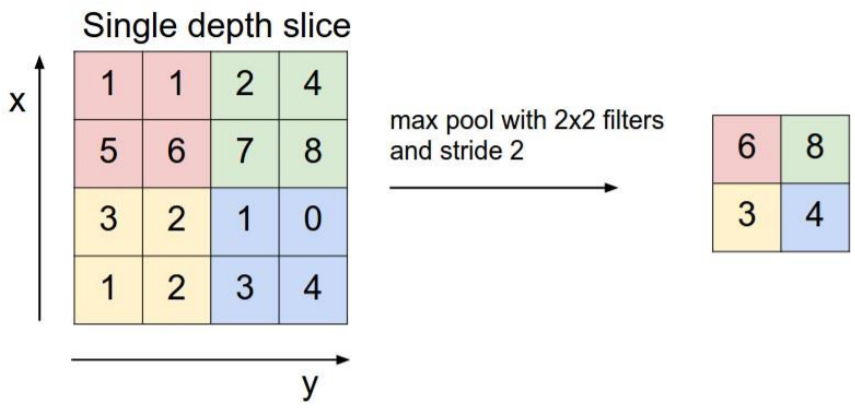
****

**Pooling**

Pooling layers reduce the dimensions of data by combining the outputs of neuron clusters at one layer into a single neuron in the next layer.

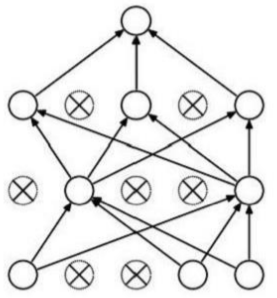
****

* **Max pooling:**

****The maximum pixel value of the batch is selected

* **Min pooling:** The minimum pixel value of the batch is selected.
* **Average pooling:** The average value of all the pixels in the batch is selected.

*Dropout*

**

**Data augmentation** - vytvoří se tak více dat pro trénování

* Náhodná rotace
* Afinní transformace
* Náhodné škálování
* Color augmentation
* Noise input
* Thin plate deformation
* ...cokoliv si umíš přestavit

## Poznámky

*Předpoklad: Features jsou navzájem nezávislé -> pak mluvíme o naive Bayes approach.*

*Neuronové sítě nelze zapsat jako jednu lineární funkci (kvůli aktivační fci, ..)  
 → je popsána tunou parametrů*