Computational Learning Theory

Sommersemester 2018

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 3

Ausgabe: 30.04.2018
Abgabe: 07.05.2018

Die erste Aufgabe ist eine Bonusaufgabe, mit der Sie vergangenen und zukünftigen Punkteverlust in den Übungen ausgleichen können.

Bonusaufgabe 3.1. *Sauers Lemma ist scharf!* (8* Extrapunkte)

Seien $d, s \in \mathbb{N}$. Zeigen Sie, dass für jede endliche Menge X mit $|X| = s > d$ eine Konzeptklasse $\mathcal{C}$ über X mit $\mathrm{VC}(\mathcal{C}) = d$ existiert, sodass

$$\Pi_{\mathcal{C}}(s) = \sum_{i=0}^{d} \binom{s}{i}.$$

Aufgabe 3.2 *No Free Lunch für die Gleichverteilung* (2 + 4 + 4 + 2 = 12 Punkte)

Sei $n \in \mathbb{N}_{>0}$, $X = \{0,1\}^n$ ein Beispielraum und D die Gleichverteilung auf X. Wir betrachten einen deterministischen Lernalgorithmus A, der genau $s = \frac{1}{2} \cdot |X|$ Beispiele anfordert, um ein Zielkonzept über X mit der Hypothesenklasse $\mathbf{BOOLEAN}_n = \mathcal{P}(X)$ zu erlernen. In dieser Aufgabe zeigen wir, dass

$$\text{prob}\left[\text{fehler}_D(c, h_S) \geq \tfrac{1}{8}\right] \geq \tfrac{1}{8} \qquad (*)$$

für mindestens ein Konzept $c \in \mathbf{BOOLEAN}_n$ und die von A bestimmte *konsistente* Hypothese $h_S \in \mathbf{BOOLEAN}_n$ gilt.

Gehen Sie wie folgt vor: Fassen Sie den Lernalgorithmus als Funktion auf, die jede Beispielmenge auf eine konsistente Hypothese abbildet. Fixieren Sie eine beliebige Beispielmenge S mit $s = \frac{1}{2} \cdot |X|$, untersuchen Sie den erwarteten Fehler für zufällig gezogene Konzepte $c \in \mathbf{BOOLEAN}_n$ und zeigen Sie schließlich, dass A mit hoher Wahrscheinlichkeit den erwarteten Fehler macht. Insbesondere:

a) Bestimmen Sie die exakte Anzahl der mit S konsistenten Konzepte.

b) Sei D' die Gleichverteilung auf $\mathbf{BOOLEAN}_n$ und $c \in \mathbf{BOOLEAN}_n$ ein gemäß D' zufällig gezogenes Konzept. Bestimmen Sie den erwarteten Fehler $\mathbb{E}_{c \sim D'}[\text{fehler}_D(c, h_S)]$.
Hinweis: Verwenden Sie für jedes potenzielle Beispiel $x_i \in X \setminus S$ die Indikatorvariable

$$X_i = \begin{cases} 1, & \text{falls } x_i \in c \oplus h_S \\ 0, & \text{sonst.} \end{cases}$$

c) Zeigen Sie mithilfe der Chernoff-Schranke (Satz 2.36), dass es sehr unwahrscheinlich ist, dass der Lernalgorithmus stark vom erwarteten Fehler aus b) abweicht.

d) Folgern Sie schließlich die Aussage $(*)$.

Fazit: Sogar für die Gleichverteilung gibt keinen universellen Algorithmus, der jede beliebige Konzeptklasse mit konsistenten Hypothesen erlernen kann und nur wenige Beispiele anfordert. Wir müssen uns also vorab auf „vernünftige" Hypothesenklassen festlegen.

Aufgabe 3.3 *Die Grenzen des PAC-Modells* $(3+3+2=8$ Punkte)

Sei $\mathbf{INTERVALL} = \{[a,b] : a,b \in \mathbb{R},\ a \leq b\}$ die Konzeptklasse aller abgeschlossenen reellen Intervalle. Für jedes $k \in \mathbb{N}_{>0}$ definieren wir

$$\mathbf{INTERVALL}^k := \bigvee_{i=1}^{k} \mathbf{INTERVALL} = \left\{ \bigcup_{i=1}^{k} [a_i, b_i] \ : \ [a_1,b_1], \ldots, [a_k,b_k] \in \mathbf{INTERVALL} \right\}$$

als die Konzeptklasse aller Vereinigungen von höchstens k Intervallen. Schließlich sei

$$\mathbf{INTERVALL}^+ := \bigcup_{i=1}^{\infty} \mathbf{INTERVALL}^i$$

die Konzeptklasse aller Vereinigungen endlich vieler Intervalle.

a) Zeigen Sie: $\mathrm{VC}\left(\mathbf{INTERVALL}^k\right) = 2k$ für alle $k \in \mathbb{N}_{>0}$.

b) Zeigen Sie: Für alle Konzeptklassen $\mathcal{C}_1, \mathcal{C}_2$ gilt: Wenn $\mathcal{C}_1 \subseteq \mathcal{C}_2$, dann $\mathrm{VC}(\mathcal{C}_1) \leq \mathrm{VC}(\mathcal{C}_2)$.

c) Folgern Sie: Es gibt keinen PAC-Algorithmus für $\mathbf{INTERVALL}^+$.

Aufgabe 3.4 *Die Macht der Validierung: Abseits von PAC* $(2+4+6=12$ Punkte)

In der Aufgabe 3.3 mussten wir vor der Konzeptklasse $\mathbf{INTERVALL}^+$ kapitulieren. Aber müssen wir das wirklich? Nur, wenn wir uns vorher auf die Anzahl der angeforderten Beispiele festlegen müssen. Wir fordern nun iterativ eine Folge $(S_1, S_2, S_3, \ldots)$ von Mengen klassifizierter Beispiele an.

Der Lernalgorithmus A habe nach der Anforderung der Menge S_i die Hypothese h_i bestimmt. Für die *Validierung* von h_i kann der Algorithmus ein Orakel mit einem Fehlerparameter ε_i und einem Misstrauensparameter δ_i anfragen. Das Orakel gibt daraufhin eine Menge V_i klassifizierter Beispiele aus, die A benutzt, um den Fehler $\mathrm{fehler}_D(c, h_i)$ für das unbekannte Zielkonzept c zu schätzen. Ist der mittels V_i geschätzte Fehler klein, d. h. $\frac{|V_i \cap (c \oplus h_i)|}{|V_i|} \leq \varepsilon_i$, so wird die Hypothese akzeptiert, andernfalls wird sie verworfen. Die Wahrscheinlichkeit, dass eine Hypothese h_i mit $\mathrm{fehler}_D(c, h_i) > \varepsilon$ die Validierung dennoch besteht oder dass eine Hypothese h_i mit $\mathrm{fehler}_D(c, h_i) \leq \varepsilon/4$ verworfen wird, ist höchstens δ_i.

Weitere Details zum Thema Validierung werden wir zu einem späteren Zeitpunkt in der Vorlesung behandeln.

a) Sei $c \in \mathbf{INTERVALL}^k$ das unbekannte Zielkonzept. Wie viele Beispiele sind notwendig, wie viele hinreichend, um c im PAC-Sinne zu erlernen?

b) Sei nun k unbekannt. Angenommen, eine Hypothese $h_i \in \mathbf{INTERVALL}^+$ wird nach der Validierung verworfen. Wie groß sollte die Menge S_{i+1} sein?

c) Entwerfen Sie einen Lernalgorithmus, der für jede Verteilung D mit Wahrscheinlichkeit mindestens $1-\delta$ jedes unbekannte Konzept $c \in \mathbf{INTERVALL}^+$ mit Fehlerwahrscheinlichkeit höchstens ε lernt. Ihr Algorithmus sollte $\mathbf{INTERVALL}^+$ auch als Hypothesenklasse benutzen und eine konsistente Hypothese ausgeben. Wenn Ihr Algorithmus von einer Hypothese nicht „überzeugt“ ist, darf er (im Gegensatz zu PAC-Algorithmen) weitere Beispiele anfordern, eine neue Hypothese bestimmen und wieder validieren. Wie sind ε_i und δ_i für die Aufrufe des Orakels zu wählen?

   Hinweis: In dieser Aufgabe geht es nicht darum, die Größe der Menge V_i abzuschätzen, sondern die Parameter ε_i und δ_i für die Aufrufe des Orakels so zu bestimmen, dass für jede akzeptierte Hypothese h gilt:

$$\mathrm{prob}_D\left[\mathrm{fehler}_D(c,h) \leq \varepsilon\right] \geq 1-\delta.$$

   Die Chernoff-Schranke kann hier wieder hilfreich sein.