**Tehnici de Optimizare**

*1) Concepte generale*

Amintim înainte câteva concepte de IA relevante lucrării:

* Seturi de date:
  + De antrenare (perechi de date problemă – rezultat folosite pentru a antrena un program de IA)
  + De testare (date pentru care vrem să aflăm rezultatele folosind programul de IA)
* Tipuri de algoritmi de IA:
  + De clasificare
  + Regresii (prezic o valoare fixă)
  + De detectare de anomalii
  + De clustering (gruparea seturilor de date conform unor pattern-uri găsite)
* Tipuri de învățare automată:
  + Supervizată
  + Nesupervizată
  + Învățarea prin feedback
* Variabile:
  + Independente
  + Dependente
* Rezultate:
  + Valori numerice
  + Categorii (valori dintr-un set anume care spun cărei clase de obiecte aparține obiectul analizat)

*2) Optimizări*

Algoritmii de IA trebuie să fie cât mai eficienți și să facă cât mai puține greșeli (adică să aibă acuratețe cât mai mare). Din acest motiv, algoritmii de IA sunt întâi îmbunătățiți din punct de vedere al acurateței, de multe ori rezultând un algoritm complet nou, și apoi din punct de vedere al complexității, ca să folosească cât mai puține resurse și cât mai puțin timp. Numim acest proces optimizarea algoritmilor de IA.

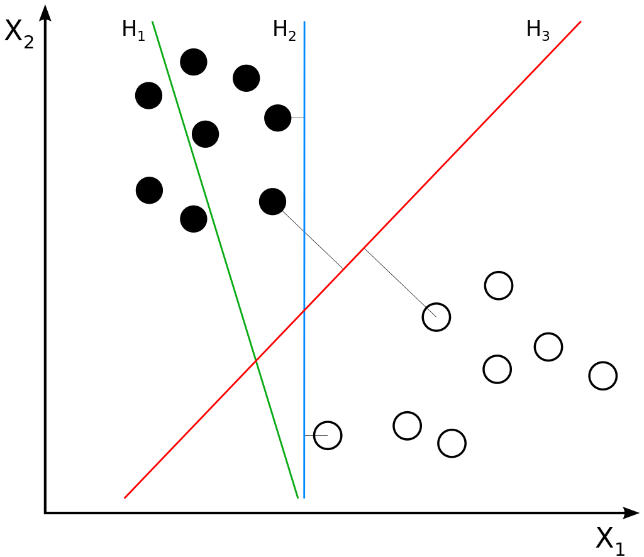
Lucrarea aleasă de noi face optimizări pe algoritmi de IA care folosesc SVM-uri așa că vom discuta SVM-uri și optimizările lor în cele ce urmează.

2.1) SVM

Un SVM (Support-Vector Machine) este un model pentru algoritmi de IA de învățare supervizată. De obicei, SVM-urile sunt folosite de algoritmi de IA de clasificare (de exemplu, KNN) sau de regresie (liniară, multiplă, logistică etc.). Algoritmii care folosesc SVM-uri sunt non-probabilistici. Numele de SVM vine de la modul în care sunt reprezentate datele: având un set de date cu N caracteristici, SVM le reprezintă prin vectori din spațiul , fiecare reprezentând o intrare în setul de date cu fiecare caracteristică măsurată pe o dimensiune a spațiului. Aceste intrări sunt mapate în spațiul SVM-ului astfel încât clasele de date să fie cât mai ușor de separat. Intrări noi sunt puse în aceeași categorie ca cele din subspațiul în care se află.

În cazul în care datele de antrenare nu au categoriile asignate, trebuie trecut de la un algoritm de învățare supervizată la unul de învățare nesupervizată. Algoritmii de acest fel care folosesc SVM-uri fac „clustering” pentru a determina singuri clasele pe baza caracteristicilor comune.

Formal, rolul unui SVM în algoritmii de clasificare este de a reprezenta datele într-un spațiu N-dimensional și de a face posibilă trasarea de hiperplanuri care separa datele în clase. Mai jos avem 3 separări diferite pentru un SVM cu 2 clase.



După cum se observă, H1 nu reușește să separe datele într-un mod corect. H2 reușește acest lucru dar distanța dintre el și date este mică și deci intrări viitoare pot fi clasificate greșit. H3 oferă separarea cea mai bună, cu distanța cea mai mare între date și hiperplan și cea mai bună acuratețe.

Numim un Hiperplan (vizualizat pe un grafic in 2 dimensiuni) dreapta care separă setul de date în două categorii. Convențional, cele două categorii sunt etichetate cu -1 si +1 pentru a facilita formula cu care putem face clasificarea.

De semenea, numim Support Vectori dreptele paralele cu hiperplanul de separare care trec prin cele mai apropiate două puncte din setul de date: unul pe stânga (pentru -1) și unul pe dreapta (pentru +1).

Odată ce avem hiperplanul trasat, putem foarte ușor să prezicem din ce categorie face parte un nou punct ce nu aparține setului de date. Dacă este la stânga, atunci va avea eticheta -1. Altfel, +1.

Numim margini de separare (Street Widths) distanțele de la support vectori la hiperplanul de separare, și sunt notate convențional D- si D+. Ideal, un SVM încearcă să obțină cea mai mare distanță între cele două seturi de date, adică să maximizeze marginile D- si D+.

Un SVM pune o problema constrânsă de optimizare convexă: încercarea de a maximiza distanțele D- si D+.

Dacă ecuația unei drepte este dată de:

y = w \* x + b

Ecuația unui hiperplan este dată de formula:

y = w^T x + b

Adică:

y = w1x1 + w2x2 + ... + wnxn + b

Astfel, problema de optimizare a unui SVM constă în doi factori:

- minimizarea normei lui w

- maximizarea lui b

Nota: ||w|| := norma lui w = sqrt | w1^2 + … + wn^2

Pentru toate punctele de forma (x, y) din setul de date, constrângerea este dată de formula:

y(w^T \* x + b) >= 1

Important: y = 1 sau -1 și se numește clasă (reprezintă eticheta). y NU este coordonata de pe axa OY. Dacă x-urile sunt pe două coordonate, atunci x va conține o coordonată pe axa OX și una pe axa OY.

Există mule w și b care satisfac condiția de mai sus.

Vectorii suport vor satisface ecuația:

y(w^t \* x + b) =~ 1

Un SVM va aproxima valorile respective și vor rezulta valori foarte aproape de soluția exactă. De obicei, o aproximare bună este îndeajuns

Minimizarea normei lui w este o problemă de optimizare convexă deoarece valoarea sa poate fi reprezentată pe un grafic convex; punctul minim de pe grafic va fi punctul optim.

În acest caz, pentru că graficul este convex, ||w|| minim se numește punctul de minim global.

Rezolvarea banală a problemei unui SVM este prin forța brută: se incearcă „toate” opțiunile făcând pași constanți până găsim cel mai mic ||w||.

La fiecare pas, se testează condiția y(w^T + b) pentru toate punctele (x, y).

Deoarece semnele coeficienților lui w contează, când încercăm un anumit w, trebuie sa încercăm toate combinațiile posibile de semne ale elementelor sale.

Spre exemplu: dacă w este (5, 5), va trebui să încercăm și (-5, 5), (-5, -5) și (5, -5).

Complexitatea acestui algoritm este:

n(w) \* n(sw) \* n(dataset) \* n(b)

Unde:

n(w) := numărul de iterații prin w

n(sw) := numărul posibilităților semnelor lui w

n(dataset) := numărul de puncte din setul de date

n(b) := numărul de iterații prin care trecem ca să îl aflăm pe b

Notă: testarea semnelor elementelor lui w se poate face prin generarea tuturor vectorilor de aceeași dimensiune ca w de forma (+/-1, +/-1, ... +/-1); inmulțirea lui w transpus cu un astfel de vector va rezulta într-o versiune a lui w în care termenii săi au semnele elementelor din vectorul respectiv.

În anexa lucrării se poate găsi un exemplu simplu de implementare a unui SVM în limbajul Python (Python 3.6); programul este bine documentat în codul sursă.

Algoritmul abordat este puțin mai eficient decât forța brută.

La fiecare pas pentru ||w|| se verifică dacă valoarea curentă este mai mică decât cea precedentă. Dacă da, atunci continuăm. Dacă nu, atunci schimbăm sensul parcurgerii (pentru că înseamnă că am trecut de punctul de minim) și micșorăm drastic mărimea pasului. În algoritm avem un număr arbitrar/euristic de epici prin care trecem - repetăm de câteva ori tot procesul (de 3 ori în algoritm) și rămânem cu o valoare aproximativă decentă pentru w și b.

Un algoritm de optimizare și mai eficient este „Gradient Descent”, aplicat pentru a găsi minimul local al unei funcții diferențiabile. Pentru a găsi minimul funcției cu „Gradient Descent”, facem pași proporționali cu inversul gradientul aplicat funcției în punctul curent. Discutăm „Gradient Descent” și „Stochastic Gradient Descent” in descriere algoritmilor implementați în 3.2) și 3.3). Anexa conține implementarea celor două tipuri de Gradient Descent asupra unei regersii liniare.

2.2) Kernel Tricks

De cele mai multe ori, separarea nu se poate face printr-un hiperplan drept.

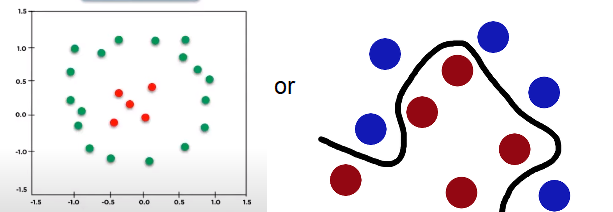
Spre exemplu, dacă setul nostru de date este pe o singură dimensiune (adică x-șii din setul de date au un singur element fiecare), putem avea situația următoare:

IMG_256

În acest caz nu putem separa punctele cu un singur hiperplan unidimensional.

Putem folosi un ”Kernel Trick” (o functie kernel) care adaugă o dimensiune în plus setului de date pentru a reprezenta punctele într-un plan bidimensional pe o parabolă. Pentru fieacare punct pe coordonata x, calculăm kernel(x) pe axa OY. Astfel vom putea separa punctele printr-o dreaptă.

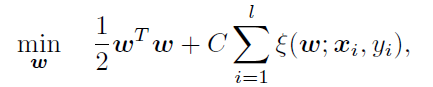
Alt caz pentru un Kernel Trick este când avem puncte în mijloc sau plasate „aleator” în două dimensiuni.



În aceste cazuri, vom aplica o funcție kernel de la 2 dimensiuni la 3 dimensiuni și vom putea separa datele cu un hiperplan tridimensional.

2.2) L1-SVM și L2-SVM

L1-SVM și L2-SVM sunt optimizări pe SVM. L1-SVM și L2-SVM încearcă să reprezinte datele astfel încât distanțele dintre grupuri („cluster”) de date să fie cât mai mare și astfel distanța dintre date și hiperplanele care le separă să fie cât mai mare și eroarea să fie cât mai mică. Se încearcă aceasta fără o distorsionare prea mare a datelor prin rezolvarea problemei de optimizare:



Diferența dintre L1-SVM și L2-SVM este valoarea aleasă pentru funcția

L1-SVM:

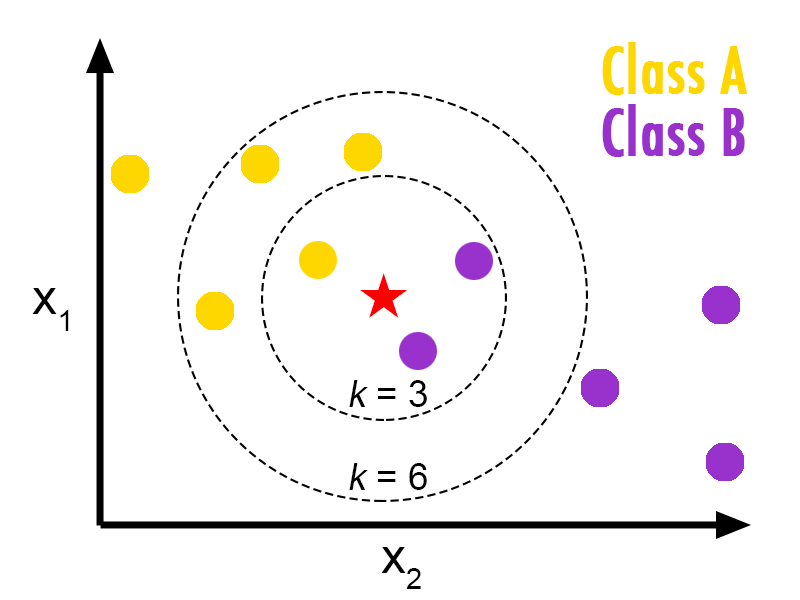
L2-SVM:

*3) Algoritmi implementați*

În cazul algoritmilor de IA, acuratețea și minimizarea numărului de operații complexe efectuate de aceștia sunt factorii cei mai importanți care descriu un algoritm. În implementările noastre am încercat să creștem semnificativ acuratețea unor algoritmi de IA și apoi să îi optimizăm.

3.1) Optimizări pe KNN

Algoritmul KNN este unul din cei mai simpli algoritmi de clasificare. KNN (K-Nearest Neighbours) decide clasa unei intrări astfel: algoritmul caută cei K mai apropiați vecini ai intrării și îi asignează clasa cea mai comună dintre acești vecini.



Deși algoritmul este simplu de înțeles și implementat, exista 2 factori importanți care pot influența acuratețea și performanța algoritmului: funcția aleasă pentru calcularea distanței și valoarea aleasă pentru K. Există multe funcții propuse pentru calcularea distanței, cea mai comună fiind distanța Euclidiană ~~distanța Euclidiană fiind cea mai comună~~ și este cea aleasă de noi în implementări.

Avem trei implementări de KNN care rulează concomitent, cu optimizări alese pentru găsirea unei valori pentru K. Aceștia sunt antrenați pe același set de date de antrenare (numit A) și acuratețea lor la finală este măsurată pe același set de date de testare (numit T).

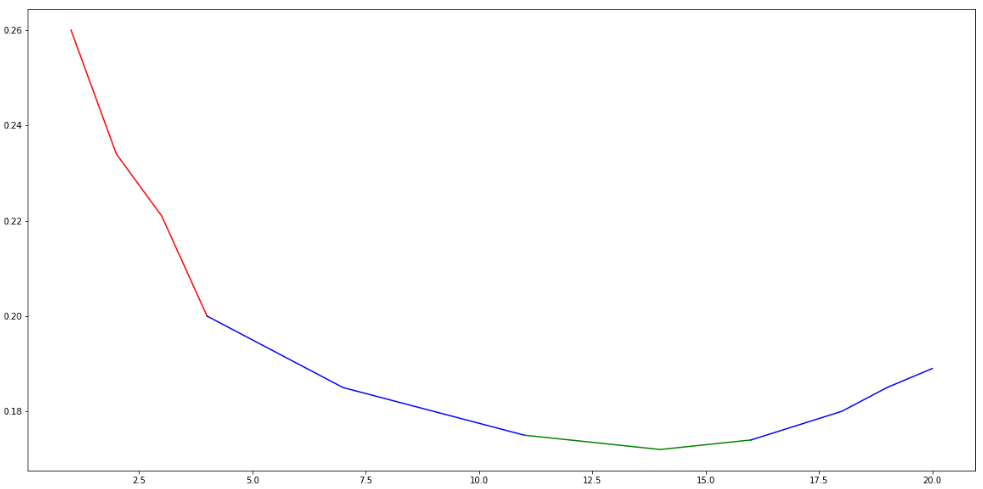
Prima implementare este un KNN simplu, fără optimizări, cu valoarea lui K aleasă ca 3 (majoritatea implementărilor aleg un K arbitrar, cel mai des 2 sau 3). Deși aceasta este cea mai rapidă dintre implementări, suferă din punct de vedere al acurateței.

Celelalte implementări împart setul de date de antrenare in 2: un set pe care se face antrenarea efectivă (90% din datele totale ale setului de antrenare, pe care îl numim α) și un set de testare pentru K (restul datelor de antrenare, pe care îl numim β). După selectarea unui K și antrenarea datelor pe α, se testează acuratețea algoritmului pe setul β.

Al doilea algoritm măsoară acuratețea modelului pentru toate valorile posibile ale lui K (de la 1 la N, unde N este numărul intrărilor din α) și alege K cu cea mai bună acuratețe. Această implementare devine foarte lentă și ineficientă pentru un set de date foarte mare.

Al treilea algoritm aplică o metodă „Divide et Impera” pentru a-l alege pe K, folosind tot acuratețea pentru alegerea sa. Se pornește de la intervalul 1, ..., N și se aplică recursiv până se găsește K optim. Pentru un interval ales, se măsoară acuratețea pentru valorile din capetele sale, intervalul restrângându-se la jumătate în funcție de valorile acestea. Algoritmul este mult mai eficient ca cel precedent și știm că găsește aceeași valoare optimă, cu excepția cazurilor în care seturile de date sunt foarte mici și acuratețea pe valorile lui K nu este stabilă. Noi am găsit un set de date relativ mic pentru antrenare si testare (300 de intrări în total, antrenarea efectivă fiind făcută pe 67 de intrări), totuși se observă că algoritmul funcționează și pe acesta, algoritmii 2 și 3 având aceeași acuratețe. Numărul mic de date de intrare pe care îl avem explică și acuratețea slabă în general a modelului nostru (57.70 pentru algoritmul 1 și 62.55 pentru algoritmii 2 și 3) deoarece KNN are nevoie de seturi de date mai mari decât alți algoritmi de clasificare pentru a ajunge la o acuratețe bună. Totuși, și în aceste condiții, se observă o creștere semnificativă a acurateței măsurate pe setul T după aplicarea algoritmilor.

Al treilea algoritm este optimizat și are cea mai bună acuratețe. Mai jos avem un grafic, reprezentativ KNN aplicat pentru seturi mari de date. Pe axa OX sunt valorile alese pentru K și pe OY este eroarea de clasificare (invers proporțională cu acuratețea).



După cum se observă, pentru valori mici ale lui K (primele 2 secțiuni) eroarea este foarte mare dar scade cu cât K crește, ajungând până la un interval de stabilizare (secțiunea verde) în care se află K-ul optim (cu eroarea cea mai mică) și apoi începe iar să crească (ultima secțiune).

3.2) Gradient Descent

Gradient Descent este o tehnică de optimizare pentru găsirea punctului de minim al unei funcții convexe. Această tehnică se poate aplica la multi algoritmi de IA, precum Regresia Liniară, Regresia Logistică sau Support Vector Machine.

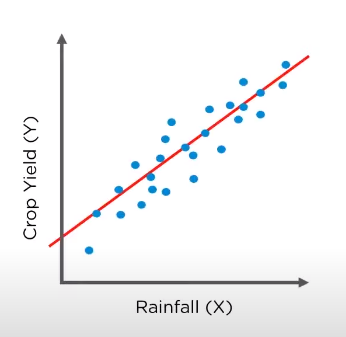
Dacă o dreaptă are o pantă, un hiperplan are un gradient.

Algoritmul se bazează pe repetarea a 3 pași:

1. Alegerea unei direcții de parcurgere. Se analizează panta în punctul curent din iterație pe baza derivatei funcției
2. Se alege o dimensiune a pasului. Dacă iteratia este departe de punctul minim, se vor face pași mai mari. Cu cât se apropie de punctul minim, cu atât pasul este mai mic, și deci are o acuratețe mai bună.
3. Se face verificarea convergenței. Se verifică dacă s-a găsit punctul de minim sau dacă s-a apropiat destul de mult de el.

În continuare, se va descrie Gradient Descent aplicat asupra unei regresii liniare.

O regresie liniară trasează o linie pe graficul setului de date care să fie cât mai aproape pe axa OY de toate punctele de pe grafic. Astfel se poate prezice o coordonata a unui nou punct (cu o marjă de eroare care trebuie luată în calcul).



Această marjă de eroare este utilă și se numește eroare reziduală. Ea se calculează cu formula:

Res(punct) = punct.y - c - m \* punct.x

Unde m și c sunt panta și interceptul ecuației dreptei regresiei:

y = m \* x + c

Deși panta m poate fi aflată eficient cu Gradient Descent, vom folosi metoda Least Squares pentru aflarea acesteia. Gradient Descent intervine pentru aflarea valorii c.

Pentru aflarea pantei dreptei, întâi se calculeaza media x-șilor (notată media\_x) și media y-lor (notată media\_y).

Pentru fiecare punct (x, y), fie x’ = x - media\_x, fie y’ = y - media\_y.

Panta m se afla din următoarea formulă:

m = (Suma x’ \* y’) / (Suma x’^2)

Se pornește cu c la o valoare euristică în ”stânga” punctului de minim. Opțional, pentru a începe la o valoarea corectă, putem folosi

Fie Loss(c) funcția de loss, și se calculează cu formula:

Loss(c) = Sum -- for each dataset point -> Res(point)^2

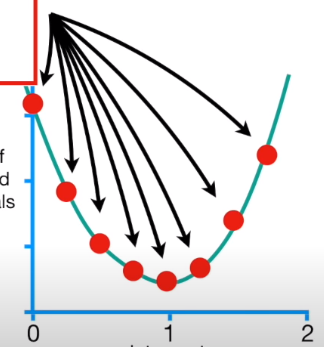
Funcția obiectiv a algoritmului de optimizare este funcția Loss

Notă: există multe variații a funcției Loss.

Scopul algoritmului este, deci, să minimizeze funcția Loss.

Din moment ce punctele se știu și m se știe, singura variabilă a funcției Loss este c.

Deoarece c poate crește liniar, iar Loss(c) este o parabolă, punctele de forma (c, Loss(c)) formează un grafic convex (c este pe axa OX iar Loss(c) pe axa OY):

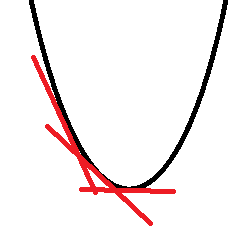


Cu cât linia regresiei se apropie de c-ul perfect, cu atât se apropie c-ul de punctul de minim de pe graficul de mai sus.

În continuare trebuie calculată derivata funcției Loss:

Loss’(c) = Sum | for each dataset point -> (-2) \* Res(point)

Aceasta este utilă pentru aflarea pantei într-un anumit punct. Cu cât iterația se apropie de punctul de minim al funcției Loss, cu atât panta derivatei devine mai aproape de 0:



Tot ce rămâne este să definim incrementarea lui c în funcție de o rată de învățare aleasă euristic 0.05:

c <- c + abs(Loss’(c)) \* 0.05

Algoritmul se încheie când Loss’(c) se apropie suficient de mult de 0.

După algoritm, rămânem cu ecuația unei drepte y = mx + c care trasează o linie aproximativ egal îndepărtată de toate punctele pe axa OY.

3.3) Stochastic Gradient Descent

Stochastic Gradient Descent este o metoda de optimizare bazata pe Gradient Descent si aproximeaza minimul unei functii.

În Gradient Descent obisnuit se calculeaza derivata funcției Loss, care are ca punct de minim valoarea optimă pentru c (intercept). Panta se află prin derivata funcției Loss într-un punct c; cu cât se apropie de panta egala cu 0, cu atât se apropie de soluție.

La fiecare iterație, Gradient Descent trebuie să itereze prin toate punctele din setul de date. Această metodă este foarte înceată când avem seturi mari de date. Spre exemplu, 1.000.000 de date înseamnă că algoritmul este de 1.000.000 de ori mai încet decât Stochastic Gradient Descent. Iată de ce:

În Stochastic Gradient Descent, funcția Loss nu iterează prin toate punctele, ci printr-un singur punct luat aleator. La fiecare apelare a funcției Loss, se ia un alt punct aleator din setul de date și se folosește calculul formula

StocLoss(c) = (r.y - m\*r.x - c)^2

Unde r este un punct aleator din setul de date.

Ca urmare, funcția Loss este mai imprecisă, dar mult mai rapidă pentru seturi mari de date.

Derivata funcției StocLoss este:

StocLoss’(c) = (-2)(r.y - m\*r.x - c)

Calculând derivata acesteia intr-un punct aleator, ne vom apropia încet de punctul c optimi, adică de punctul minim al funcției StocLoss(c).

Anexa lucrării conține un exemplu simplu de Stochastic Gradient Descent pentru regresia liniară.

*4) Lucrarea „A Dual Coordinate Descent Method for Large-scale Linear SVM”*

Problema data este una de optimizare pentru un SVM de clasificare binara (adică doar 2 valori posibile de rezultat, -1 si 1). Se analizează N caracteristici (fiecare devine o dimensiune in SVM). Abordarea lucrării este de a caută caracteristicile cele mai importante ale căror valori determina aceasta clasificare. Unele date nu sunt importante pentru clasificare si pe ele se efectuează operații costisitoare care nu sunt necesare altfel.

Problema inițiala de creare a unui clasificator primește la început un set de date:

{(, ), . . . ,(, )}

care sunt date de antrenare si pe baza cărora se construiește clasificatorul.

reprezintă un punct in spațiul care definește unic o data de intrare. Datele propriu-zise pe care se va aplica acest algoritm de clasificare vor fi tot din spațiul .

reprezintă valori din {-1, 1} si sunt clasele din care aparțin aceste puncte xi.

Problema inițiala se concentrează pe construirea unui asemenea clasificator folosind un SVM, importanta fiind acuratețea si nu optimizarea algoritmului. Problema abordata de articol este optimizarea acestui clasificator.

Funcțiile SVM „loss function”, de exemplu L1-SVM și L2-SVM fac aceasta optimizare însă algoritmii sunt costisitori, mai ales pe seturi de date foarte mari. Se încearcă deci mai multe metode de modificare a acestor algoritmi pentru a reduce numărul de calcule efectuate. Metoda descrisa in articol este o metoda aplicata pe L2-SVM de optimizare a acestui algoritm.

Metoda consta in aplicarea mai multor iterații asemenea celei descrise mai jos, pornind cu un :

Iterația :

pentru i = 2 la N:

=

, unde

// calculam pentru a fi folosit la pasul următor

Funcția f descrisa mai sus face calcule numai in cazul in care e nevoie. De fiecare data când se folosește acest f (o data per integrație mica, N ori per iterație mare) se calculează un gradient pe componenta curenta (i din iterația mica). Daca proiecția gradientului este 0 (dreapta d=0 este optimul ecuației ), rezulta ca nu mai trebuie updatata componenta i din si suntem scutiți de calcule adiționale pentru aceasta iterație, de aici optimizarea.

Proiecția gradientului se calculează astfel: