Modeling

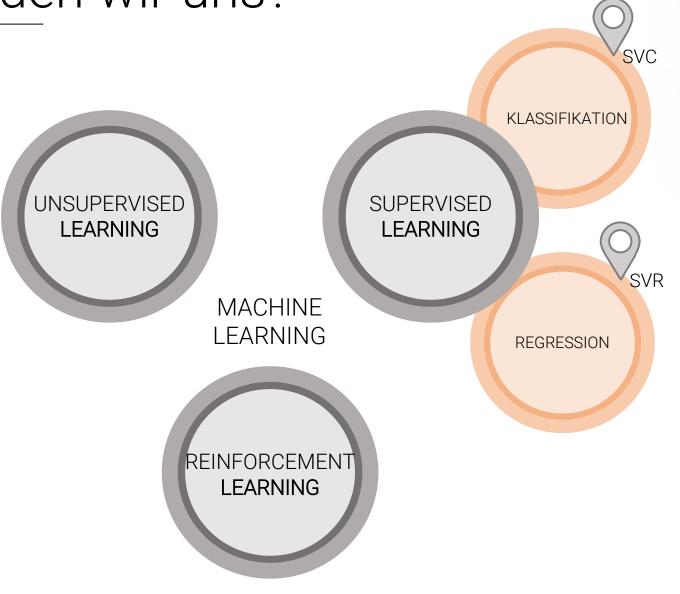
Supervised Learning: Support Vector Machines

Agenda

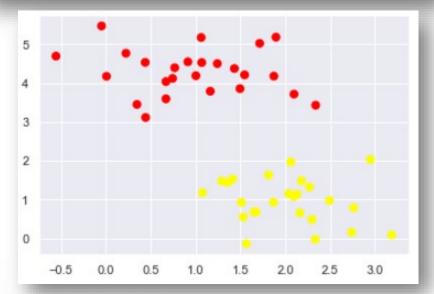


- 1. SVM: Margin Maximierung und Support Vectors
- 2. Mathematischer Hintergrund zu SVMs
- 3. Soft-Margin SVM und Optimierung
- 4. Nicht-lineare Probleme und Kernel-Trick

SVM: wo befinden wir uns?



SVM: allgemein



Unsere Ausgangssituation:

Zwei Klassen in einem 2D-Featureraum, die wir mit einem Klassifikator zu trennen versuchen

Was denken Sie?

Welches Problem sehen wir hier sofort?

- Support Vector Machines (SVM) sind eine der bekanntesten Modelle im Machine Learning
- Vor allem für klein- und mittelgroße Datensätze geeignet
- Sie sind flexibel und können für Klassifikations- und Regressionsprobleme verwendet werden
- SVMs stellen im Kontext der Klassifikation diskriminative Klassifikatoren dar

Was denken Sie?

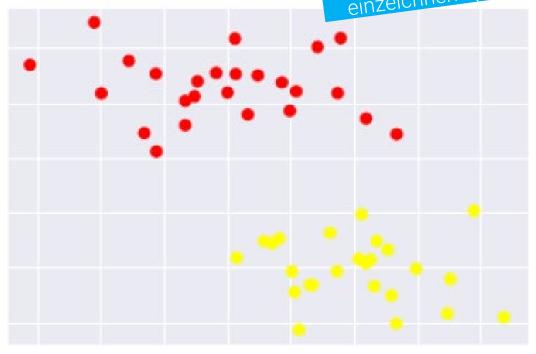
Was heißt diskriminativ?

Wir als Klassifikatoren 2

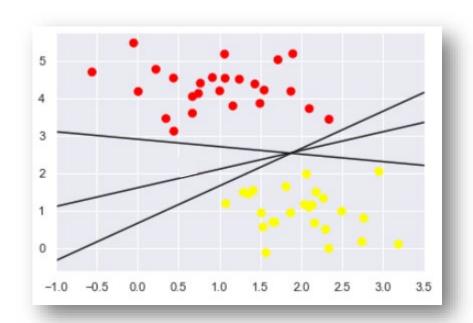


Was denken Sie?

Wie würden Sie – als Klassifikator – eine optimale Trennlinie einzeichnen? (Zoom: zeichnen)



SVM: allgemein



- Wir können also beliebig viele Geraden einzeichnen, die unsere Klassen trennen
- Alle drei Geraden separieren unsere Klassen quasi ideal
- Wie sieht es nun mit neuen Datenpunkten aus? Je nachdem welche Gerade wir in unsere Ausgangssituation legen, können neue Datenpunkte unterschiedlich klassifiziert werden

```
1  xfit = np.linspace(-1, 3.5)
2  plt.scatter(X[:, 0], X[:, 1], c=y, s=50, cmap='autumn')
3  plt.plot([0.6], [2.1], 'x', color='red', markeredgewidth=2, markersize=10)
4  for m, b in [(1, 0.65), (0.5, 1.6), (-0.2, 2.9)]:
6   plt.plot(xfit, m * xfit + b, '-k')
7  plt.xlim(-1, 3.5);
```

Was denken Sie?
Wie würden Sie intuitiv

Wie würden Sie intukk das "x" zuordnen – je nach Gerade? Was denken Sie?

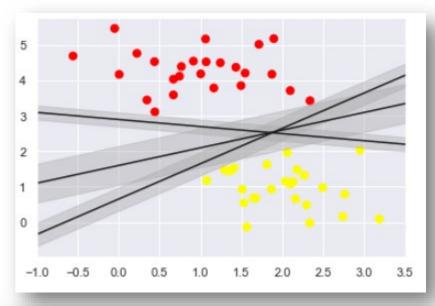
Wie würden Sie intuitiv entscheiden, welche Gerade die beste ist?

SVM: Margin Maximierung



Was denken Sie?

Was könnte man noch tun – außer nur eine Gerade zu zeichnen?



- Anstatt nur eine "nackte" Gerade zur Trennung der Klassen zu nutzen, wird ein sog. Margin (dt. Rand, Spanne) um die Gerade gelegt
- Dieser Margin wird bis zu den nächstliegenden Punkten der Klassen erweitert
- Die optimale Gerade ist dann die mit dem größten Margin
- → SVMs sind sog. *Maximum Margin Estimators*



Was denken Sie?

Welche Gerade wird wohl die beste sein – und warum?

SVM: Fitting/Training



• Wie wir es bei der Einführung der sklearn-Syntax gelernt haben instanziieren wir das SVM Modell Support Vectors

```
SVC(kernel=<kernel_type>, C=<regularization_parameter_value>)
```

Was kernel und C repräsentieren lernen wir später

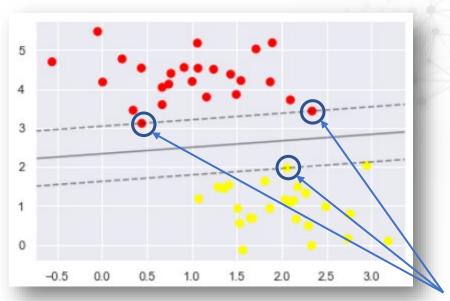
- Dann können wir die .fit()-Methode verwenden, um das Modell auf unsere Daten in x (Features) und y (Labels) anzupassen/fitten/trainieren
- Dadurch erhalten wir die Trennlinie mit dem maximalen Margin, die unsere beiden Klassen am besten trennt
- SVC bedeutet Support Vector Classifier SVMs können also auch regressiv verwendet werden

SVM: Support Vectors

- Diese Support Vectors stellen einen entscheidenden Aspekt dieses ML-Modells dar
- Der Fit des Modells hängt nur von diesen Datenpunkten ab!
- Wir können über das Attribut

 support_vectors_ auf diese

 zugreifen

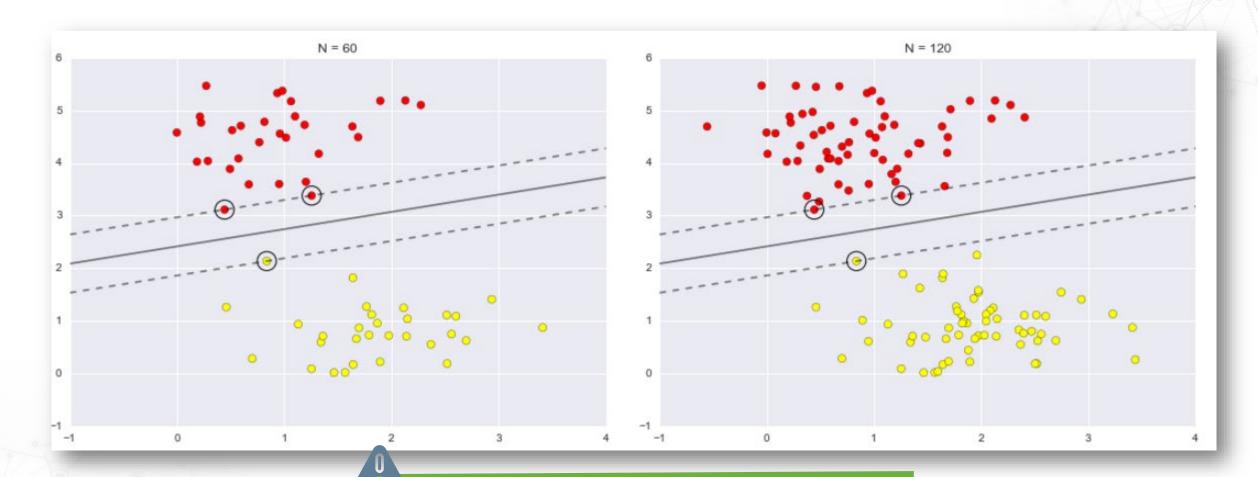


Support Vectors

So what?
In höheren Dimensionen spricht man nicht mehr von Geraden, sondern Hyperebenen, die unsere Klassen trennen



SVM: Support Vectors



So what?
Diese Unempfindlichkeit des Modells auf entfernt
liegende Punkt ist eine der Stärken dieser Art ML-Modelle

Wir als Klassifikatoren 2.0 2.1



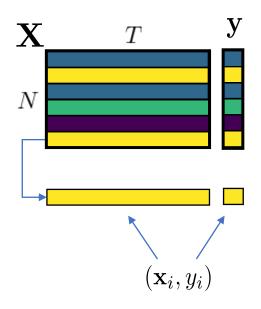
Was denken Sie?

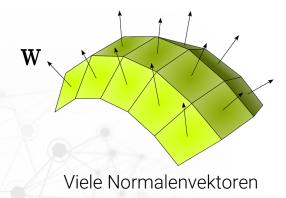
Wie würden Sie <u>nun</u> – als Klassifikator – eine optimale Trennlinie einzeichnen? (Zoom: zeichnen)

Was denken Sie?

Was sind die Support Vektoren? (Zoom: zeichnen)







Uns liegt ein historischer Datensatz bzw. Trainingsdatensatz vor

$$\{(\mathbf{x}_i, y_i)|i=1,\ldots,N, y_i \in \{-1,1\}\}$$

Anhand dessen wird unsere Hyperebene gelernt. Wir beschreiben unsere Hyperebene mittels des Normalenvektors **W** durch den Ursprung

und des Abstandes vom Ursprung b , den man Bias nennt

Mit diesen beiden Informationen haben wir eindeutig eine Hyperebene im Raum definiert



Was denken Sie?

Wie drückt man das in einer Formel aus?



Für die Datenpunkte auf der Hyperebene gilt

$$\langle \mathbf{w}, \mathbf{x}_i \rangle + b = 0$$

Für Punkte, die nicht auf der Hyperebene liegen ist diese Gleichung nicht 0, sondern positiv (Richtung w) bzw. negativ (entgegengesetzt zu w)

Wenn also eine Hyperebene alle Punkte unserer Klassen voneinander trennt, dann weisen die Punkte einer Klasse alle entweder positive oder negative Vorzeichen auf



Was denken Sie?

Was gilt für Punkte, die nicht auf der Hyperebene liegen?



Was denken Sie?

Wie berechnet man also die Klassen/Labels neuer Daten? Für unsere Klassen gilt dann also

Aus den unendlich vielen Hyperebenen wählt man nun die, die den größten

$$y_i = \operatorname{sgn}(\langle \mathbf{w}, \mathbf{x}_i \rangle + b)$$
 Unser Modell! $y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \geq 0$

Wie könnten wir das

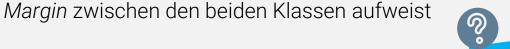
mit einer Ungleichung ausdrücken?

Was denken Sie?



Was denken Sie?

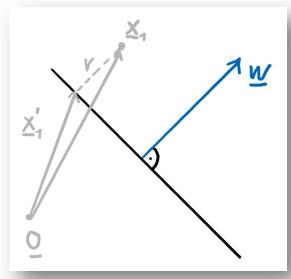
Was sucht also der Trainingsprozess?

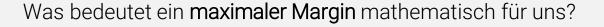


Was denken Sie?

Warum soll der Margin maximiert werden?

$$\mathbf{x}_1 = \mathbf{x}_1' + r \frac{\mathbf{w}}{||\mathbf{w}||}$$





Der Margin wird durch den Abstand zu den nächsten Punkten der Klassen zur Hyperebene definiert – wir brauchen also einen Abstand

Mit diesem Abstand *r* können wir nun unsere **Bedingung**, auf den jeweiligen Seiten der Hyperebene nur Datenpunkte je einer Klasse vorzufinden formulieren

$$y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \ge r$$

Wir können nun ein Optimierungsproblem formulieren

$$\max_{\mathbf{w},b} r$$

unter den Bedingungen

$$y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \ge r$$
 $||\mathbf{w}|| = 1$ $r > 0$

Der Normalenvektor sei nun **nicht mehr normalisiert**. Um das Optimierungsproblem *berechenbar* zu machen, müssen wir eine kleine Umformung machen: durch eine **Skalierung** der Daten auf die Bedingung

$$\langle \mathbf{w}, \mathbf{x}_a \rangle + b = 1$$

mit \mathbf{x}_a als der nächste Punkt zur Hyperebene (Support Vector) und den vorher definierten Abstand kann gezeigt werden, dass

$$r = \frac{1}{||\mathbf{w}||}$$

und für unsere Bedingung gilt dann

$$y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \ge 1$$

Damit reduziert sich unser Problem auf

$$\max_{\mathbf{w},b} \frac{1}{||\mathbf{w}||}$$
 bzw. $\min_{\mathbf{w},b} \frac{1}{2} ||\mathbf{w}||^2$

unter der Bedingung

$$y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \ge 1$$



Was denken Sie?

Wieso heißen diese Bedingungen **Hard Margin**?

SVM: Hard- und Soft-Margin



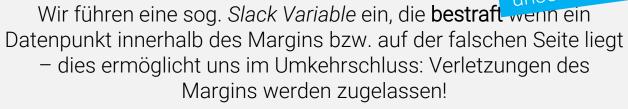
- Bei SVMs hat man die Möglichkeit die Margins entweder starr bzw. hard oder weich bzw. soft zu definieren
- In anderen Worten: lässt man zu, dass Datenpunkte innerhalb des Margins auftauchen dürfen – Leitfrage: wie viele bzw. zu welchem Ausmaß?
- Hierzu gibt es einen Hyperparameter, der getuned werden muss – in sklearn ist es das Argument C
- Große Werte entsprechen einem Hard-, kleine Werte einem Soft-Margin
- Der optimale Wert von C hängt also vom Datensatz ab und muss via z.B. Cross-Validation bestimmt werden
 - → Zuerst schauen wir, wo in der Mathematik dieses C zu finden ist

SVM: Soft-Margin: Mathematik



Was denken Sie?

Was ändern wir an unseren Formulierungen?

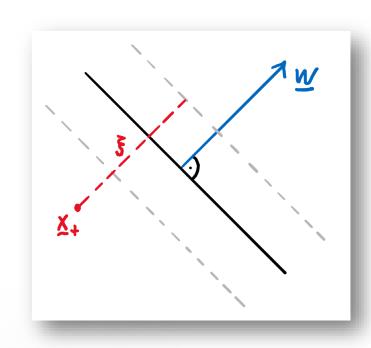


$$\min_{\mathbf{w},b,\xi} \frac{1}{2} ||\mathbf{w}||^2 + C \sum_i \xi_i$$
 mit den Bedingungen

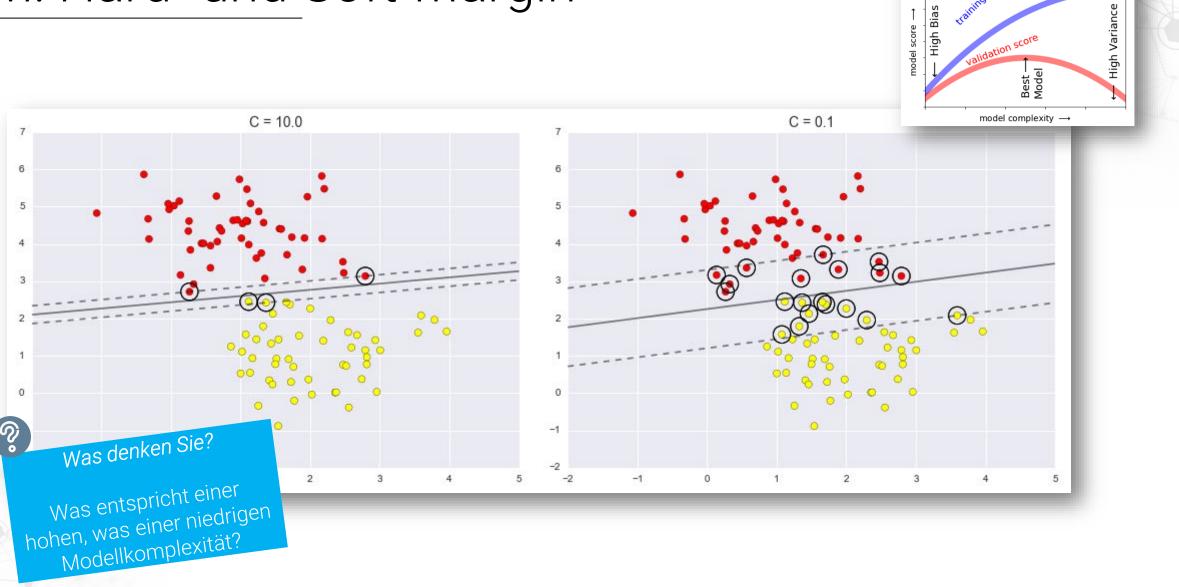
$$y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \ge 1 - \xi_i$$
 und $\xi_i \ge 0$

Der Parameter C versucht also eine Balance bzw. einen Trade-Off zwischen "Größe des Margins" und "Verletzung dessen" herzustellen

Zu diesem Parameter sagt man Regularisierungsparameter



SVM: Hard- und Soft-Margin



ि

Validation Curve Schematic

Die naheliegendste Formulierung einer Loss Function wäre d Accuracy – also: wie gut decken sich Vorhersage und Labels

SVM: Optimierung mittels Loss Function @

Diese ist jedoch ungeeignet, da es sich hierbei um ein sog. kombinatorisches Optimierungsproblem handelt

Eine kontinuierliche Loss Function ist also anzustreben – mögliche Formulierung: **Hinge Loss**

$$L(t) = \max\{0, 1 - t\}$$
 mit $t = yf(\mathbf{x}) = y(\langle \mathbf{w}, \mathbf{x} \rangle + b)$

Damit ergib sich unser letztendlich optimierbares Problem zu

$$\min_{\mathbf{w},b} \frac{1}{2} ||\mathbf{w}||^2 + C \sum_{i} \max\{0, 1 - y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b)\}$$

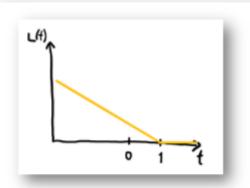
Hierzu sagt man auch **Regularisierung** – Margin Maximierung ist also Regularisierung

Anmerkung: dies ist auch gleichbedeutend mit der Minimierung der eingeführten Slack-Variablen

Was denken Sie?

Wie schaut die math. Formulierung hierzu aus?

Beispiel: SVM from Scratch: Loss Function



Was denken Sie?

Ohne es hier schon behandelt zu haben: haben Sie eine Vermutung wie man damit nun die optimalen Modellparameter findet?

Wir haben gesehen, dass man durch ein paar mathematische Umformungen zu einem übersichtlichen Optimierungsproblem bzw. einer relativ überschaubaren Kostenfunktion gelangt. Wir wollen uns nun in diesem Beispiel damit beschäftigen die Loss Function

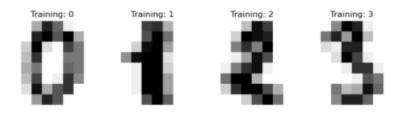
$$\min_{\mathbf{w},b} \frac{1}{2} ||\mathbf{w}||^2 + C \sum_{i} \max\{0, 1 - y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b)\}$$

als Funktion in Python abzubilden.

So what?

Nun wissen wir wie die SVM als mathematisches Modell aussieht und welche Kostenfunktion minimiert werden soll. Das Werkzeug für die Minimierung – z.B. den sog. *Gradientenabstieg* – sehen wir uns in einer späteren Veranstaltung an.

Beispiel: SVM zur Handschrifterkennung



Stellen Sie sich vor Sie müssten einem Modell aus handschriftlichen Notizen beibringen geschriebene Zahlen zu erkennen. Dieser Use Case kann Ihnen an vielen Stellen begegnen - z.B.

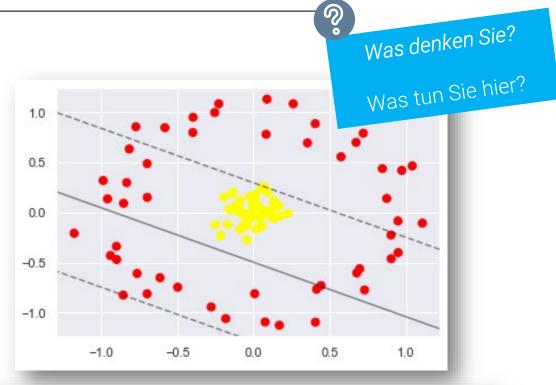
- wenn Sie als Post von Briefen die geschriebene Postleitzahl und Hausnummer digitalisieren müssten und so die Weiterverarbeitung von Briefen beschleunigen würden
- wenn in hochautomatisierten Produktionsanlagen in Bauteilen eingestanzte Seriennummern erkannt und digitalisiert werden müssen
- wenn Sie im Rahmen einer Absatzprognose Notizen von Mitarbeitern erhalten, auf denen noch Absatzzahlen handschriftlich festgehalten werden. In diesem Beispiel wollen wir eine SVM nutzen, um genau diesen Use Case zu lösen. Hierzu nutzen wir das sog. *Digits-Dataset* aus sklearn, in dem eine Vielzahl handschriftlicher Zahlen in (8, 8) großen Arrays abgespeichert sind. Unser Ziel ist es, dass die SVM so trainiert wird, dass sie **ungesehene** handschriftliche Zahlen in die richtige Klasse (die zugrundeliegende Zahl) einordnen kann. Bemerkung: wir kommen hier mit einer *Multi-Class SVM* in Berührung.

0

So what?

Hier haben wir etwas neues kennengelernt: SVMs können auch für Multi-Class-Probleme verwendet werden (sprechen wir später kurz an)

SVM: Nicht-lineare Probleme



```
from sklearn.datasets.samples_generator import make_circles
X, y = make_circles(100, factor=.1, noise=.1)

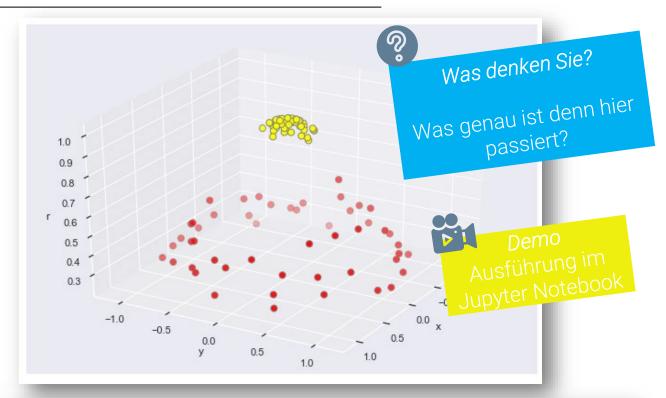
clf = SVC(kernel='linear').fit(X, y)

plt.scatter(X[:, 0], X[:, 1], c=y, s=50, cmap='autumn')
plot_svc_decision_function(clf, plot_support=False);
```

- Bei unserem Digits-Beispiel haben wir implizit angenommen, dass wir die Klassen linear – also mit einer geraden Linie – trennen können. Was passiert wenn dem nicht so ist?
- Keine lineare Hyperebene wird die beiden Klassen jemals trennen können
 → Es liegt also ein nicht-linear separierbares Problem vor
- SVMs sind in der Lage auch solche Probleme zu lösen

Lösung: Projektion der Daten in einen höherdimensionalen Raum!

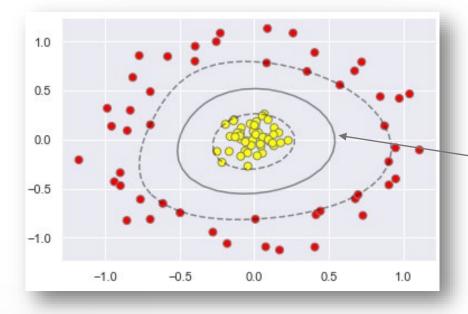
SVM: Nicht-lineare Probleme



- Eine Möglichkeit eine neue Dimension an unseren Raum hinzuzufügen ist z.B. sogenannte *Radial Basis Functions* zu verwenden
- RBFs sind skalare Funktionen $\phi(r)$, die nur vom Abstand zum Ursprung abhängen
- Dadurch machen wir also aus unserem 2D- einen 3D-Datensatz
- → Das Problem wird in einer höheren Dimension linear separierbar

SVM: Kernel-Trick





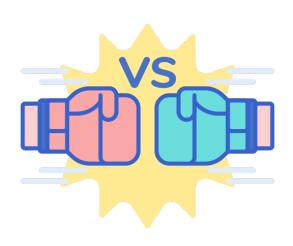
- Diese Projektion in höhere Dimensionen wird durch den sog. *Kernel-Trick* auf die Spitze getrieben
- Man kann implizit an jeden der N Datenpunkt eine zusätzliche Dimension anfügen – ohne diese Projektion wirklich durchzuführen
- In diesem *N*-dimensionalen Raum wird dann eine linear separierende Hyperebene gesucht
- Diese lineare Hyperebene im N-dimensionalen Raum wird im ursprünglichen, niedrigdimensionalen Raum zu einer nicht-linearen Hyperebene
- In sklearn wird das mittels des Hyperparameters kernel='rbf' realisiert

Multi-Class SVMs



Was denken Sie?

Sie kennen jetzt eine SVM, die zwei Klassen unterscheiden kann: wie funktioniert das bei mehreren Klassen?



- Liegen mehr als zwei Klassen vor, so lässt sic obiger Ansatz nicht eins-zu-eins anwenden
- Eine Möglichkeit mehrere Klassen zu unterscheiden ist: für jede Klassenpaarung einen Klassifikator bzw. eine SVM zu trainieren
- Diesen Ansatz nennt man "one-versus-one" im Gegensatz zu "one-versus-rest"
- Für *N* Klassen müssen dann

$$\frac{N(N-1)}{2}$$

SVMs trainiert werden

Die Entscheidungsgrenzen ergeben sich dann auder Kombination aller Klassifikatoren

Was denken Sie?

Was könnte "one-versusrest" hier bedeuten?

Was denken Sie?

Wie viele SVMs müssen dann erzeugt werden?

Vorteile, Nachteile, Besonderheiten: SVM



Pros:

- SVMs sind sehr effektiv bei h\u00f6herdimensionalen Datens\u00e4tzen
- SVMs helfen in Fällen, in denen die Anzahl der Dimensionen größer ist als die Anzahl der Datenpunkte
- SVMs sind komputativ effizient
- Pädagogisch: SVM lassen geometrische Interpretationen zu

Cons:

- SVMs haben Probleme mit sehr großen Datensätzen
- SVMs haben Probleme bei stark überlappenden Klassen bzw. viel Rauschen in den Daten
- Probabilistische Interpretation nicht möglich

Beispiel: SVM zur Face Recognition













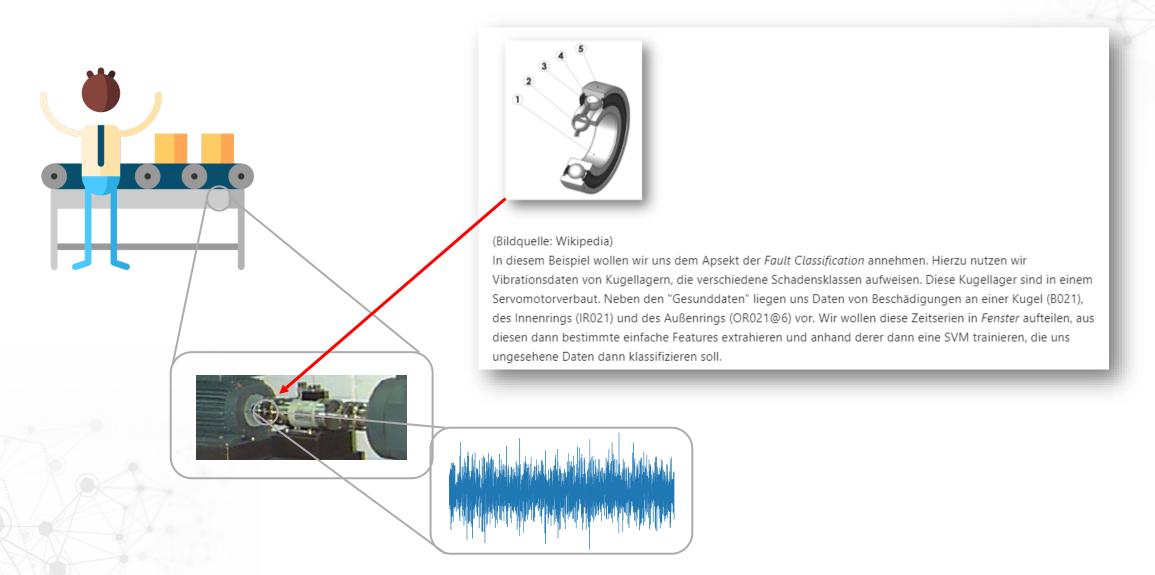


Wir wollen uns in diesem Beispiel gleich einem interessanten ANwendungsfall im maschinellen Lernen widmen: der Gesichtserkennung. Hierzu laden wir uns mittels eines sog. Fetchers aus sklearn.datasets einen Datensatz, der Bilder von Gesichtern berühmter Personen beinhaltet. Unser Ziel ist es eine SVM zu trainieren, die diese Gesichter erkennen - also klassifizieren - kann. Zu jeder Person gibt es eine Vielzahl verschiedener Aufnahmen - jede Person stellt also eine Klasse dar. Die Bilder haben die Dimensionalität (62,47) und somit ca. 3000 Pixel. Wenn jeder Pixel einer

Dimension in einem Raum entsprechen würde, dann wäre ein Gesicht ein Datenpunkt in diesem Raum. Dieser Raum ist uns zu hochdimensional. Daher *projizieren* wir die Gesichter in einen niedrigdimensionaleren Raum (wir greifen hier den Themenblock PCA vorweg).

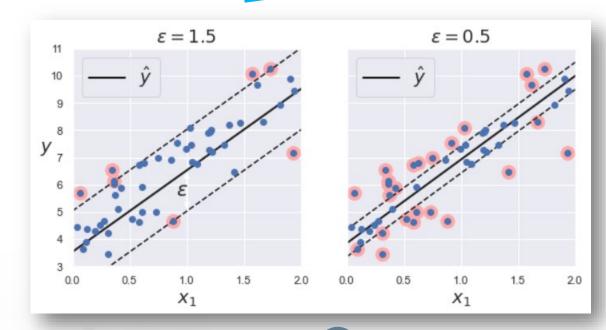
So what? Wir haben unser erstes, quantitatives Gütemaß kennengelernt: den accuracy score aus sklearn.metrics → Entspricht der gewöhnlichen Genauigkeit: wie viel Prozent der Labels im Testdatensatz wurden korrekt vorhergesagt

Beispiel: Fault Classification of Bearing Faults



SVR: Support Vector Regression

Was denken Sie?
Wieso benötigen wir
nun ein Epsilon?



Was denken Sie?

Wie könnte nun unsere Kostenfunktion aussehen? Was denken Sie?

Was ist der clevere Trick, der uns von einer Klassifikation zu einer Regression bringt?

- SVMs können auch zur Regression verwendet werden – hierzu sagt man dann Support Vector Regression
- Hierzu kehrt man unsere Optimierungsbedingung um – wir suchen nun nach einer Hyperebene plus Margin, innerhalb dessen sich so viele Datenpunkte wie möglich befinden
- Auch die Bestrafung muss hierzu umgekehrt werden: Datenpunkte außerhalb des Margins führen zu Penalties!
- Uns liegen in dieser Situation keine wirklichen Support Vectors zwischen verschiedenen Klassen mehr vor → Ein weiterer Hyperparameter € nötig, der variiert werden muss
- Die Kostenfunktion der SVR ist dann:

$$\min_{\mathbf{w},b} \frac{1}{2} ||\mathbf{w}||^2 + C \sum_{i} \max\{0, |y_i - (\langle \mathbf{w}, \mathbf{x}_i \rangle + b)| - \varepsilon\}$$

SVR: Support Vector Regression: sklearn

```
1 # Some data
  2 np.random.seed(42)
       = 2 * np.random.rand(m, 1) - 1
       = (0.2 + 0.1 * X + 0.5 * X**2 + np.random.randn(m, 1)/10).ravel()
  7 # Show
  8 plt.scatter(X, y);
0.8
0.7
0.5
0.3
0.2
0.1
   -1.00 -0.75 -0.50 -0.25 0.00
                                     0.50
```

```
    In sklearn haben wir eine entsprechende Klasse vorliegen
```

```
SVR(kernel=<kernel_type>,
C=<regularization_parameter_value>,
epsilon=<margin_width>)
```

 Auch hier gilt wieder: wir können sowohl lineare, als auch nicht-lineare Probleme lösen → der Kernel-Trick findet auch hier Anwendung

