Hans U. Simon
Christoph Ries

Bochum, den 28. Mai 2018
Abgabe bis zum 05.06.2018

Übungen zur Vorlesung

# Theorie des maschinellen Lernens

Sommer 18

Übungsblatt 05

**Aufgabe 5.1** (4 Punkte)
Sei $\mathcal{H}$ die Menge aller boolschen Konjunktionen mit bis zu fünf Variablen $x_1, x_2, ..., x_5$. Bestimme für die nachfolgende Trainingsmenge $S \subseteq (\{0,1\}^5 \times \{0,1\})^7$ eine konsistente Hypothese mit Hilfe des Closure-Algorithmus.

$$\begin{aligned} S &= \{((0,1,0,1,0),0),((1,1,0,0,0),1),((1,0,1,0,1),0),((0,1,1,1,0),0), \\ &\quad ((1,1,0,0,1),1),((0,0,0,0,0),0),((1,0,0,0,1),1)\} \end{aligned}$$

**Aufgabe 5.2** (4 Punkte)
Graph 3-Colorability ist das Problem für einen gegebenen Graphen mit Knoten $V$ und Kanten $E$ eine Färbung mit maximal drei Farben zu finden, d.h. keine Kante aus $E$ verbindet zwei Knoten aus $V$ der selben Farbe. Es ist bekannt, dass dieses Problem NP-vollständig ist.

Nutze das Problem Graph 3-Colorability, um zu zeigen dass 3-Term DNF nicht PAC-lernbar ist (unter der Annahme RP $\neq$ NP).

**Aufgabe 5.3** (4 Punkte)
Das Diskrete-Quadratwurzel-Problem:
Sei $N \in \mathbb{N}$ das Produkt von zwei $n/2$-Bit Primzahlen. Sei $a$ das Quadrat eines $z \in \mathbb{Z}_N^*$. Gesucht ist nun ein $x \in \mathbb{Z}_N$ mit

$$a = x^2 \mod N.$$

a) Seien $p$ und $q$ zwei beliebige aber ungerade Primzahlen und sei $N = pq$. Setze $a = x^2 \mod N$ für ein $x \in \mathbb{Z}_N^*$. Zeige, dass ein $y \in \mathbb{Z}_N^*$ existiert mit

$$a = y^2 \mod N \qquad \wedge \qquad y \neq x \mod N \qquad \wedge \qquad y \neq -x \mod N.$$

b) Beweise: Es existiert genau dann ein effizienter Algorithmus für das Diskrete-Quadratwurzel-Problem, wenn ein effizienter Algorithmus zum Faktorisieren von Zahlen aus $\mathbb{Z}$ existiert.

— Bitte wenden! —

**Aufgabe 5.4** (4 Punkte)
Zeige, dass sich Entscheidungsbäume von Rang $k$ schwach auf $k$-Entscheidungslisten L-reduzieren lassen.

**Definition Entscheidungsbäume**
Ein Entscheidungsbaum über $X_n = \{0,1\}^n$ ist eine Funktionenklasse, in der jede Funktion durch einen binären Baum (mit einer ausgezeichneten Wurzel) gegeben ist, wobei jeder innere Knoten mit einem Literal aus $x_1, \overline{x}_1, \ldots, x_n, \overline{x}_n$ und jedes Blatt mit einem Bit beschriftet ist.
Bei der Berechnung von $f(x)$ starten wir an der Wurzel des Baumes und gehen nach rechts, falls das Literal an der Wurzel von $x$ erfüllt wird, ansonsten gehen wir nach links. In dieser Art durchlaufen wir den Baum bis wir bei einem Blatt angekommen sind. Das zu dem Blatt gehörende Bit ist die Ausgabe von $f(x)$.

**Definition Rang eines Baumes**
Sei $T$ ein binärer Baum und $T_L$, $T_R$ der linke bzw rechte Teilbaum von der Wurzel aus. Dann ist der Rang von $T$ folgendermaßen definiert:

$$\mathrm{rang}(T) := \begin{cases} 0 & \text{, falls } T \text{ nur einen Knoten enthält} \\ \mathrm{rang}(T_L) + 1 & \text{, falls } \mathrm{rang}(T_L) = \mathrm{rang}(T_R) \\ \max\{\mathrm{rang}(T_L), \mathrm{rang}(T_R)\} & \text{, sonst} \end{cases}$$