

Machine Learning

Rudolf Mayer (mayer@ifs.tuwien.ac.at)

November 27th, 2019



Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines



Exercises

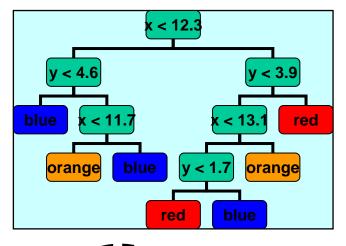
- Exercise 1 (Regression) discussion
 - 28.11. 6.12. (apply if you haven't done it yet)
 - Everyone needs to attend

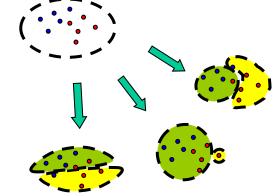
- Exercise 2 (Classification & Exercise 3
 - Need to present either Exercise 2 or Exercise 3
 - You need to attend the whole slot (\sim 2 2,5 hours)
 - All group members should be present
 - Submission: Report for both Exercise 2 & 3
 - In addition a presentation for the one that you present
 - (has a different DL)
 - Dates: December 16 20 resp. January 27 31



Short Recap

- Decision Tree Learning
 - Finding optimal split
 - Categorical attributes
 - Different criteria for optimality
 - Information Gain
 - (Gini Index)
 - Binary & multiple classes
 - Overfitting & (pre)pruning
 - Stability
 - Binary / n-ary trees
 - Categorical & numerical data



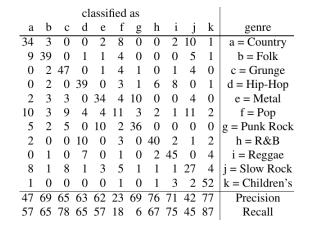




Short Recap

- Evaluation
 - Confusion Matrix
 - Micro vs. Macro averaging

Leave-p-out cross-validation



$$\frac{1}{\mid C \mid} \sum_{i=1}^{\mid C \mid} \frac{TP_{i} + TN_{i}}{TP_{i} + FP_{i} + TN_{i} + FN_{i}}$$

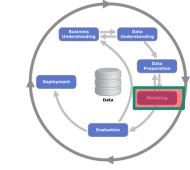




Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines

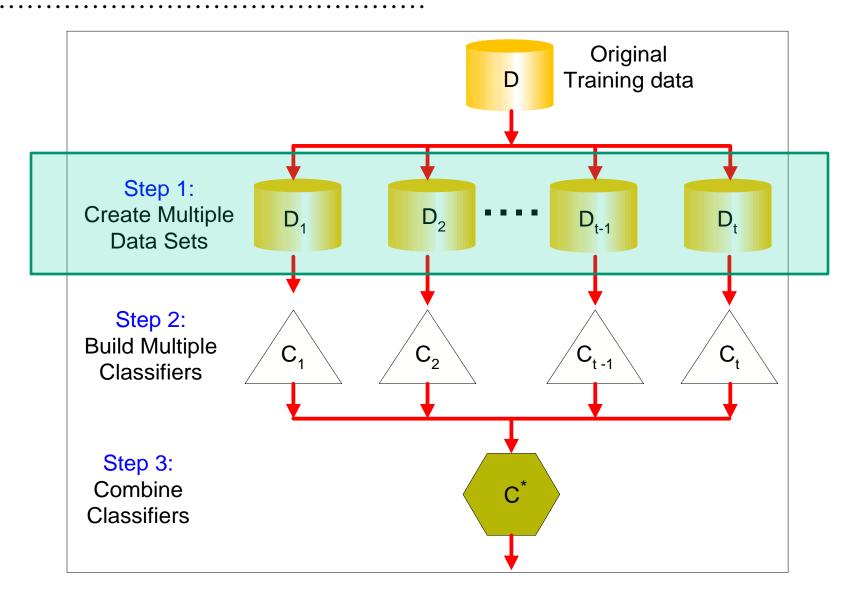




- Combination of Decision Tree and Bootstrapping concepts
- Proposed ~1995
 - by Leo Breiman & Adele Cutler
- Basic Idea & Name
 - a large number of decision trees is "grown in the forest"
 - each on a different bootstrap sample
 - Utilises instability of Decision Trees









For each tree: use bootstrap sample



- For each tree: only a random number of the original variables is available
 - i.e. small selection of columns
 - much smaller than original number
 - Change at each tree node!



No stopping, no pruning





Input

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
sunny	80	90	true	Don't Play
overcast	83	78	false	Play
rain			false	Play
rain	68	80	false	Play
rain	65	70	true	Don't Play
overcast	64	65	true	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
sunny	75	70	true	Play
overcast	72	90	true	Play
overcast	81	75	false	Play
rain	71	80	true	Don't Play



Input

Output

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play

Bootstrap sample



Input

Output

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play

?



Input

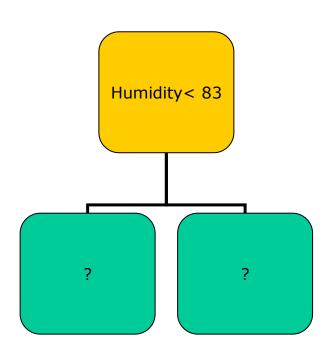
Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play





Input

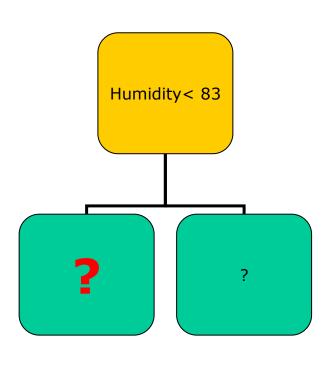
Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play





Input

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play

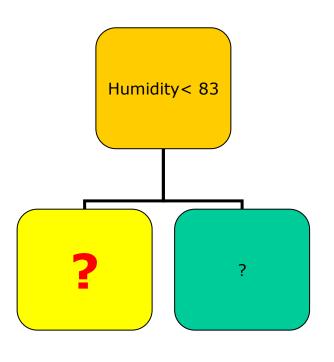




Input

Output !! Select new attributes at each tree node!!

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play





Input Output

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play



Input

Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play



Input

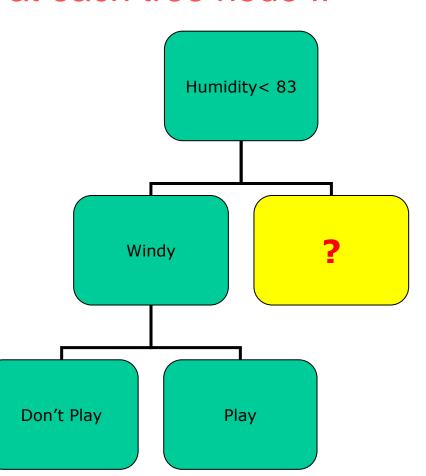
Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play



Input

Output !! Select new attributes at each tree node!!

Outlook Temperature Humidity Windy Play? false Don't Play 85 85 sunny 83 78 false overcast 68 80 false rain 72 95 false Don't Play sunny 69 false 70 sunny 75 80 false rain 72 90 Play overcast true Don't Play 71 80 rain true

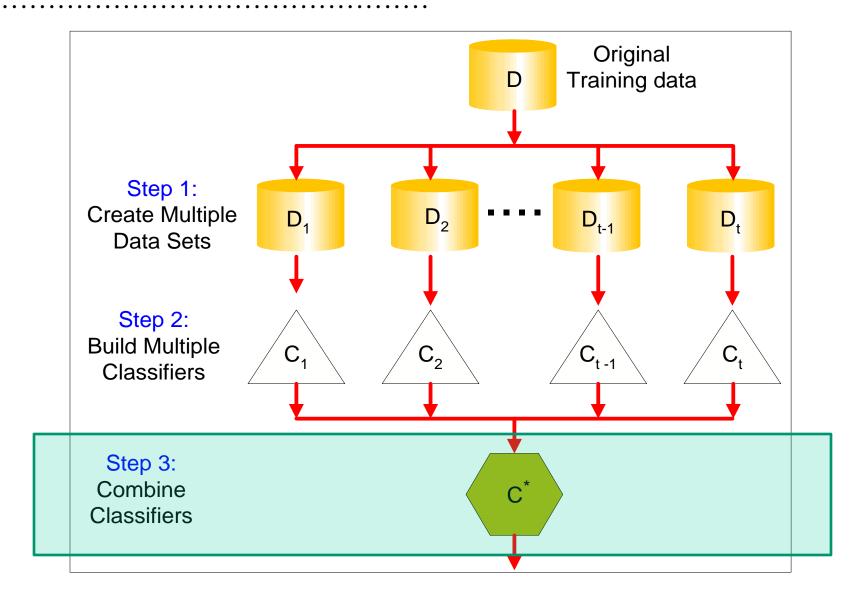




Input Output

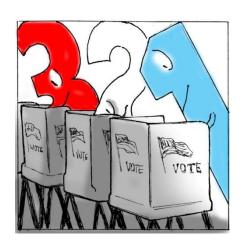
Outlook	Temperature	Humidity	Windy	Play?
sunny	85	85	false	Don't Play
overcast	83	78	false	Play
rain	68	80	false	Play
sunny	72	95	false	Don't Play
sunny	69	70	false	Play
rain	75	80	false	Play
overcast	72	90	true	Play
rain	71	80	true	Don't Play





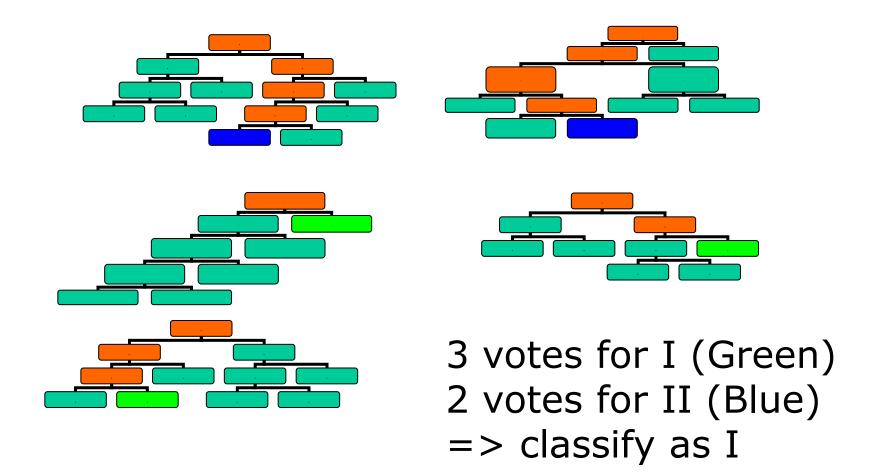


- Train a number of trees
 - Tens, hundreds or sometimes even more
- Classify new data by majority voting of the individual trees
 - Count which class is predicted by most trees





Classification with Random Forests



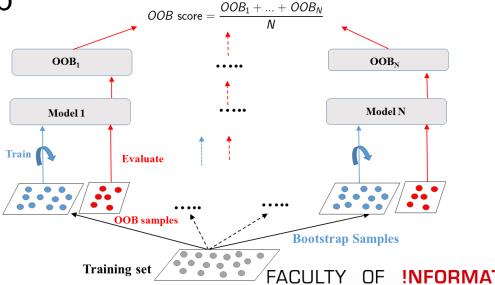


Random Forests – Evaluation

- How to evaluate performance of Random Forests?
 - Holdout, cross-validation, etc..
- Alternatively: out-of-bag error / estimate (OOB)
 - General method for bootstrapped algorithms
 - Compute mean error on each training sample $x_{i,}$ using only trees that did not have

x_i in their bootstrap

sample





Properties of Random Forests

- Only few parameters
 - Number of trees, number of variables for split, ...
 - Good default values, rather robust
- Still mostly simple concepts
- Very high accuracy for many data sets
- No over-fitting when selecting large number of trees

- Becomes slower with increasing number of trees
 - Maybe not so critical why?
 - Can be parallelised



Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines

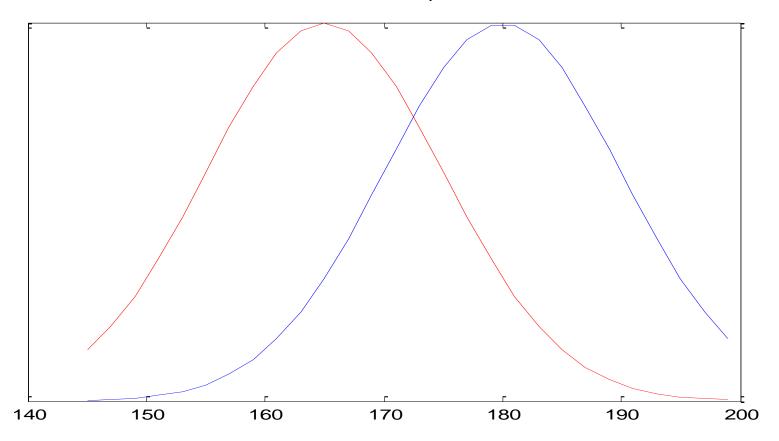


- Overfitting: model is trained too specific to learning examples
 - Examples of classifiers?

- Generalisation: ability of model to perform well on the general problem
 - i.e. the real distribution that generated the training data

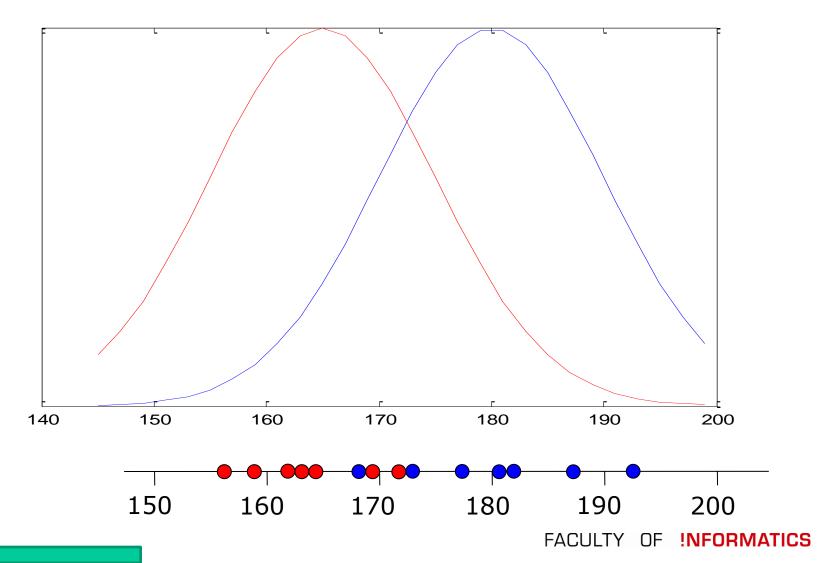


• Distributions of two classes (Gaussian, different mean)



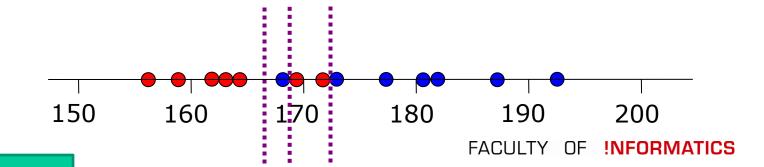


Points drawn from that distributions





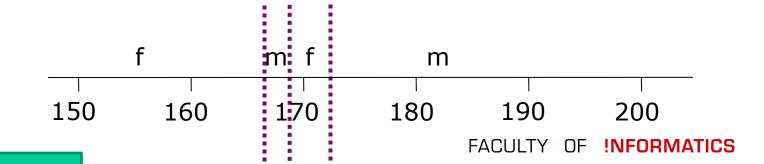
- Train e.g. a k-nn with k=1
- Assign each point to the closest neighbour
- decision boundaries half-way between points of different class





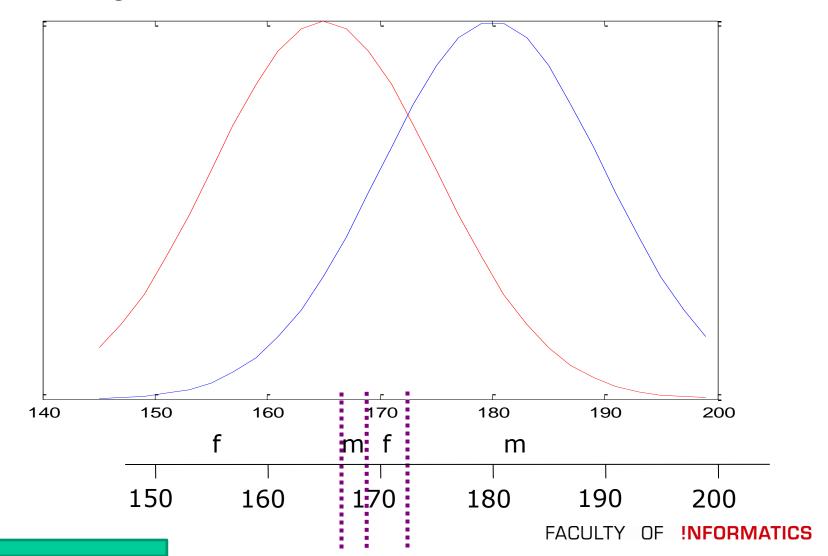
- Train e.g. a k-nn with k=1
- Assign each point to the closest neighbour
- decision boundaries half-way between points of different class

Classify according to closest point



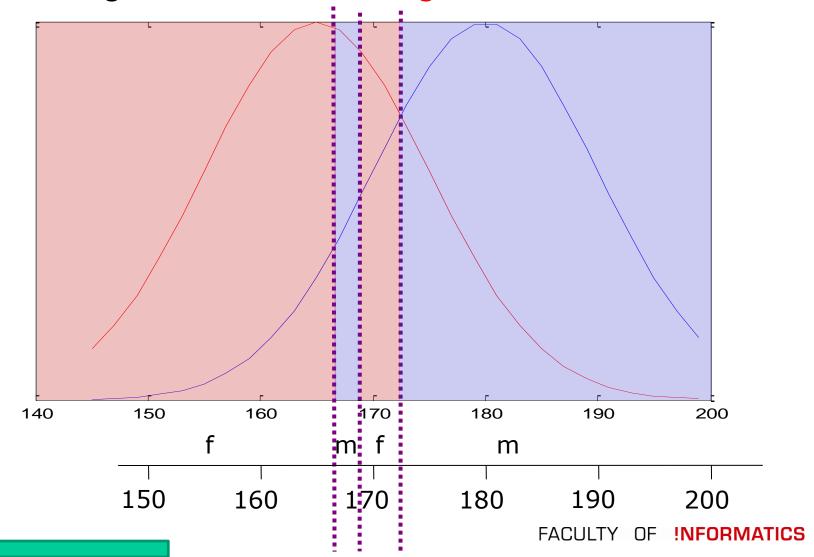


Train e.g. a k-nn with k=1





Train e.g. a k-nn with k=1: good classifier?

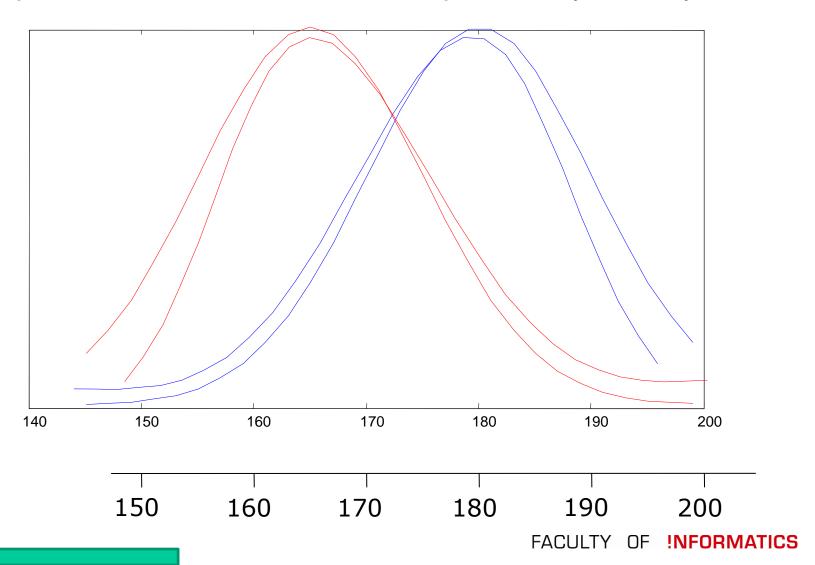




- Bayes Optimal Classifier:
 - Simple probabilistic classifier
 - Classification by taking the most likely output value for a given input
 - I.e. the highest probability
 - Probabilities normally not known ...
 - Estimate probability densities based on samples
 - C.f.: similar to what Naive Bayes does
 - But by assessing all attribute values together, not independently



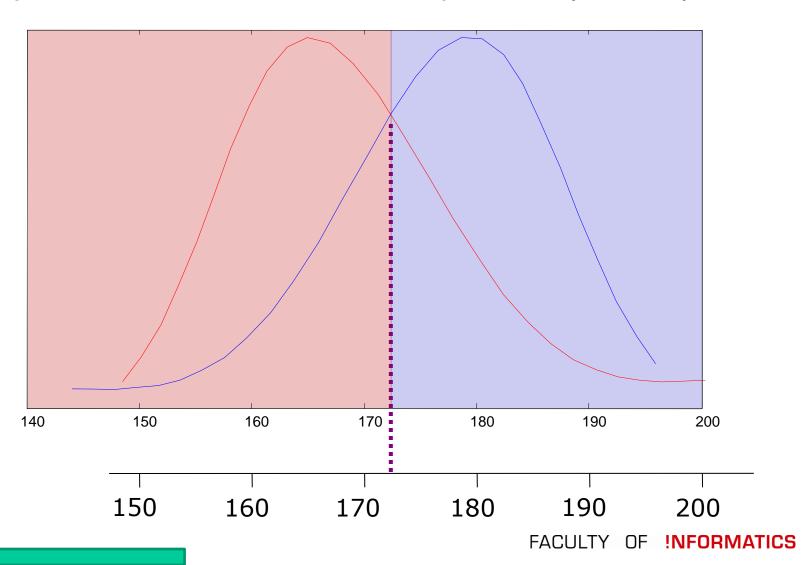
Bayes optimal classifier: estimation of probability density function





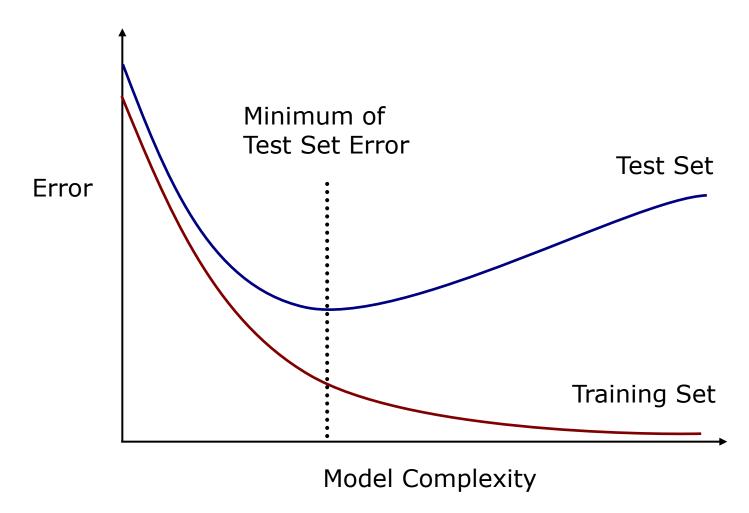
Overfitting & Generalisation

Bayes optimal classifier: estimation of probability density function





Trade-off complexity vs. generalization



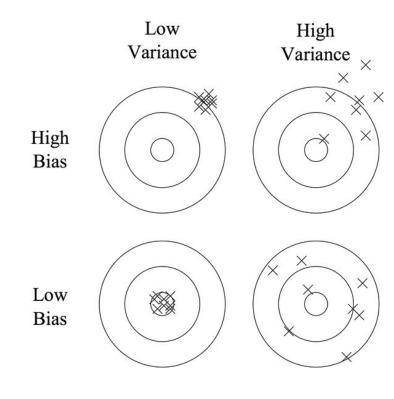


- Errors: difference prediction ← → actual output value
- Bias and variance component

- Bias: errors from erroneous assumptions in learning algorithm
 - High bias: model misses relevant relations
 - "Model not complex enough"
- Variance: error stems from sensitivity to small fluctuations in training set
 - Small fluctuations → large difference in model
 - "Models noise"; "instable"
 - Example?



- Bias is the algorithm's tendency to consistently learn the wrong thing by not taking into account all the information in the data (underfitting)
- Variance is the algorithm's tendency to learn random things irrespective of the real signal by fitting highly flexible models that follow the error/noise in the data too closely (overfitting)





- Low bias: models are usually more complex
 - Represent the training set more accurately
 - Might also represent noise
- High bias: simpler models that don't tend to overfit
 - May underfit, failing to capture important regularities

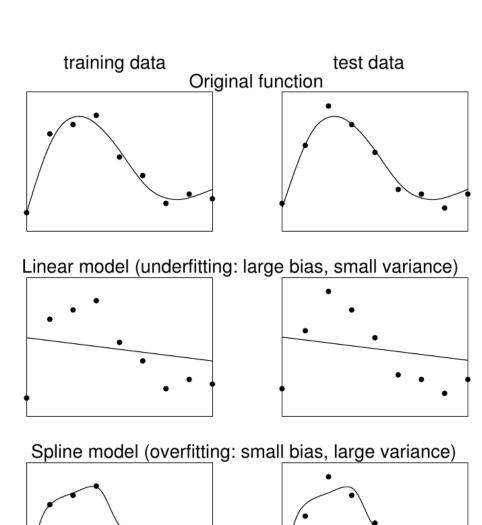


- High Variance
 - If different training sets lead to (very) different classifiers / decision boundaries
 - Learning methods able to represent training set well
 - Risk of overfitting to noisy or unrepresentative training data

- "Measure for prediction consistency"
- Variance is the "memory capacity"
 - To which detail characteristics of training data can be remembered

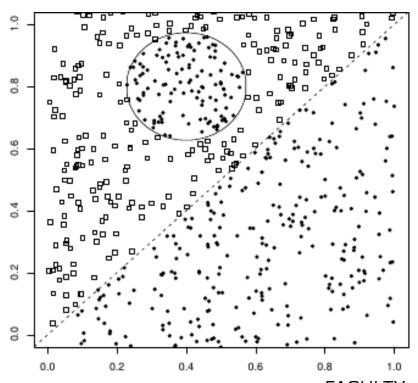


 Example for continous (regression) case



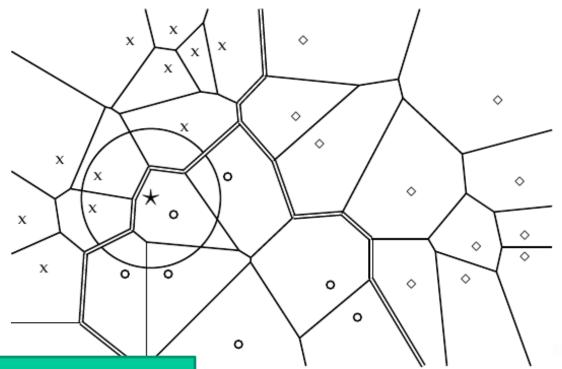


- Linear classifiers: high bias on non-linear problems
 - (Almost) regardless of training data (low variance)





- k-nn (non-linear) classifier low bias (with small k)
- Changes in training set can influence decision boundary greatly
 - → high variance (low stability)



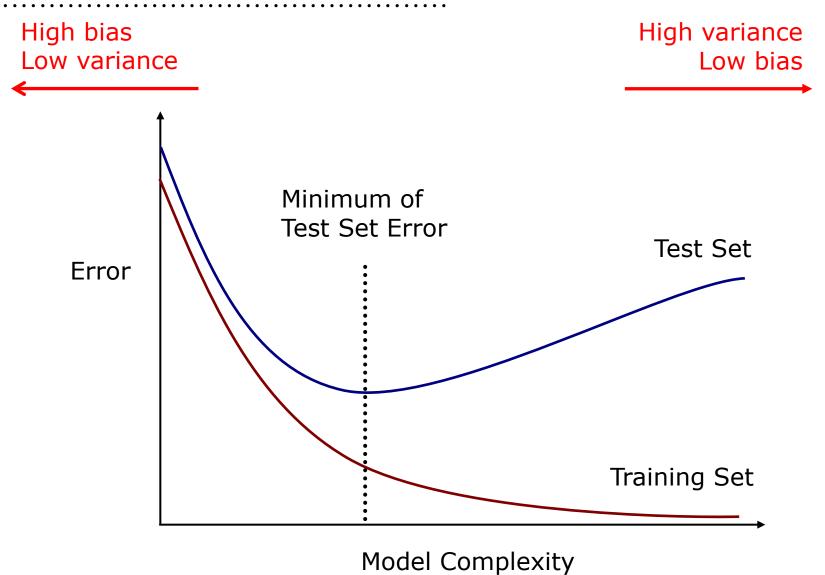


- Bias-variance tradeoff
 - Would want model that
 - Accurately captures regularities in training data (low bias)

AND

- Generalises well to unseen data (low variance)
- Typically impossible to do both simultaneously!
 - cf. precision-recall tradeoff







Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines



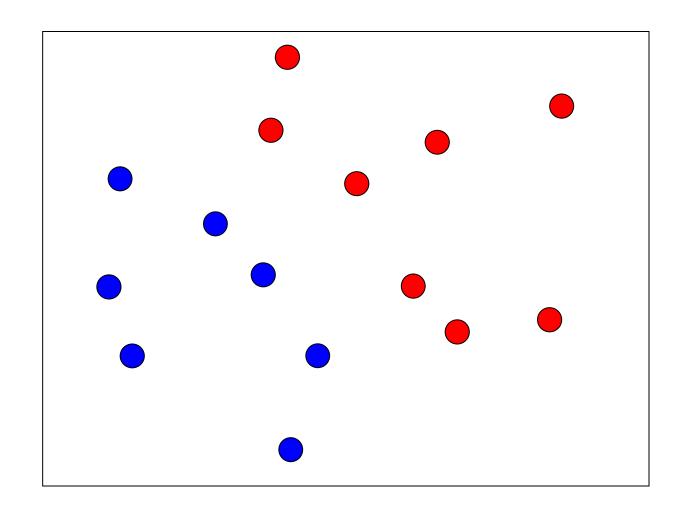
Support Vector Machines

- Introduced by Vladimir Vapnik & Alexeyl Chervonenkis in early 1960s (!)
 - Kernel-trick added in 1992



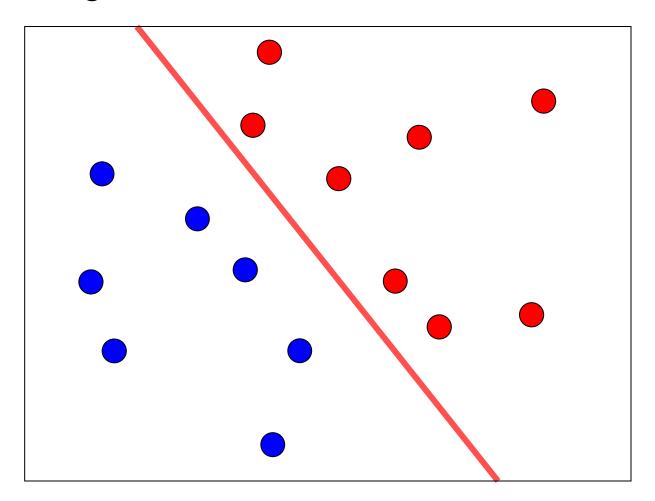
- Also known as maximum margin classifiers
- Heavily used & researched in last decade(s)
- Rather sophisticated mathematical model
- Basic concepts
 - Linear separation
 - Optimisation of hyperplane
 - Soft margin & kernel function
 - When linear separation is not possible





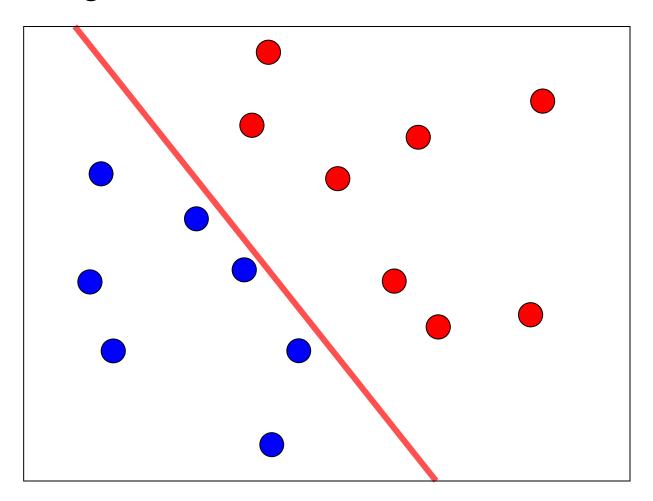


Separating line #1



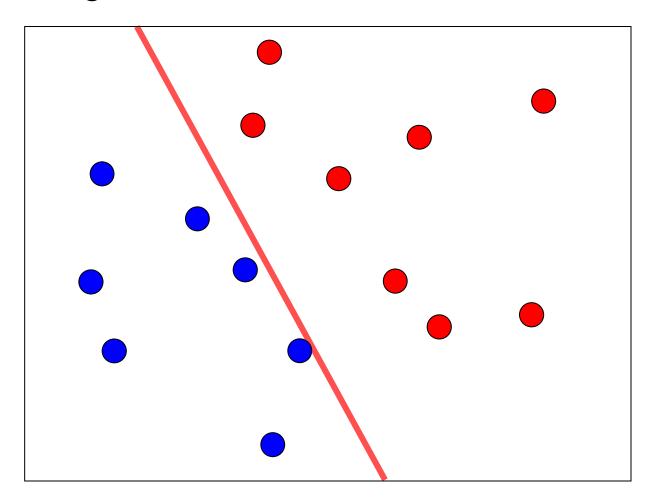


Separating line #2



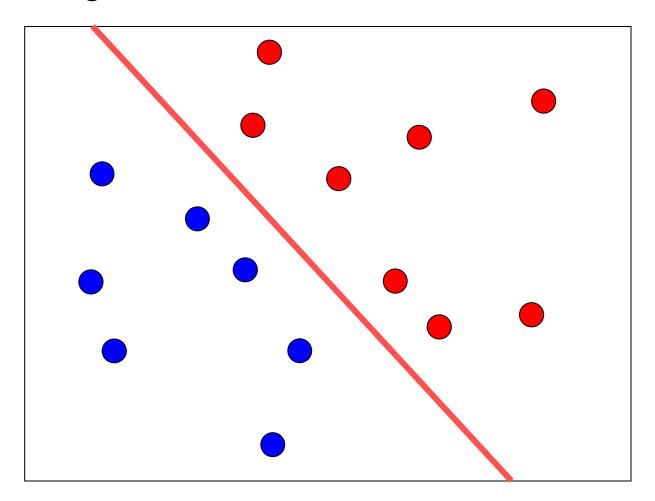


• Separating line #3



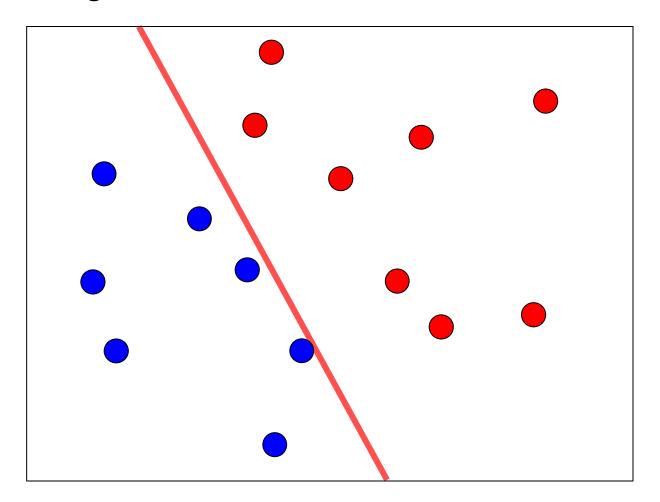


Separating line #4





Separating line #5





- Which other classifier(s) use linear separation?
- What's the difference to SVMs?

- Optimization
 - maximisation of margin separating items

Later: soft margin, kernels, ...



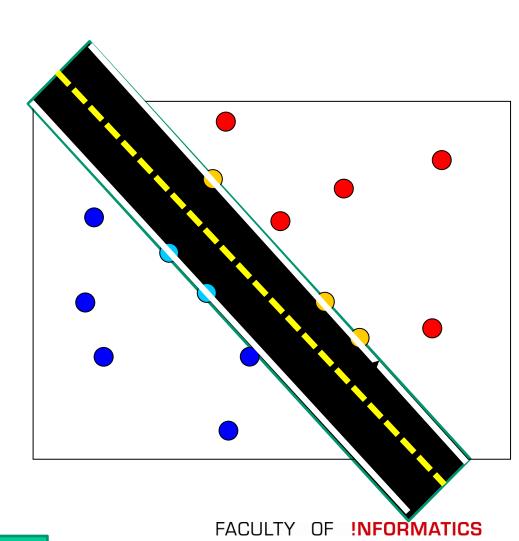
- All separations are valid
 - Which separation is the best?

- Margin of a linear classifier:
 width that boundary could be increased to
 - before hitting any data-point
- Support Vectors are those data-points that the margin pushes up against
- What's the minimum number of support vectors?

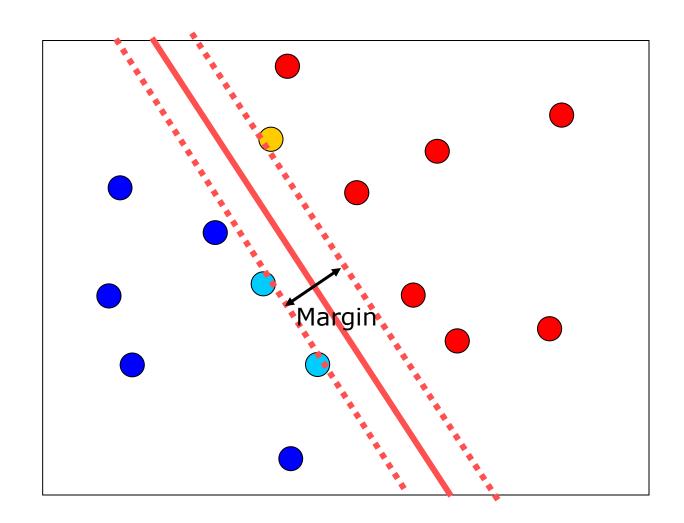


Margin – a simple analogy

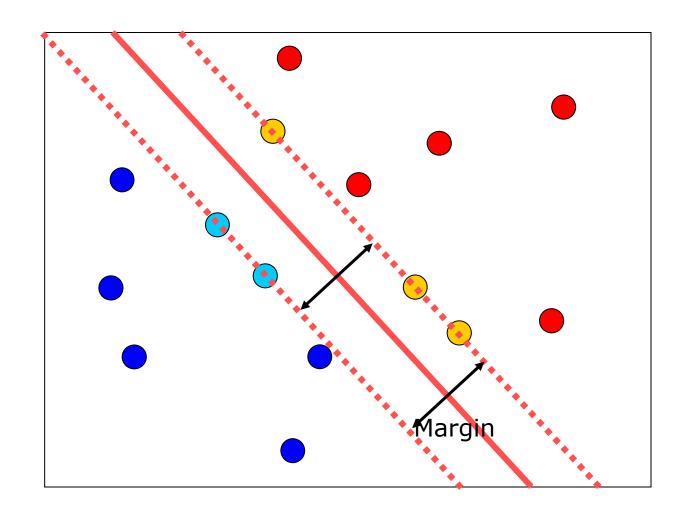
- Margin is a road
 - Decision boundary is the *median separator*
 - Support vectors are reflector posts
 - Margin = width of the road









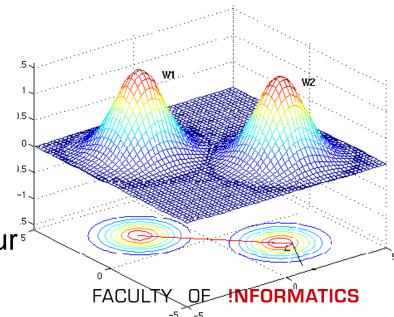




Which separation/margin is the best?

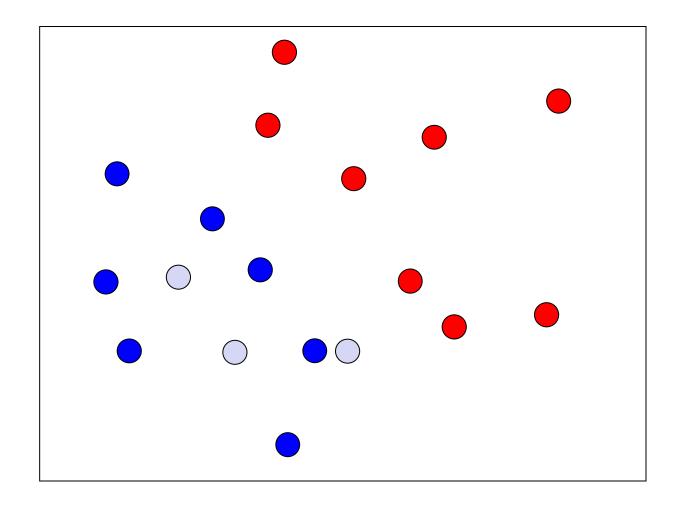
Claim: bigger margin is better

- Intuitive illustration example
 - Assumption in previous dataset: samples are drawn from probability distribution
 - E.g. two Gaussians with different means (& variances)
 - Now, draw more samples from these distributions to increase our data set (training/testing)



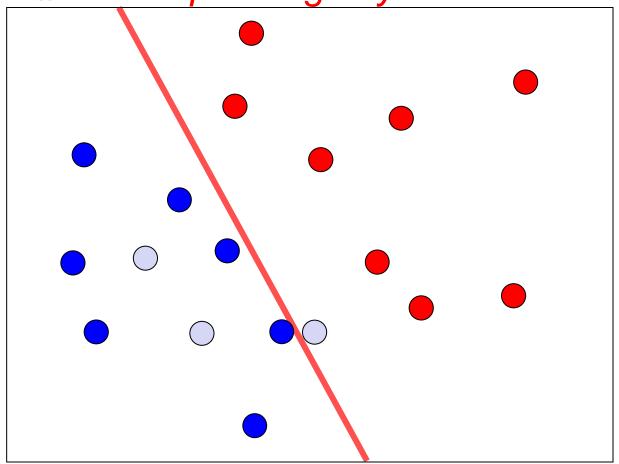


Draw more samples from the distribution



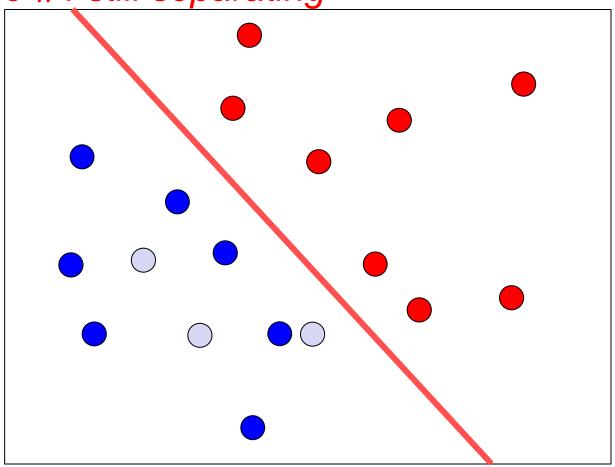


- Draw more samples from the distribution
 - → Line #3 not separating anymore



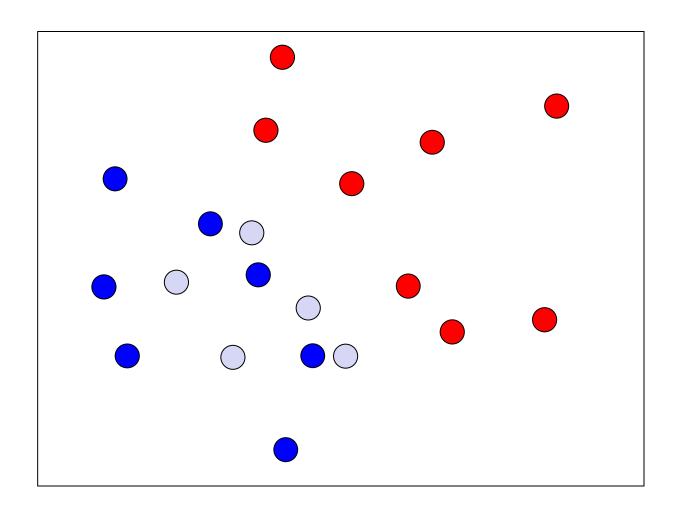


- Draw more samples from the distribution
 - → Line #4 still separating



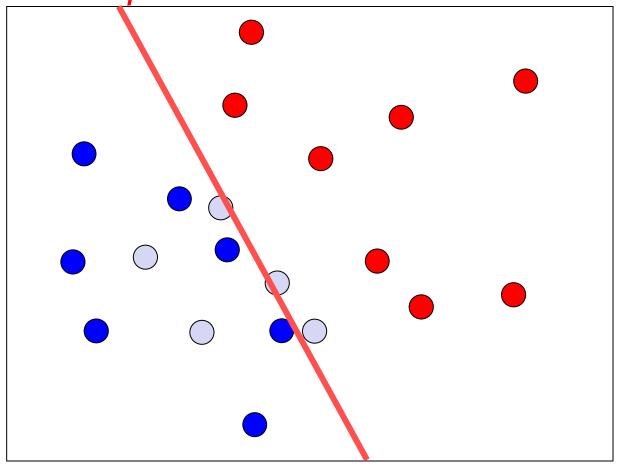


Draw even more samples from the distribution



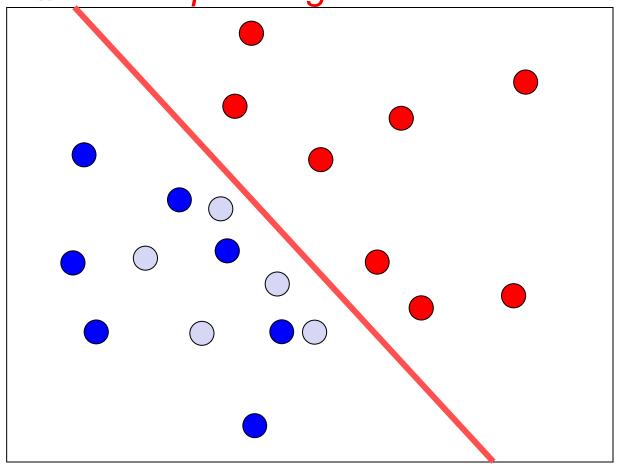


- Draw even more samples from the distribution
 - → Line #3 separates even worse





- Draw even more samples from the distribution
 - → Line #4 still separating





Which separation/margin is the best?

- Claim: bigger margin is better
- Intuitive demonstration
 - The bigger the margin → the better is the separating plane fitting to slightly different data
 - I.e. less "overfitting", more generalization
- Later: how to optimise the margin
 - Using Lagrange multipliers, quadratic programming,

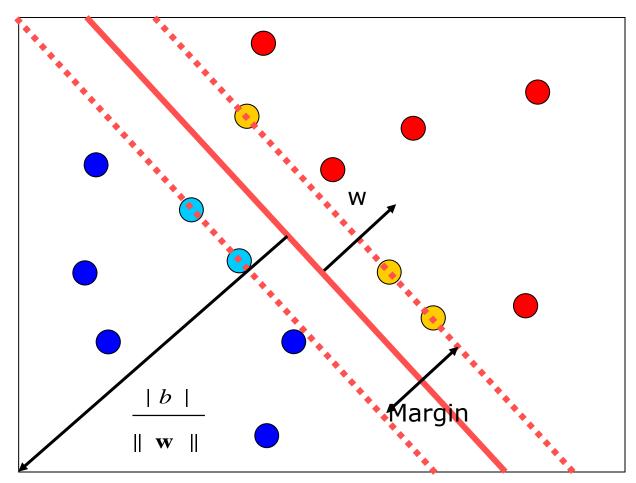
. . .



- Given set of points x_i (n-dimensional)
 - belonging to binary class: $y_i = 0$ or $y_i = 1$
- Hyperplane dividing points
 - Satisfying: $\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} = 0$
 - w is normal to the hyperplane (weight vector)
 - b determines offset from origin (intercept/bias)
 - | b | perpendicular (normal) distance from origin
 | w ||

In general: infinite number of possibilities





Origin



- Recap *Perceptron*: Activation $a = \sum_{i=1}^n w_i x_i$ Classification $f(x) = \begin{cases} 1 \text{ if } a \ge 0 \\ 0 \text{ if } a < 0 \end{cases}$
- SVM: often ≥ +1 / < -1
- Classification function: $f(\vec{x}) = sign(\vec{w}^T \vec{x}_i + b)$
 - Alternative formulation: $f(x) = \begin{cases} 1 & \text{if } a \ge 1 \\ 0 & \text{if } a < -1 \end{cases}$
- Hyperplane dividing points in -1 & +1
 - Satisfying: $\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} = 0$ with $\vec{a} \cdot \vec{b} = \vec{a}^T \vec{b}$

$$\Rightarrow \vec{v}_{XX} = -b$$



- Task: find hyperplane with largest margin
 - → minimise | w | (will show why)
 - Given the constraints

$$\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} \ge +1$$
 for $\mathbf{y}_i = +1$ (1)

$$\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} \le -1$$
 for $\mathbf{y}_i = -1$ (2)

- Constraints (1) and (2) combined:

$$y_i(\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b}) -1 \ge 0$$
 for all i

• if
$$y_i = +1$$
: $\mathbf{w} \cdot \mathbf{x}_i + b - 1 \ge 0 \implies \mathbf{w} \cdot \mathbf{x}_i + b \ge 1$

• if
$$y_i = -1$$
: $(-1) (\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b}) -1 \ge 0 \implies (-1) (\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b}) \ge 1$
 $\implies \mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} \le -1$



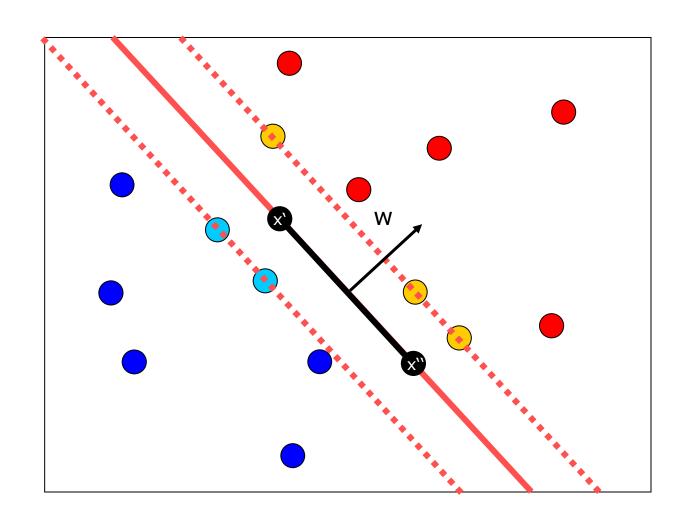
- Hyperplane dividing points in -1 & +1
 - Satisfying: $\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} = 0$
 - w is normal to the hyperplane
- Demonstration: pick 2 points x', x"on the plane, thus

$$- w \cdot x' + b = 0$$
 and $w \cdot x'' + b = 0$

$$\rightarrow$$
 w · (x' - x'') = 0

- → w is normal to the plane
 - as it is normal to any vector on the plane
 - and x'x" is a vector on the plane





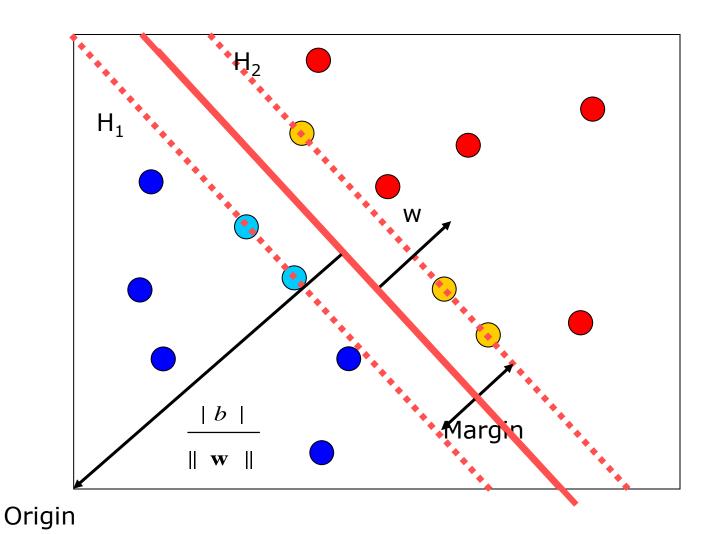


- Can decompose margin into two components
- d_+ : shortest distance from hyperplane to closest positive sample $(y_i = +1)$
- d_.: shortest distance from hyperplane to closest negative sample (y_i = -1)
- Width of margin: d₊ + d₋



- Points for which equality in (1) holds
 - Points on hyperplane H_1 : $\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} = 1$
- Points for which equality in (2) holds
 - Points on hyperplane H_2 : $\mathbf{w} \cdot \mathbf{x}_i + \mathbf{b} = -1$
 - Distance from origin: $\frac{|-1-b|}{\|\mathbf{w}\|}$
- Optimisation: find H₁ and H₂, described by
 w · x_i + b = 1 and w · x_i + b = -1







- How to find the largest margin?
- Analytical solution, e.g. via quadratic programming and Langrage multipliers
 - E.g. SMO (Sequential Minimal Optimisation) algorithm
 - 1998 by John Platt (Microsoft Research)
 - Breaks the optimisation in a series of sub-problems
 - Used e.g. in WEKA, LibSVM, ...
- Heuristic Optimisation
 - Sub-gradient descent, coordinate descent
 - Sub-gradient when there are many training examples
 - Coordinate descent when the dimensionality is high
- Difference in the two approaches?



Largest Margin: Analytical

After quite some math, using Lagrange
 Multipliers

$$Lp = \sum_{i=1}^{n} \alpha_{i} - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} y_{i} y_{j} x_{i} \cdot x_{j}$$

and Convex quadratic programming, we obtain

$$\mathbf{w} = \sum_{i=1}^{n} \alpha_{i} y_{i} x_{i}$$

$$-b = \mathbf{w} \cdot \mathbf{x}_{i} - y_{i}$$

- Depends on dot-product of x_i
- Quadratic programming complexity increases with n²
- "Quite some Math": tutorial in TUWEL
 - Discussed in a later lecture (time permitting)



Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines: soft margin

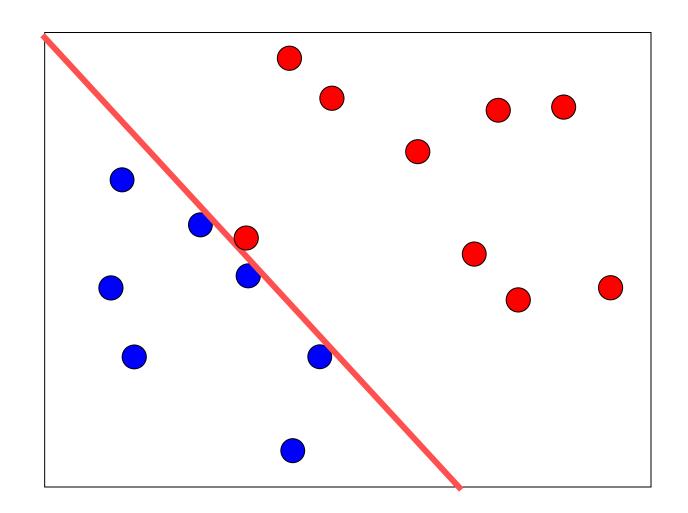


Soft margin

- SVMs optimise the decision boundary ...
- ... but still rely on linear separation!
- 1. Sometimes linear separation not possible
- 2. Sometimes, linear separation would lead to a badly generalising model
 - When?



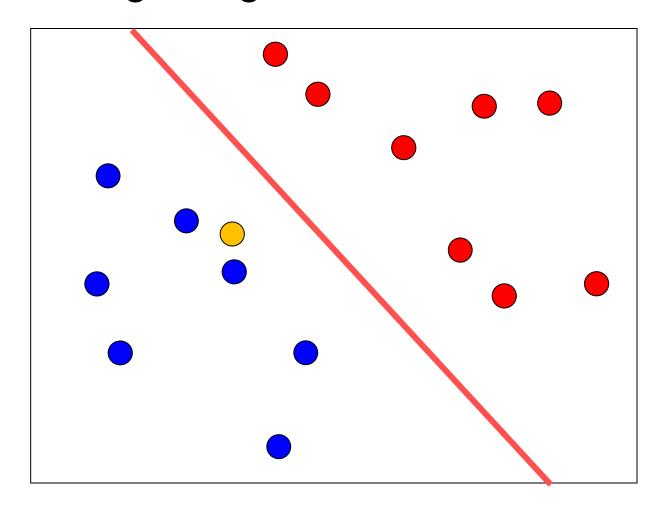
Bad generalisation





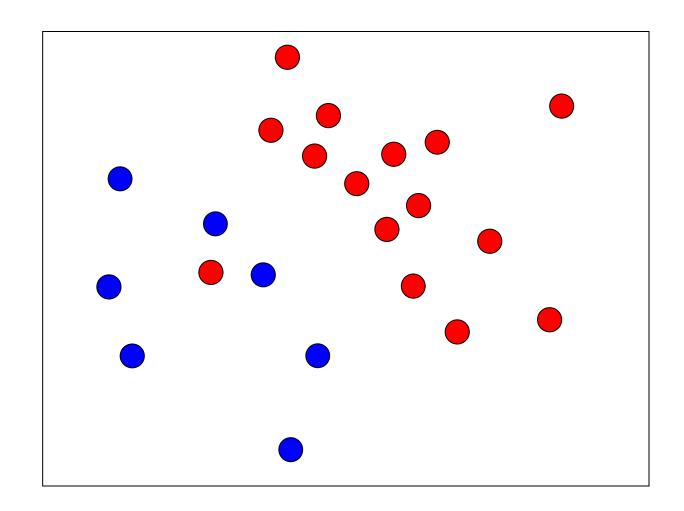
Bad generalisation

• Wider margin might be better





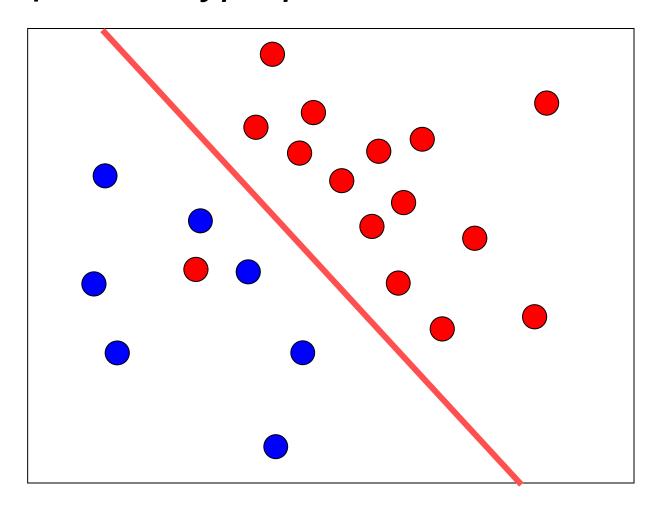
Linear separation not possible





Linear separation not possible

• "Acceptable" hyperplane could still be found





Soft margin

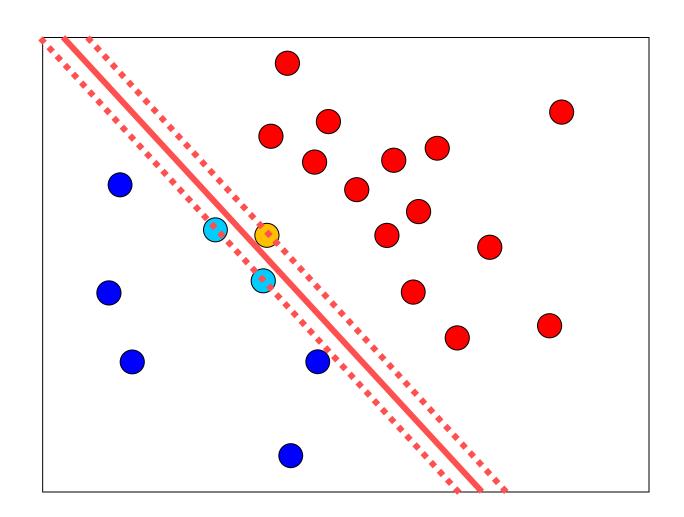
- Sometimes linear separation not possible, or
- Linear separation would lead to a badly generalising model

→ Soft margin

- Hyper plane that splits "as cleanly as possible/desirable"
- While maximising margin

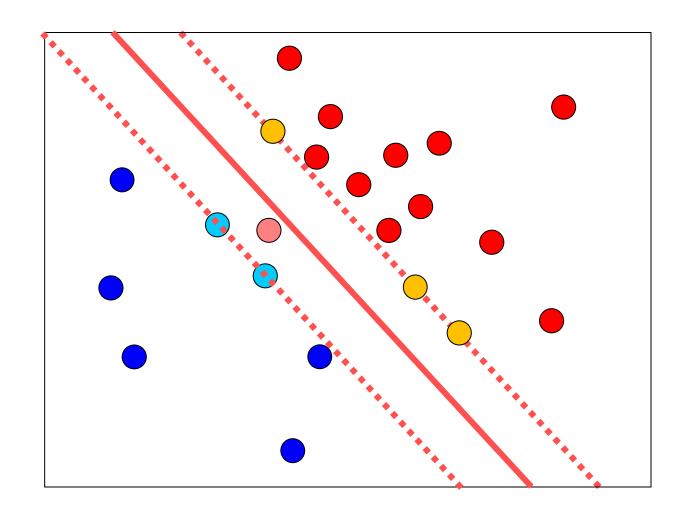


Hard Margin ...



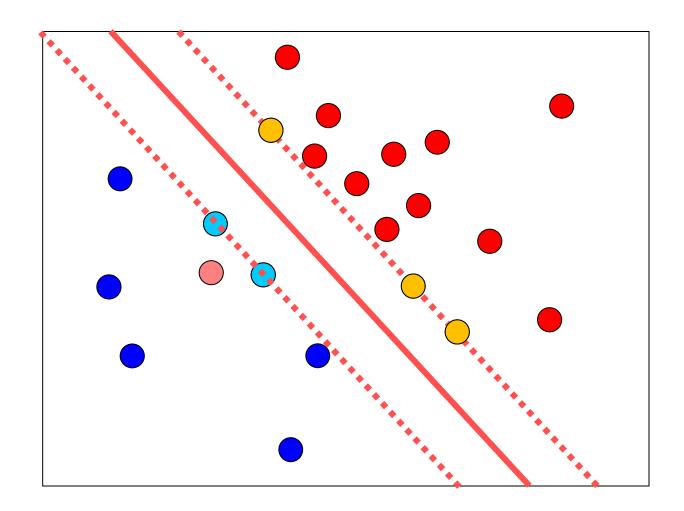


Soft Margin: for larger margin



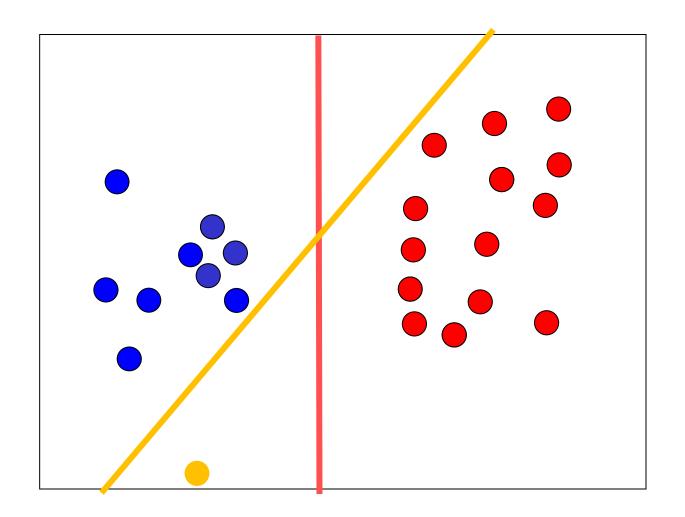


Soft Margin: to find separation





Soft Margin: larger margin with outliers





Soft Margin

- Introduction of slack variables
 - penalises misclassification
 - adapt constraint

$$y_i (\mathbf{w} \cdot \mathbf{x}_i - \mathbf{b}) \ge 1 - \xi_i$$
 for all i

Penalise non-zero ξi

$$\rightarrow$$
 min $\| \mathbf{w} \|^{+} C \sum_{i=1}^{n} \xi_{i}$

- How to solve it?
 - Similar to "hard-margin" case
- Implications?



Soft Margin

- Introduction of slack variables for optimisation problem
 - penalises misclassification
- Implications?
 - Not necessarily 100% classification accuracy on training set
 - Even if linearly separable

- Optimisation: trade off between large margin and small error penalty (controlled by C)
 - Trade-off between fitting to training data and general model
- C becomes part of optimisation problem
 - Sometimes called the "complexity parameter"
 - Large C: penalising errors more

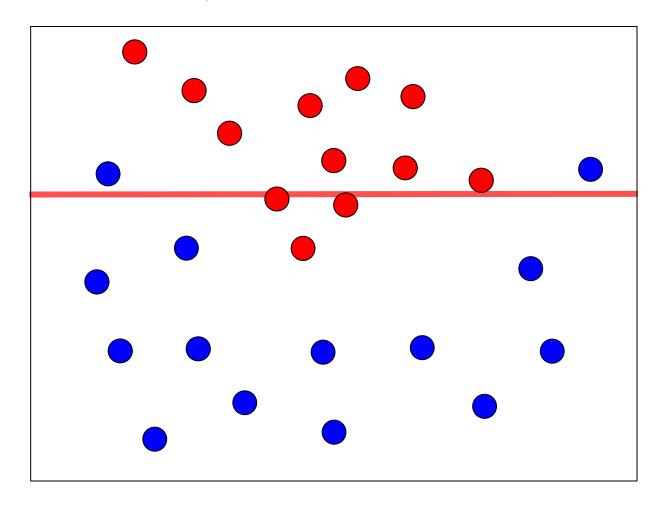


Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines: kernels

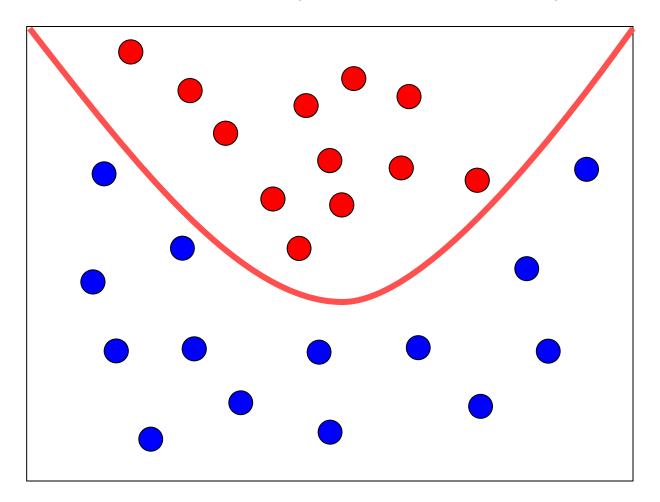


• "Acceptable" hyperplane can not be found

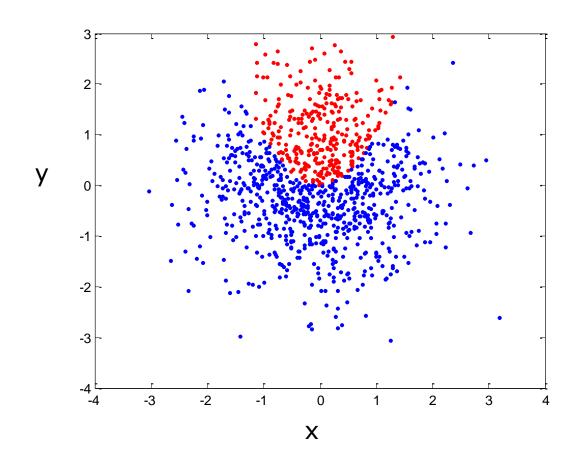




Data would be easily separable by a polynom

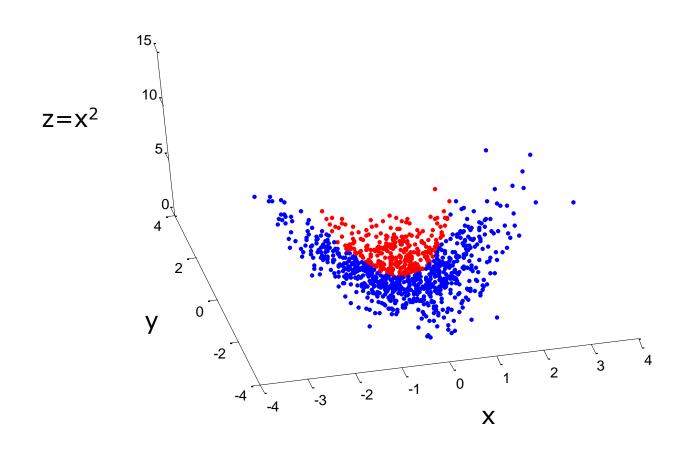








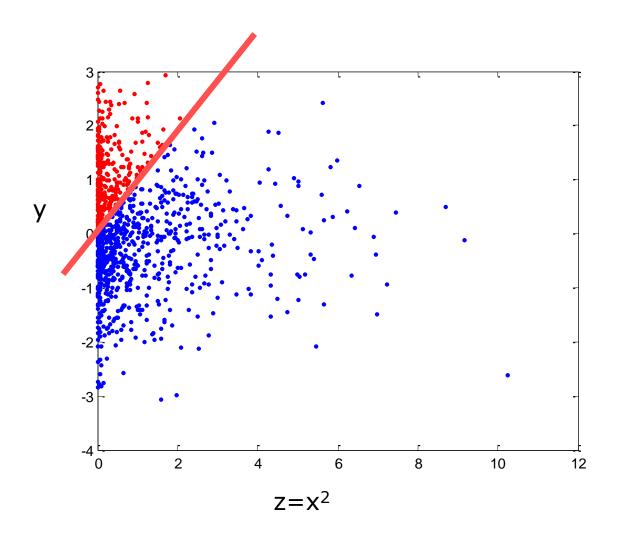
New coordinate $z=x^2$



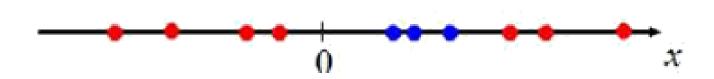


New coordinate $z=x^2$

•••••

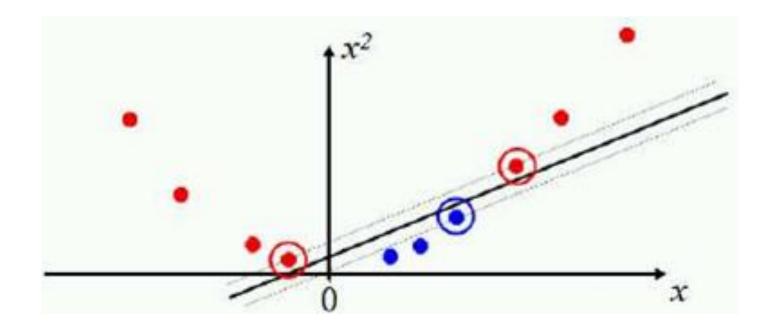




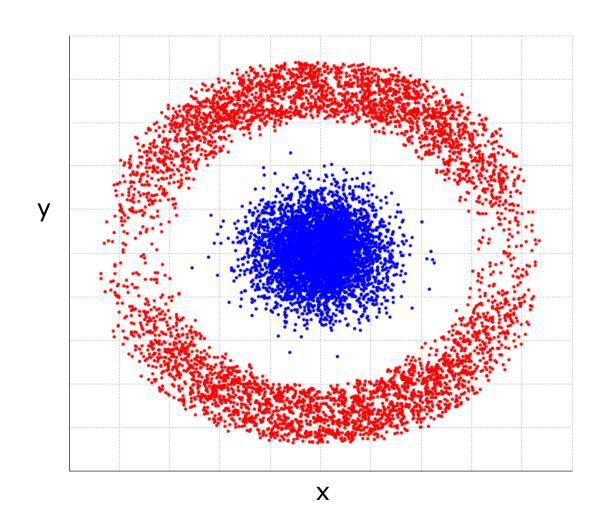




New coordinate $y=x^2$

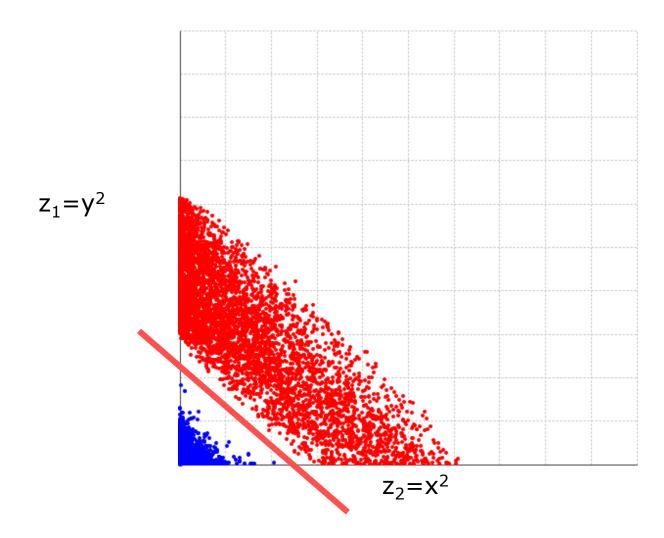








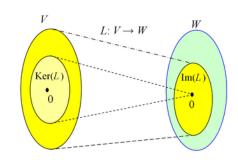
New coordinates $z_1=x^2 \& z_2=y^2$





SVM: Kernels

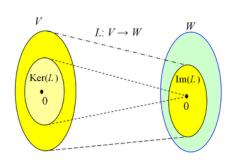
- Projection of data into higher dimensional space
 - Data may be separable in this space
- Projection: multiplication of vectors with kernel matrix



- Often: projected space has dimensionality equal to number of training vectors
- Kernel matrix determines shape of possible separators
 - In previous example: polynomial (quadratic)



Common Kernels



Quadratic

$$- e.g. k(x,y) = (x \cdot y)^2$$

- General Polynomial (arbitrary degree)
 - $-k(x,y) = (x \cdot y)^d$ (homogenous)
 - $-k(x,y) = (x \cdot y + 1)^d$ (inhomogenous)
- Gaussian $k(x, y) = \exp\left(\frac{\|x y\|^2}{2^{\sigma^2}}\right)$
- Radial Basis Function $k(x, y) = \exp(-\gamma \| x y \|^2), \gamma > 0$
- Sigmoid $k(x, y) = \tanh(\kappa_x \cdot y + c)$ for some $(not\ every\)^{\kappa} > 0_{FACULA}^{c}$



Best suited Kernel

- Best kernel depends on the data and its underlying distribution
- How to chose
 - Kernel family?
 - Exact parameters?
 - Model selection:
 - Train several models with different kernels
 - Chose best performing
- Linear kernels work well with sparse data (e.g. Text)



Kernel Trick

- Other ML algorithms could work with projected (high dimensional) data
 - So why bother with (rather) complicated SVM?

 Working with higher dimensional data is problematic: increased computational complexity



Kernel Trick

- Working with high dimensional data is problematic (computational complexity)
- Outlook: SVMs depend only on dot-product between vectors
 - Kernel Trick: replace dot-product with kernel function
 - This is computationally inexpensive (relatively)

$$Lp = \sum_{i=1}^{n} \alpha_{i} - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} y_{i} y_{j} x_{i} \cdot x_{j}$$



Outline

- Short recap
- Random Forests
- Evaluation
- Support Vector Machines: multi-class



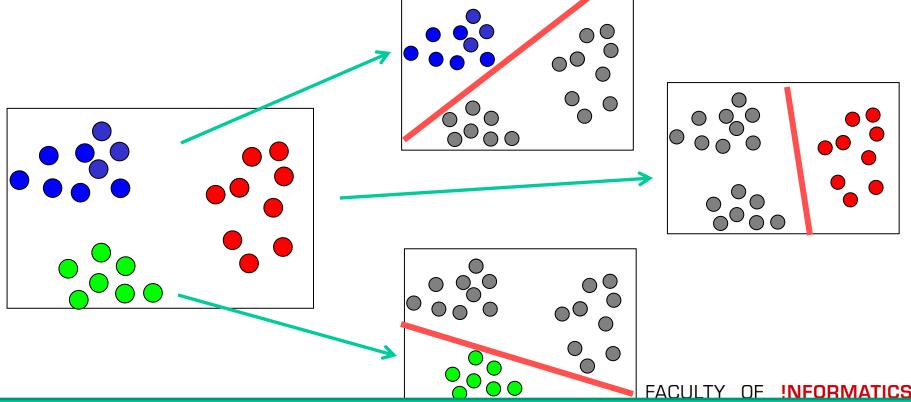
Multi-class SVM

- Standard SVM algorithm just solves binary problems (i.e. two classes)
- Multi-class problem (three or more classes)
- Reduce (single) multi-class problem to multibinary problems
 - One vs. all → chose the classifier with the greatest margin
 - One vs. One → chose class selected most often



Multi-class SVM

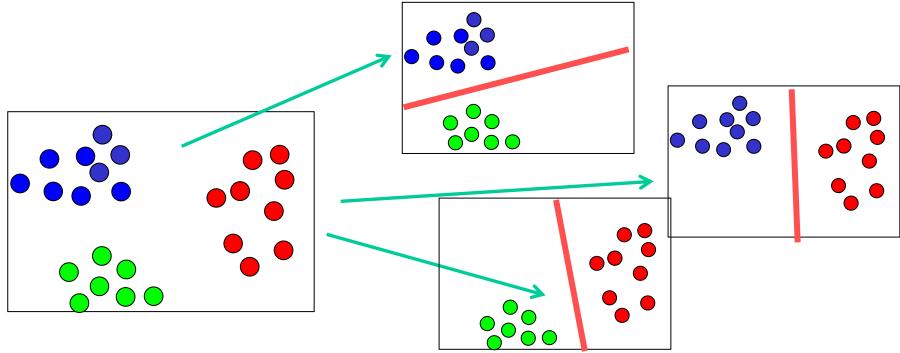
- One vs. All
 - Build binary classifiers that distinguish between class i and the rest (i = 1, ..., #numClasses)
 - Classifier with highest output f(x) is the winner





Multi-class SVM

- One vs. One
 - Build binary classifier for each pair of classes
 - Class with highest number of votes wins

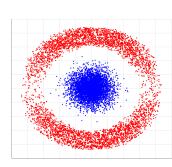


- How many classifiers?
 - Needs |C|(|C|-1)/2 classifiers (but smaller)



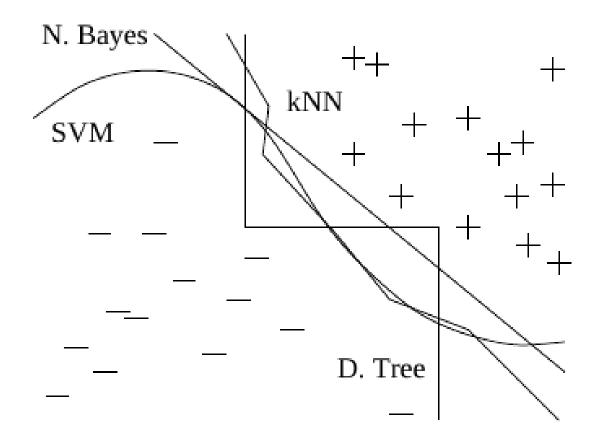
Properties of SVM

- High classification accuracy
 - Good generalisation, even though decision boundary in original space is complex
- Linear kernels: Good for sparse, high dimensional data, e.g. text mining
- Much research has been directed at SVM, and it's foundations → solid background
- Implementation available in open-source software (e.g. libSVM)





Comparison of decision boundaries





Questions?

