Lappangó programhibák megkeresése gépi tanulással

Bolgár Bence

Méréstechnika és Információs Rendszerek Tanszék

Szoftver verifikáció és validáció, 2013. december 12.

Lappangó programhibák

Brun Y. et al.: Finding latent code errors via machine learning over program executions.

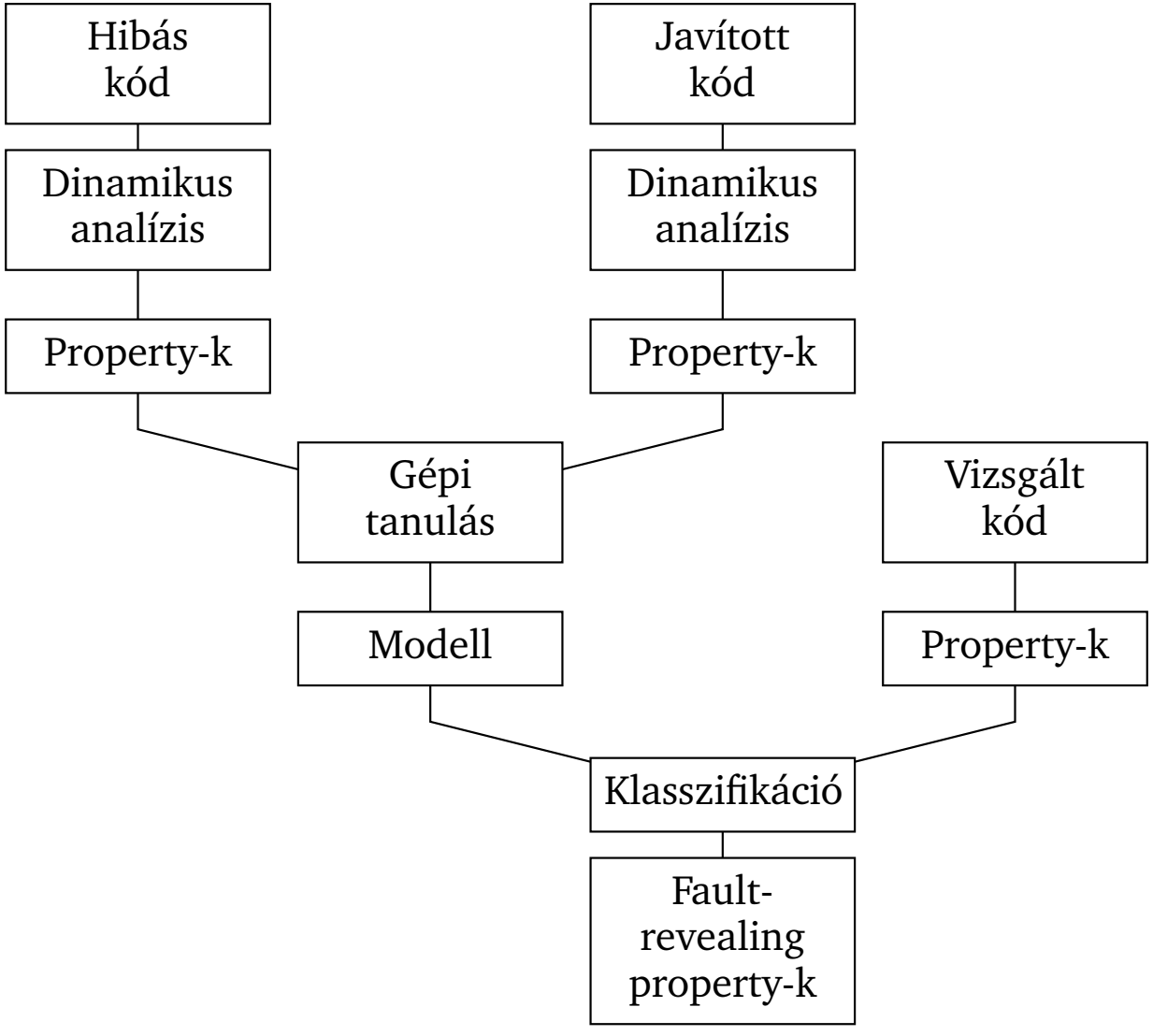
Cél: olyan programhibák megtalálása, amelyekre nincsen tesztünk. Hasznos lehet pl.:

- Ha új tesztesetek generálása nem megoldható vagy túl költséges.
- Ha az elvárt viselkedés reprezentációja nehézkes.
- Nehezen megtalálható programhibák azonosítása.

Eljárás: felügyelt tanulás

1. Tanulás: ismerten hibás programkódok és javított verziók alapján
   - Pl. korábbi projektek kritikus hibáit felhasználva
   - Property-k generálása dinamikus analízissel (Daikon)
   - Modellépítés „fault-revealing” property-k megtalálására (SVM, döntési fa)
2. Klasszifikáció: vizsgálandó kód
   - Property-k klasszifikációja a modell felhasználásával
   - „Pozitív” property-k ellenőrzése manuálisan

Felügyelt tanulás



Példa

```
// Return a sorted copy of the arg.
double[] bubble_sort(double[] in)
{
 double[] out=array_copy(in);
 for (int x=out.length-1; x>=1; x--)
 {
  // lower bound should be 0, not 1
  for (int y=1; y<x; y++)
  {
   if (out[y]>out[y+1])
    swap(out[y],out[y+1]);
  }
 }
 return out;
}
```

Property	FR
$\texttt{out[1]} \leq \texttt{in[1]}$	Yes
$\forall\ \texttt{i:}\ \ \texttt{in[i]} \leq 100$	No
$\texttt{in[0]} = \texttt{out[0]}$	Yes
$\text{size}(\texttt{out}) = \text{size}(\texttt{in})$	No
$\texttt{in} \subseteq \texttt{out}$	No
$\texttt{out} \subseteq \texttt{in}$	No
$\texttt{in} \neq \texttt{null}$	No
$\texttt{out} \neq \texttt{null}$	No

Dinamukus analízis: Daikon

A módszer szempontjából lehetne statikus analízist is használni! Így viszont:

- Sokkal inkább a program viselkedését vizsgáljuk a szintaxis helyett.
- A futási idejű property-k alkalmasabbak a helyes és helytelen viselkedés elkülönítésére.

Daikon (dinamikus invariáns detektor):

- Property-k detekciója specifikus pontokon: pl. eljárások belépési és kilépési pontjai.
- Detektált property-k pl.:
  - Egyenlőség, értékfelvétel adott tartományban.
  - Nullitás.
  - Modulus.
  - Lineáris ill. egyéb függvénykapcsolatok.
  - Tömbökre: a fentiek elemenként, sorrendezés (lexografikus is), szélsőértékek, stb.
  - Implikációk, diszjunkciók, pl.: `if p` $\neq$ `null then p.value` $>$ `x`

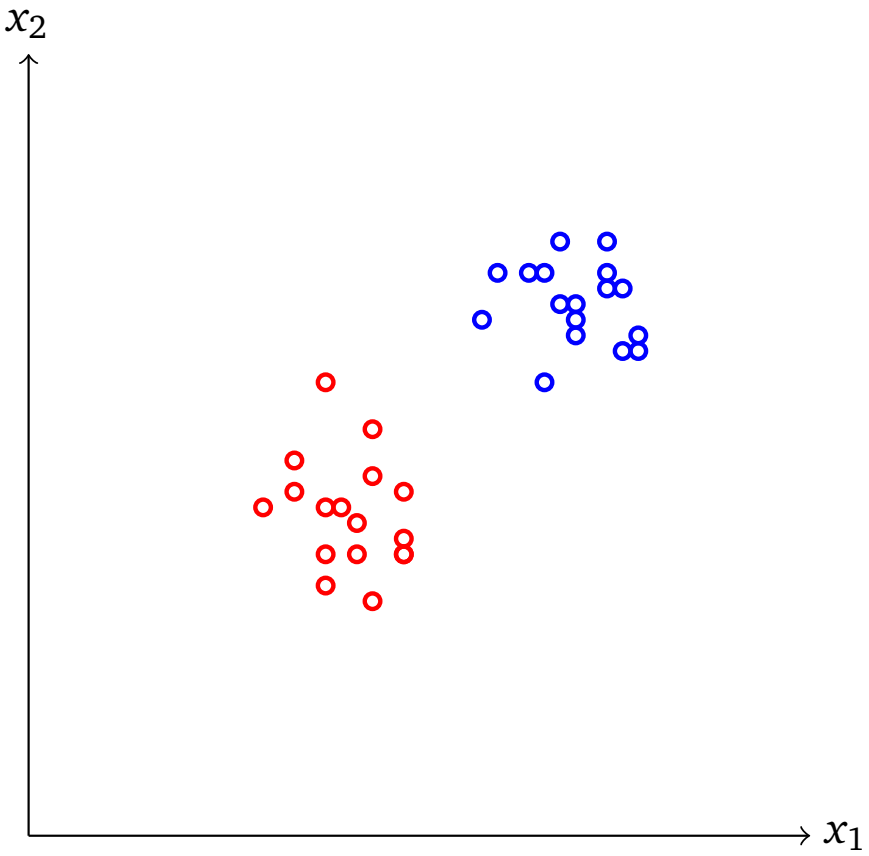
Feature vektorok előállítása

Property	Equation				Variable type			Number of vars
	$\leq$	$=$	$\neq$	$\subseteq$	int	double	array	
`out[1]` $\leq$ `in[1]`	1	0	0	0	0	1	0	2
$\forall$ `i:` `in[i]` $\leq$ `100`	1	0	0	0	0	1	0	1
`in[0] = out[0]`	0	1	0	0	0	1	0	2
size(`out`) = size(`in`)	0	1	0	0	1	0	0	2
`in` $\subseteq$ `out`	0	0	0	1	0	0	1	2
`out` $\subseteq$ `in`	0	0	0	1	0	0	1	2
`in` $\neq$ `null`	0	0	1	0	0	0	1	1
`out` $\neq$ `null`	0	0	1	0	0	0	1	1

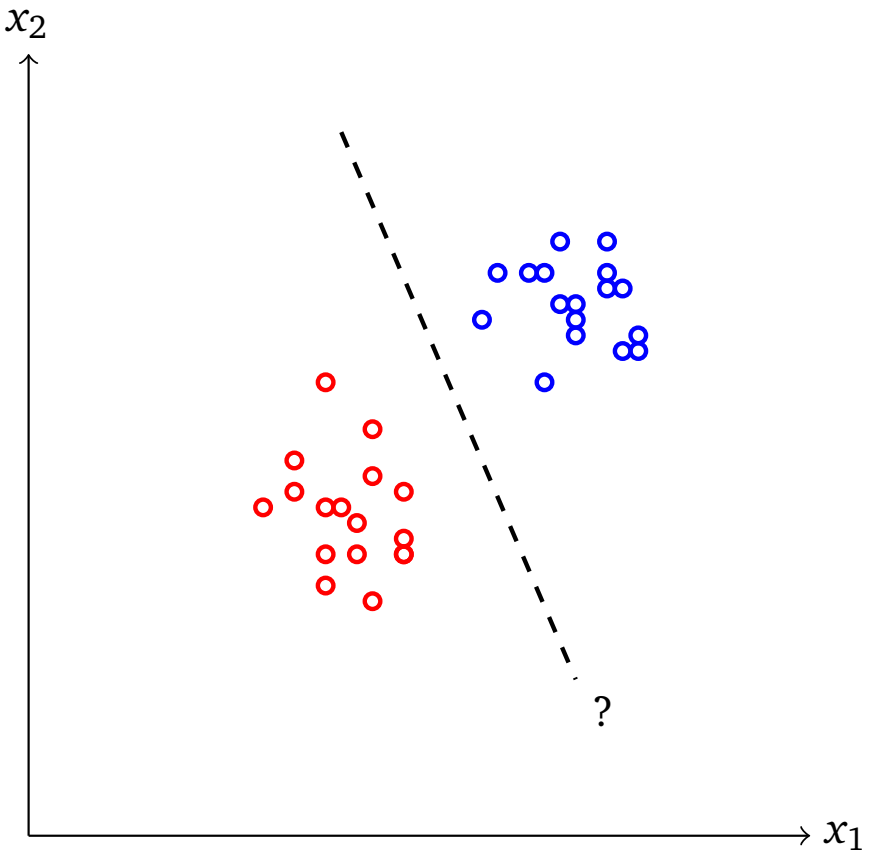
Gyakorlatban: $\boldsymbol{x}_i \in \mathbb{R}^{388}$, $y_i \in \{-1, +1\}$, $T := \{\boldsymbol{x}_i\}_i^P$,
$F :=$ {Hibás program property-jei}, $S :=$ {Javított program property-jei}.
Címkék:

- $y_i = +1 \Leftrightarrow \boldsymbol{x}_i \in F, \boldsymbol{x}_i \notin S$
- $y_i = -1 \Leftrightarrow \boldsymbol{x}_i \in S \cup F$
- $\boldsymbol{x}_i \notin F \Rightarrow \boldsymbol{x}_i \notin T$

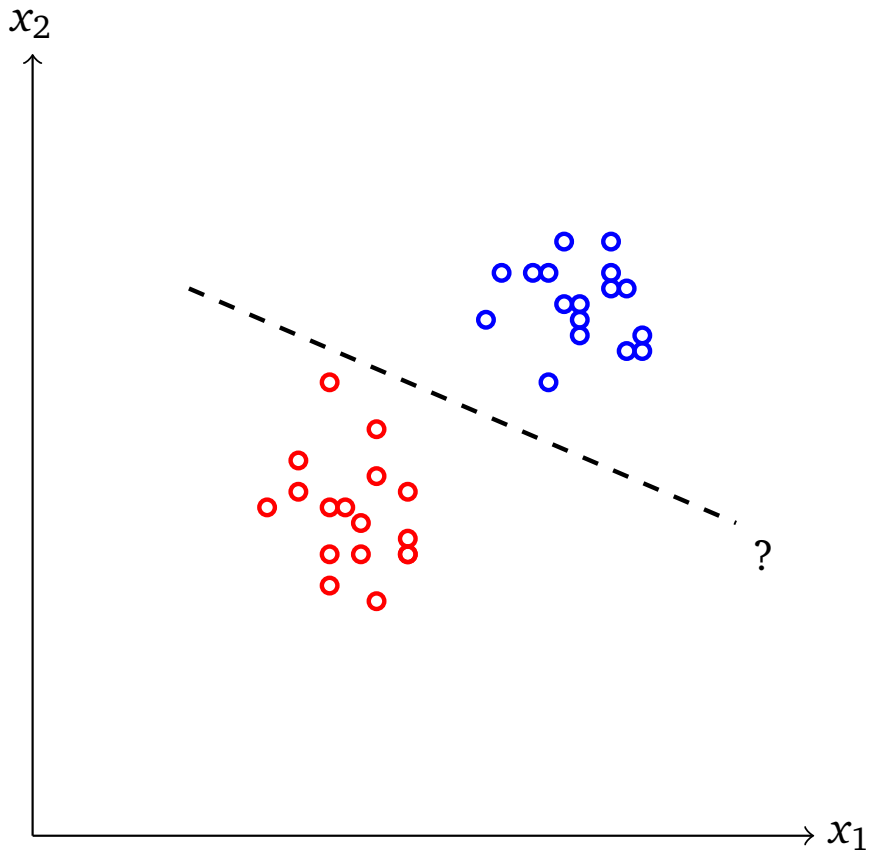
Szupportvektor-gépek



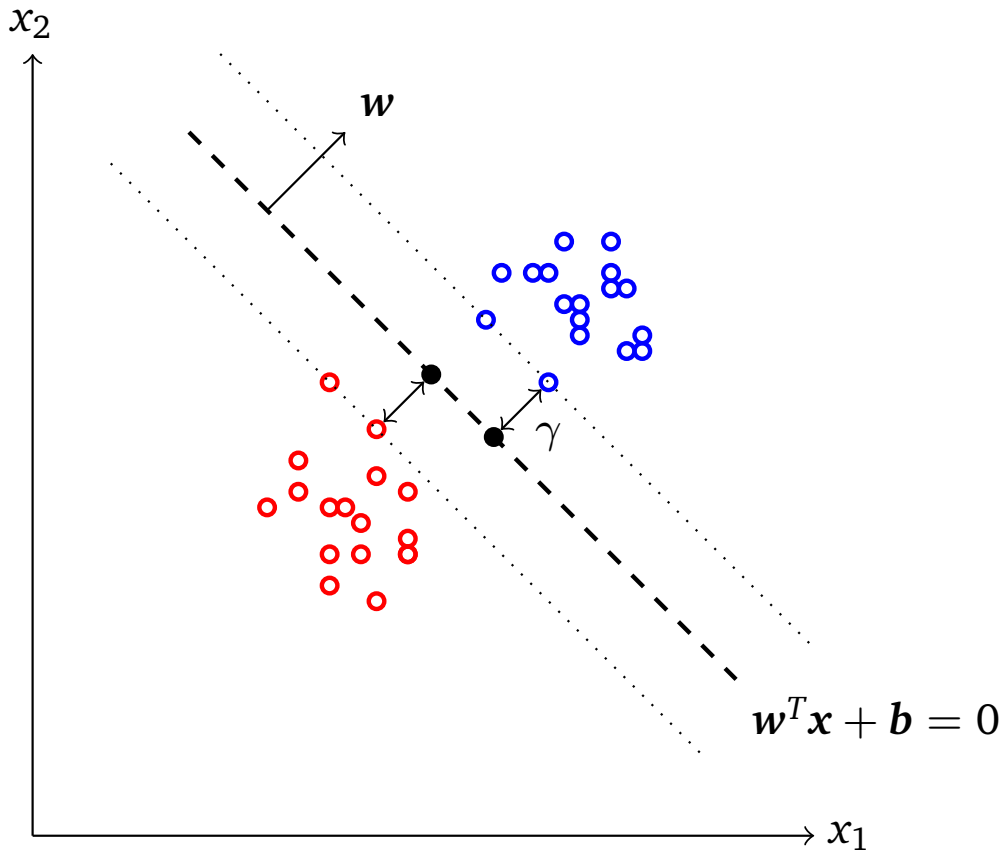
Szupportvektor-gépek



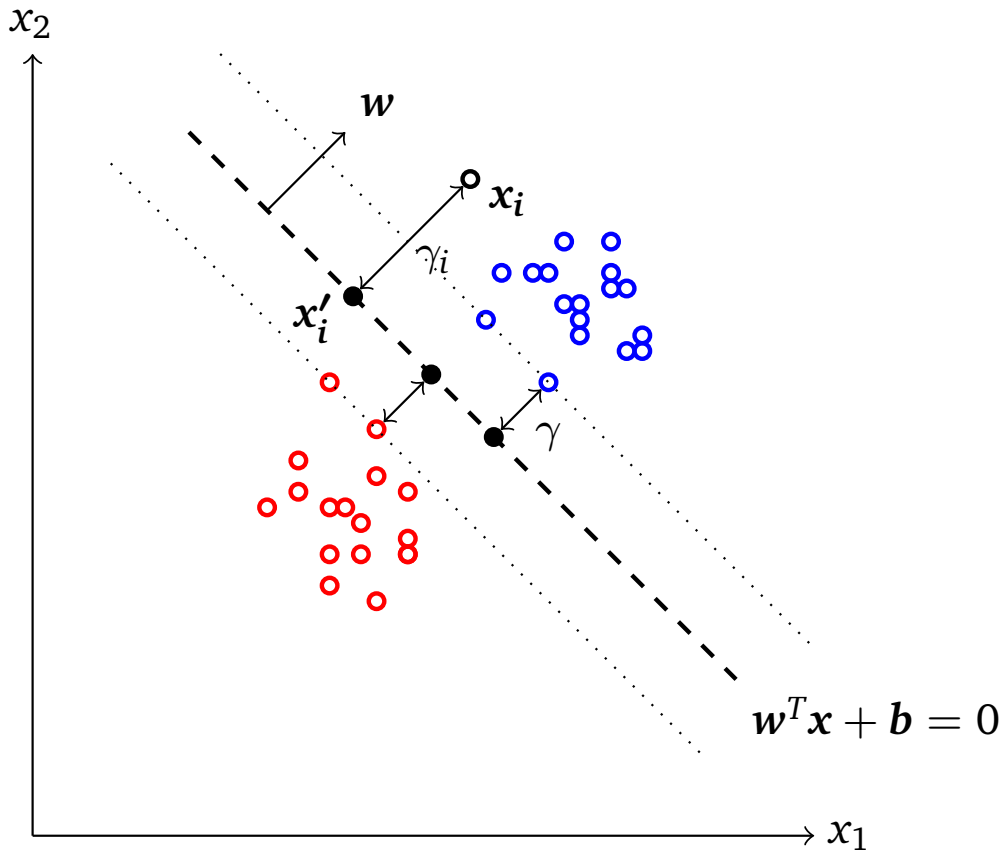
Szupportvektor-gépek



Szupportvektor-gépek



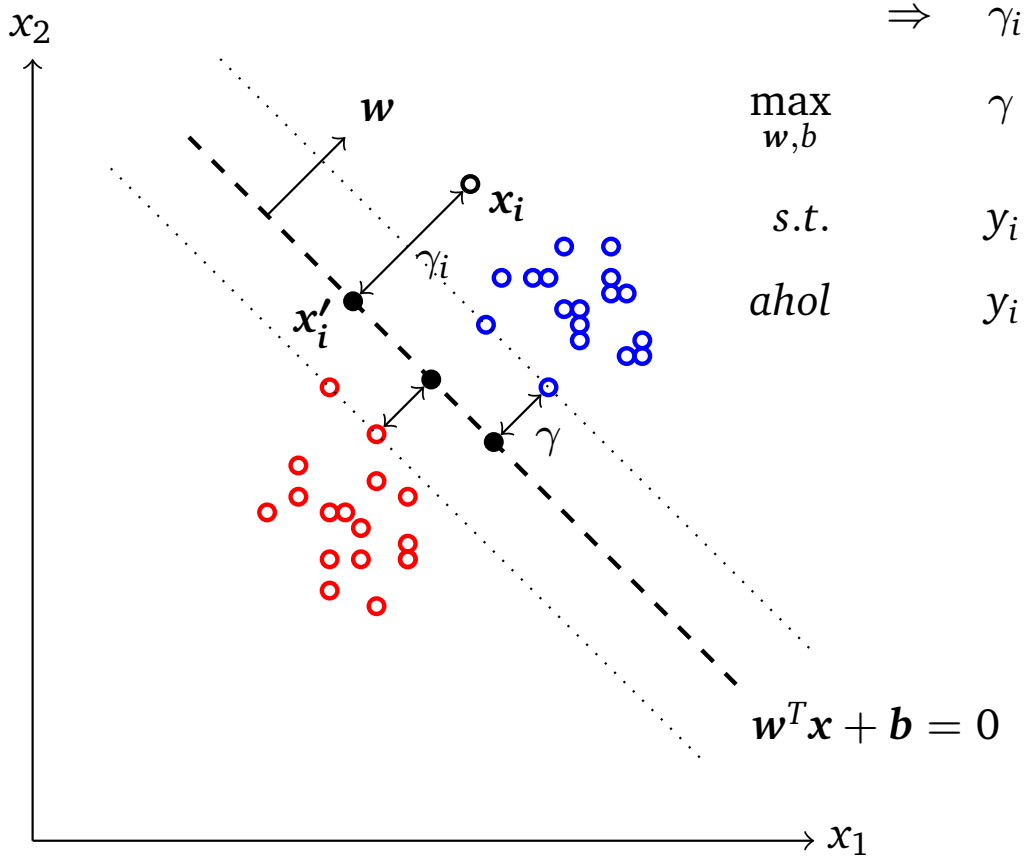
Szupportvektor-gépek



Szupportvektor-gépek

$$\begin{aligned} \boldsymbol{w}^T\boldsymbol{x}_i' + b &= \boldsymbol{w}^T\left(\boldsymbol{x}_i - \gamma_i \frac{\boldsymbol{w}}{\|\boldsymbol{w}\|}\right) + b = 0 \\ \Rightarrow \quad \gamma_i &= \left(\frac{\boldsymbol{w}}{\|\boldsymbol{w}\|}\right)^T \boldsymbol{x}_i + \frac{b}{\|\boldsymbol{w}\|}. \end{aligned}$$

$$\begin{aligned} \max_{\boldsymbol{w},b} \quad & \gamma \\ s.t. \quad & y_i\left(\boldsymbol{w}^T\boldsymbol{x}_i + b\right) \geq \gamma, \quad \|\boldsymbol{w}\| = 1, \\ ahol \quad & y_i \in \{-1, +1\}. \end{aligned}$$



Szupportvektor-gépek

Ekvivalens feladat:

$$\begin{aligned} \min_{\boldsymbol{w},b} \quad & \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} \\ s.t. \quad & y_i\left(\boldsymbol{w}^T\boldsymbol{x_i}+b\right) \geq 1. \end{aligned}$$

„Soft-margin” verzió:

$$\begin{aligned} \min_{\boldsymbol{w},b,\boldsymbol{\xi}} \quad & \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} + C\sum_i \xi_i \\ s.t. \quad & y_i\left(\boldsymbol{w}^T\boldsymbol{x_i}+b\right) \geq 1-\xi_i, \quad \xi_i \geq 0. \end{aligned}$$

Bázisfüggvények + „soft-margin”:

$$\begin{aligned} \min_{\boldsymbol{w},b,\boldsymbol{\xi}} \quad & \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} + C\sum_i \xi_i \\ s.t. \quad & y_i\left(\boldsymbol{w}^T\varphi(\boldsymbol{x_i})+b\right) \geq 1-\xi_i, \quad \xi_i \geq 0. \end{aligned}$$

Duál feladat

$$\max_{\boldsymbol{\alpha}\geq 0,\boldsymbol{\beta}\geq 0}\min_{\boldsymbol{w},b,\boldsymbol{\xi}}\mathcal{L}:=\frac{1}{2}\boldsymbol{w}^T\boldsymbol{w}+\sum_i\left(C-\beta_i\right)\xi_i-\sum_i\alpha_i\left[y_i\left(\boldsymbol{w}^T\varphi(\boldsymbol{x_i})+b\right)-1+\xi_i\right].$$

$$\begin{aligned}
\nabla_{\boldsymbol{w}}\mathcal{L} &= \boldsymbol{w}-\sum_i\alpha_i y_i\varphi(\boldsymbol{x_i})=0\\
&\Rightarrow \quad \boldsymbol{w}=\sum_i\alpha_i y_i\varphi(\boldsymbol{x_i}).\\
\frac{\partial\mathcal{L}}{\partial b} &= -\sum_i\alpha_i y_i=0\\
&\Rightarrow \quad \sum_i\alpha_i y_i=0.\\
\frac{\partial\mathcal{L}}{\partial\xi_i} &= C-\beta_i-\alpha_i=0\\
&\Rightarrow \quad 0\leq\alpha_i\leq C.
\end{aligned}$$

$$\begin{aligned}
\max_{\boldsymbol{\alpha}} \quad & \sum_i\alpha_i-\frac{1}{2}\sum_i\sum_j\alpha_i\alpha_j y_i y_j\varphi(\boldsymbol{x_i})^T\varphi(\boldsymbol{x_j})\\
s.t. \quad & \sum_i\alpha_i y_i=0,\quad 0\leq\alpha_i\leq C.
\end{aligned}$$

A duál közelebbről

Mátrixos formában:

$$\begin{aligned} \max_{\boldsymbol{\alpha}} \quad & \mathbf{1}^T\boldsymbol{\alpha} - \frac{1}{2}\boldsymbol{\alpha}^T Q\boldsymbol{\alpha} \\ s.t. \quad & \boldsymbol{y}^T\boldsymbol{\alpha} = 0, \quad 0 \leq \alpha_i \leq C \\ where \quad & Q_{ij} = y_i y_j \varphi(\boldsymbol{x_i})^T \varphi(\boldsymbol{x_j}). \end{aligned}$$

a predikált címke pedig:

$$y(\boldsymbol{x}) = sgn\left(\boldsymbol{w}^T\varphi(\boldsymbol{x}) + b\right) = sgn\left(\sum_i \alpha_i y_i \varphi(\boldsymbol{x_i})^T\varphi(\boldsymbol{x}) + b\right) = sgn\left(\sum_i \alpha_i y_i k(\boldsymbol{x_i}, \boldsymbol{x}) + b\right),$$

vagy rangsorolás esetén:

$$score(\boldsymbol{x}) = \frac{\left(\sum_i \alpha_i y_i k(\boldsymbol{x_i}, \boldsymbol{x}) + b\right)}{\sqrt{\boldsymbol{\alpha}^T Q\boldsymbol{\alpha}}}.$$

Döntési fák

- Iteratívan, mohó módon mindig a legnagyobb információ-nyereséggel járó particionálás kiválasztása.
- Ember számára is könnyen értelmezhető `ha-akkor` szabályrendszer tanulása.

Entrópia:

$$H(X) = -\sum_i log(p(x_i))p(x_i).$$

Információ-nyereség: a particionálás által kiváltott várható csökkenés az entrópiában:

$$IG(X,a) = H(X) - \sum_{v \in values(a)} \frac{\{\boldsymbol{x} \in X | x_a = v\}}{|X|} H\left(\{\boldsymbol{x} \in X | x_a = v\}\right).$$

Mérési környezet

Program	# fgv	Átlagos NCNB	LOC	Hibás verziók
print_tokens	18	452	539	7
print_tokens2	19	379	489	10
replace	21	456	507	32
schedule	18	276	397	9
schedule2	16	280	299	10
space	137	9568	9826	34
tcas	9	136	174	41
tot_info	7	334	398	23
C összesen	245	11881	12629	166
Geo	49	825	1923	95
Pathfinder	18	430	910	41
Streets	19	1720	4459	60
FDAnalysis	277	5770	8864	11
Java összesen	363	7145	16156	207

Eredmények

Mérések:

- Pozitívnak ítélt minták megítélése javított verziók felhasználásával.
- Fault-revealing property-k gyakorlati felhasználhatóságának megítélésre emberi szakértők segítségével.

Eredmények:

- Rangsorolás jobb a klasszifikációnál.
- C: az első 80 property 45%-a fault-revealing, Java: 59%.
- A legnagyobb méretű programon (space) működött a legjobban.

Szakértői validáció:

- 410 pozitívnak ítélt property-t szakértő ellenőrzött: 65% valós programhiba felfedezéséhez vezetett volna.

Eredmények – példa

Procedure	Program	Description of error	Fault-revealing property
`addstr`	replace	`maxString` is initialized to 100 but `maxPattern` is 50	`maxPattern` > 50
`upgrade_process_prio`	schedule	`prio` is incorrectly set to 2 instead of 1	(`prio` ≥ 2) $\Rightarrow$ `return` ≤ 0