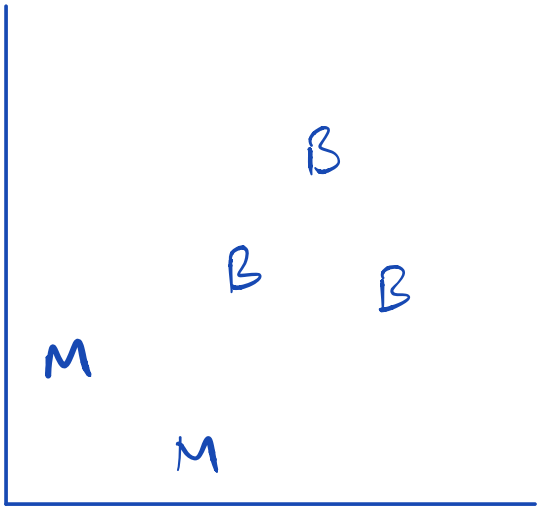
Agenda

> SVM
> Kernel Trick
> Hindroid
> Train-test split
> What has SVM Learned?

Support Vector Machines.

- classification algorithm.



Benign

$\vec{w} \cdot \vec{u} \geq c$

Classifier.

$\vec{w} \cdot \vec{u} + b \geq 0 \rightarrow$ Benign

What are the unknowns?

Constraint:

$$\begin{cases} y_i = 1 & \text{Benign} \\ y_i = -1 & \text{Malware.} \end{cases}$$

① $y_i(\vec{w}\cdot\vec{x}_i + b) - 1 \geq 0$ → All points.

② $y_i(\vec{w}\cdot\vec{x}_i + b) - 1 = 0$ → On the lines.

$$\text{width} = (x^+ - x^-)\cdot\frac{\vec{w}}{\|\vec{w}\|} = \frac{?}{\|\vec{w}\|}$$

$$\text{Max.}\ \frac{1}{\|\vec{w}\|} \rightarrow \min \|\vec{w}\| \rightarrow \min \frac{1}{2}\|\vec{w}\|^2$$

primal

$$\min \mathcal{L} = \frac{1}{2}\|\vec{w}\|^2 - \left[\sum \alpha_i [y_i(\vec{w}\cdot\vec{x}_i + b) - 1]\right]$$

$$\frac{\partial \mathcal{L}}{\partial \vec{w}} = \vec{w} - \sum \alpha_i y_i x_i = 0$$

$$\Rightarrow \vec{w} = \sum \alpha_i y_i x_i$$

$$\frac{\partial L}{\partial b} = \sum \alpha_i y_i = 0$$

$$L = \frac{1}{2}\left(\sum \alpha_i y_i x_i\right)\left(\sum \alpha_j y_j x_j\right) - \sum_i (\alpha_i y_i x_i) \sum (\alpha_j y_j x_j) + \sum \alpha_i$$

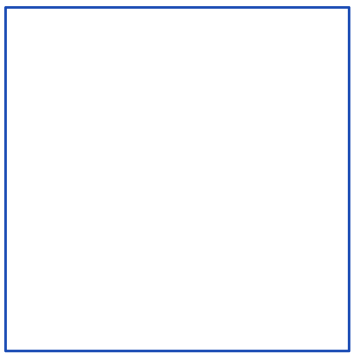
dual.

$$\Rightarrow L = \sum \alpha_i - \frac{1}{2} \sum_i \sum_j \alpha_i y_i \alpha_j y_j (\vec{x}_i \cdot \vec{x}_j)$$

Use quadratic progrmng

input :

output :



$\leq 10{,}000$

Decision Rule

KKT

$$\alpha_i [y_i (\vec{w} \cdot \vec{x}_i + b) - 1] = 0$$

α | 0 0 1 2 0 0 0 0 0 5 1 0 0 0 0 0 0 1 0 |

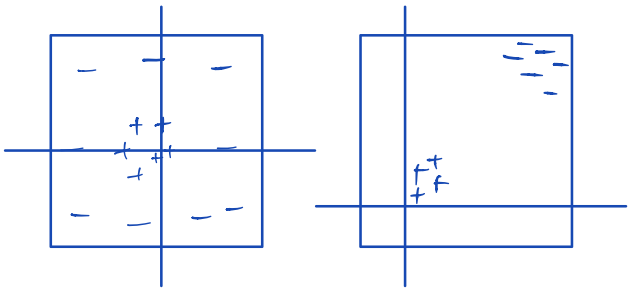
Regularization

$$\min \frac{1}{2} \|\vec{w}\|^2 + C \sum_i \xi_i$$

$$y_i (\vec{w} \cdot x_i + b) \geq 1 - \xi_i$$

$$\xi \geq 0.$$

Kernel Trick



Polynomial Kernel:

$$K(x,y) = (1 + \vec{x} \cdot \vec{y})^d$$

RBF / Gaussian Kernel:

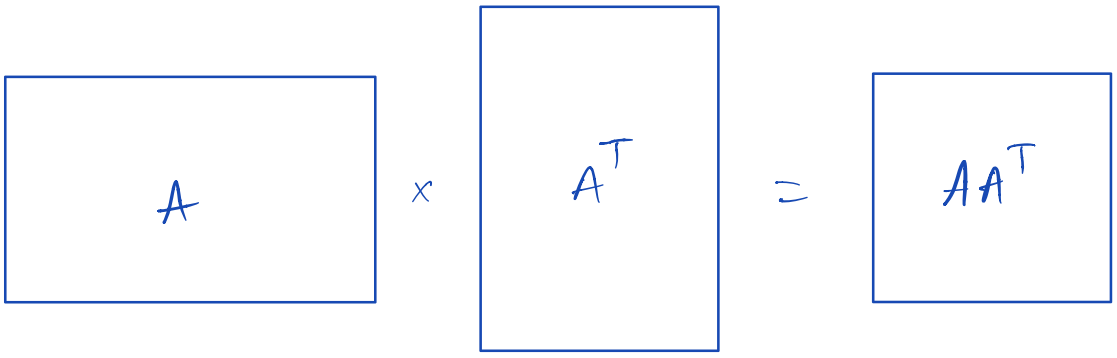
$$K(x,y) = e^{-\frac{\|\vec{x} \cdot \vec{y}\|^2}{2\sigma^2}}$$

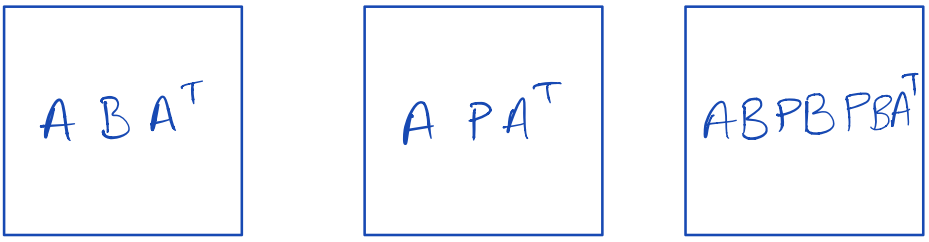
For, $\sigma = 1$

$$K(x,y) = c\left\{1 - \frac{\vec{x} \cdot \vec{y}}{1!} + \frac{(\vec{x} \cdot \vec{y})^2}{2!} - \frac{(\vec{x} \cdot \vec{y})^3}{3!} + \cdots\right\}$$

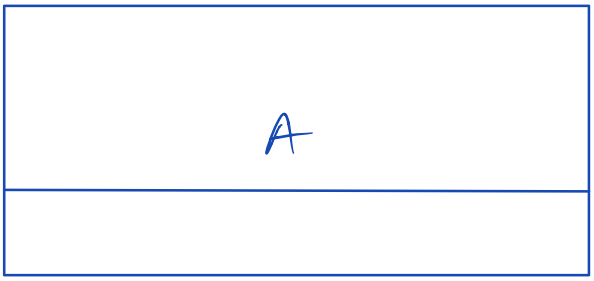
where, $c = e^{-\frac{1}{2}\|x\|^2} \cdot e^{-\frac{1}{2}\|y\|^2}$

How does this relate to HinDroid?





Train - Test Split



→ Right?

Poll:

How do you test with this method for kernel: ABB^TA^T.

Option A: ABB^TA^T

- Train
- Test

Option B: ABB^TA^T

Option C: ABB^TA^T

Option D: ABB^TA^T

Option E: Something else (No! Pls no!)

Q. What has SVM Learned?