Interactive Machine Learning (iML)

Andreas Holzinger

"Computers are incredibly fast, accurate, and stupid. Human beings are incredibly slow, inaccurate, and brilliant. Together they are powerful beyond imagination."[1]

Begriffsbildung

Ursprünglich wurde der Begriff „Machine Learning" als „künstliche Generierung von Wissen aus Erfahrung …" [11] definiert. Mittlerweile ist es ein stark wachsendes und extrem breites Gebiet der Informatik mit hohem Grundlagenforschungspotenzial und vielfältigen Anwendungsmöglichkeiten. Die klassische Fragestellung lautet: „How can we build computer systems that automatically improve with experience, and what are the fundamental laws that govern all learning processes?" (Tom Mitchell, 1989). Ein Großteil der Machine Learning Community konzentriert sich daher auf automatic Machine Learning (aML), und vollautomatisierte Lernalgorithmen zeigen auch enorme praktische Erfolge, beispielsweise in der Spracherkennung genauso wie im Bereich autonomer Fahrzeuge.

Interactive Machine Learning (iML) ist dagegen ein relativ neuer Ansatz und noch kein sehr geläufiger Begriff. *Es handelt sich dabei um Algorithmen, die mit – teils menschlichen – Agenten interagieren und durch diese Interaktion ihr Lernverhalten optimieren können.*

Die Ursprünge und Grundlagen von iML basieren auf drei bekannten Ansätzen (in historischer Reihenfolge): Reinforcement Learning (1950), Preference Learning (1987) und Active Learning (1996).

Motivation

Menschen sind vielen Algorithmen häufig noch immer überlegen, beispielsweise in der instinktiven, ja nahezu instantanen Interpretation komplexer Muster. Trotz dieses offensichtlichen Befunds gibt es bis dato kaum quantitative Evaluierungsstudien über die Effektivität und Effizienz von Algorithmen, die mit – teils auch menschlichen – Agenten interagieren. Darüber hinaus gibt es auch kaum Nachweise, wie durch eine solche Interaktion das Lernverhalten von Algorithmen tatsächlich optimiert werden kann, obwohl doch solch „natürliche" intelligente Agenten in großer Zahl vorhanden sind. Eine Erklärung für die Vorherrschaft von aML-Ansätzen könnte darin begründet sein, dass aML-Ansätze besser zu evaluieren und daher auch rascher publizierbar sind als iML-Ansätze. Bei iML-Ansätzen sind methodisch korrekte Evaluationen nicht nur wesentlich komplexer und zeitaufwendiger, sondern auch sehr schwierig oder gar nicht replizierbar, da menschliche Agenten subjektiv, individuell und

[1] http://www.benshoemate.com/2008/11/30/einstein-never-said-that/

DOI 10.1007/s00287-015-0941-6

Andreas Holzinger
Medizinische Universität Graz,
Institut für Medizinische Informatik, Statistik
und Dokumentation, Research Unit HCI-KDD,
und Technische Universität Graz,
Fakultät für Informatik & Biomedizinische Technik,
Institut für Informations Systeme & Computer Medien,
Auenbruggerplatz 2/V, 8036 Graz, Österreich
E-Mail: a.holzinger@hci-kdd.org

*Vorschläge an Prof. Dr. Frank Puppe
<puppe@informatik.uni-wuerzburg.de>
oder an Dr. Brigitte Bartsch-Spörl
<brigitte@bsr-consulting.de>

Alle „Aktuellen Schlagwörter" seit 1988 finden Sie unter:
http://www.is.informatik.uni-wuerzburg.de/as

Zusammenfassung
Während Machine Learning (ML) in vielen Domänen sehr gut funktioniert, wie die Leistung selbstfahrender Autos zeigt, bergen vollautomatisierte ML-Methoden in komplexen Domänen die Gefahr der Modellierung von Artefakten. Ein Beispiel für eine komplexe Domäne ist die Biomedizin, wo wir mit hochdimensionalen, probabilistischen und unvollständigen Datenmengen konfrontiert sind. In solchen Problemstellungen kann es vorteilhaft sein, nicht auf menschliches Domänenwissen zu verzichten, sondern vielmehr menschliche Intelligenz und ML zu kombinieren.

daher *nicht kopierbar* sind – im Gegensatz zu Daten, Algorithmen und maschinellen Agenten.

In der Biologie, der Biomedizin und der klinischen Medizin stoßen aML-Anwendungen oft aufgrund der vorhandenen Komplexität an ihre Grenzen – durch den Einsatz von vollautomatischen Algorithmen entsteht die Gefahr der Modellierung von Artefakten. Hier können interaktive Methoden, zum Beispiel durch die Einbindung eines „Doctor-in-the-Loop" [6], gerade bei der Lösung harter Problemstellungen (siehe die Beispiele im nächsten Abschnitt) eine nicht unerhebliche Rolle spielen, vor allem in Kombination mit einer großen Anzahl menschlicher Agenten (Crowdsourcing). Beispielsweise können Ärzte oft mit großer Zuverlässigkeit Diagnosen stellen, ohne die Regeln ihrer Vorgehensweise explizit angeben zu können. Hier könnte iML helfen, Algorithmen mit solch „instinktivem" Wissen auszustatten und daraus zu lernen. Die Wichtigkeit von iML wird auch deutlich, wenn der Einsatz automatisierter Lösungen aufgrund der Unvollständigkeit von Ontologien schwierig wird [1]. Vergrößert wird in Zukunft diese Problematik durch den steigenden Trend zur personalisierten Medizin [4] und einem damit unweigerlichen Ansteigen der Komplexität der anfallenden Datenmengen.

Allerdings verlangt der Einsatz von iML-Ansätzen auch ein umfangreiches Verständnis des Datenökosystems, die innovative Verknüpfung heterogener Datenmengen, skalierbare Entwicklungsmethoden und statistische Modellierungstechniken, sowie ein Verständnis visueller Analyse und Visualisierung.

Anwendungsfälle für iML

Beispiel 1: Anonymisierung von Patientendaten

Das Problem der k-Anonymisierung ist einerseits NP-schwer, andererseits kann die Qualität des erzielten Resultats zwar an den gegebenen Faktoren (k-Anonymität, l-Diversität, t-Closeness, delta-presence) gemessen, jedoch nicht im Hinblick auf die tatsächliche Sicherheit der Daten, also die Re-Identifizierbarkeit durch einen Angreifer, überprüft werden. Dazu sind gewisse Annahmen über das Hintergrundwissen des hypothetischen Gegners zu treffen, was im Hinblick auf das jeweilige demografische und kulturelle klinische Umfeld am besten durch menschliche Agenten erfolgt. Somit stellt das Problem der (k-)Anonymisierung ein natürliches Feld für iML dar.

Beispiel 2: Subspace Clustering

Häufig unterliegen Clustering-Verfahren anderen Systemen, beispielsweise als Eingrenzung der Möglichkeiten von Recommendern (z. B. Tag-Recommender bei YouTube-Videos) oder zur „Category Discovery" (z. B. fold.it – ein experimentelles Computerspiel, das Crowdsourcing zur Entdeckung neuer Proteinstrukturen nützt, was ein schweres Problem darstellt). Dabei stellt sich das Problem subjektiver Ähnlichkeitsfunktionen: Beispielsweise würde ein Mechaniker wahrscheinlich die Menge in einem Verkaufsraum ausgestellter Fahrzeuge anders gruppieren als eine Mutter kleiner Kinder (Hubraum versus Stauraum). Dieses Problem ist auch als „Subspace Clustering" bekannt, da zur Gruppierung – je nach subjektiver Sichtweise – verschiedene Eigenschaften eines Objektes herangezogen werden können (in obigem Beispiel eben Hubraum vs. Stauraum). Was Benutzern dabei als Komfort individualisierter Systeme erscheint, kann im wissenschaftlichen Umfeld zur interaktiven Exploration hochdimensionaler Datensätze erweitert werden [10], was wiederum enorme Vorteile für die Anwendung im Umfeld schwerer biomedizinischer Problemstellungen bieten kann [5].

Beispiel 3: Multi-Armed Bandit (MAB)

Ein weiteres iML-relevantes Beispiel sind Multi-armed Bandits. In sogenannten „Spielautomatentests" werden menschliche Agenten

(Crowdsourcing) eingebunden, wobei mehrere „einarmige Banditen“ (Spielautomaten) mit unterschiedlichen Auszahlungsmethoden analysiert werden. Es soll jener Spielautomat ermittelt werden, der über die beste Auszahlungsrate verfügt, aber gleichzeitig sollen die Gewinne maximiert werden. Dabei werden zum einen Automaten berücksichtigt, die in der Vergangenheit hohe Gewinne erbracht haben, und zum anderen neue oder scheinbar schlechtere Automaten, die möglicherweise noch bessere Gewinne erbringen könnten [13]. Im Prinzip modellieren MABs also Agenten, die gleichzeitig versuchen, neue Kenntnisse zu erwerben („Exploration“) und ihre Entscheidungen auf der Grundlage der vorhandenen Kenntnisse zu optimieren („Verwertung“). Die Agenten versuchen diese konkurrierenden Aufgaben auszugleichen, um den Gesamtwert über die Zeit betrachtet zu maximieren. Es gibt interessante praktische MAB-Anwendungen: Klinische Studien in der evidenzbasierten Medizin mit dem Ziel, Medikamente und/oder Behandlungsmethoden und/oder medizinische Interventionen/Therapien zu testen; oder Portfolio Optimierung in der Finanzanalyse. Das einfachste Beispiel stellen Content Tests dar (um herauszufinden, welche Elemente einer Webseite die Nutzer positiv beeinflussen), wo z. B. Google, Microsoft, Yahoo, Facebook, Amazon u. a. andauernd mehrere Funktionsvarianten testen. Anfangs werden noch alle Varianten (z. B. fünf verschiedene Layouts) gleichgewichtet bei verschiedenen Nutzern angezeigt. Sieht man nun anhand von statistischen Daten, dass Variante 1 und 3 besonders gut funktionieren, werden diese beiden häufiger und die anderen drei Varianten seltener gezeigt, bis letztlich nur mehr eine Variante übrig bleibt, welche dann meistens übernommen wird.

Diese Beispiele sollen zeigen, dass menschliche Erfahrung helfen kann, einen Suchraum exponentieller Möglichkeiten durch heuristische Auswahl von Proben drastisch zu reduzieren und dadurch NP-schwere Probleme effizient (oder zumindest für menschliche Akteure akzeptabel) anzunähern.

Menschen erweisen sich nämlich als besonders geschickt im explorativen Erlernen von Mustern anhand weniger Beispiele, während das klassische supervised ML meist sehr große Mengen an Trainingsdaten und sehr lange Trainingszeit benötigt. Bei manchen Problemstellungen, beispielsweise bei seltenen Erkrankungen in der Medizin oder Fehlfunktionen von Menschen bzw. Maschinen, stehen nämlich nur wenige Trainingsdaten zur Verfügung. Darüber hinaus ist gerade in der klinischen Medizin die Zeit ein ganz wesentlicher Faktor – wo Ergebnisse quasi in Echtzeit oder zumindest in sehr kurzer Zeit notwendig sind (z. B. in der Intensiv- bzw. Notfallmedizin). Seltene Krankheiten sind nämlich oft lebensbedrohend und erfordern rasche Intervention – die geringe Datenlage macht aber aML-Ansätze praktisch unmöglich. Ein Beispiel für eine solche seltene Krankheit mit wenig verfügbaren Daten ist CADASIL (Cerebral Autosomal Dominant Arteriopathy with Subcortical Infarcts and Leukoencephalopathy), eine Krankheit, die mit rund 5 Fällen pro 100.000 Menschen die häufigste monogen vererbte Schlaganfallerkrankung in Deutschland darstellt.

Gerade in der Erstaufnahme bei Blickdiagnosen haben menschliche Agenten den Vorteil, die Gesamtsituation sehr rasch „auf einen Blick“ zu erkennen. Diese Eigenschaft ergibt sich aus der Fähigkeit zum Wissenstransfer von einer Situation zur nächsten, wobei Modellparameter, einmal erlernte Eigenschaften oder kontextuelles Wissen übertragen werden (können). Zwei letzte „real world“-Beispiele sollen dies verdeutlichen: ein bisher unbekanntes Objekt aus ungewöhnlichem Winkel dank seiner Anordnung als Auto zu identifizieren (Eigenschaften) oder ein Flutlicht nicht mit der Sonne zu verwechseln, wenn die Szene ein Fußballspiel zeigt.

Die genannten Beispiele zeigen, dass der Einsatz von iML-Ansätzen in „real world“-Situationen von Vorteil sein kann. Im Beispiel des „contextual Bandit“ wird – im Gegensatz zu vielen statistischen Verfahren – die Unabhängigkeit von Stichproben unnötig; sogar aus der direkten Interaktion mit einem Agenten („Gegner“) können nützliche Schlussfolgerungen zur Problemlösung gezogen werden.

Ursprünge und Grundlagen

Grundlagen für iML stellen drei Ansätze dar: Reinforcement Learning, Preference Learning und Active Learning, insbesondere Active Preference Learning; diese drei Ansätze können im Folgenden nur ganz kurz vorgestellt werden. Wichtig dabei ist, dass bei iML-Ansätzen die Agenten sowohl

menschlicher als auch maschineller Natur sein können.

Reinforcement Learning (RL)

Das Verstärkungslernen ist bis heute weit verbreitet, wurde von Turing 1950 [14] diskutiert und basiert auf neuropsychologischen Grundlagen, bei der ein Agent den Nutzen (Utility) von Aktionen in (s)einer Umgebung bestimmt. RL unterscheidet sich von supervised ML durch das Fehlen einer umfangreichen Benennung von Trainingsbeispielen; stattdessen erfährt der Lerner erst nach individuellen Entscheidungen eine Belohnung (Reward) vonseiten der Umgebung.

RL wird auch das Problem „künstlicher Intelligenz im Mikrokosmos“ genannt, weil Lernalgorithmen autonom agieren müssen, um ihre Ziele mit hinreichender Genauigkeit zu erreichen. Nicht zuletzt durch die Verfügbarkeit immer größerer Datenmengen konnte RL in den letzten Jahren große Fortschritte in der Fähigkeit zur Generalisierung, Planung, Wissensentdeckung (Knowledge Discovery) und auch der empirischen Methodologie selbst verzeichnen. Diese Forschungserfolge erhöhen die praktische Einsatzfähigkeit solcher Methoden in der Wirtschaft [7].

Um RL erfolgreich in komplexen Situationen, wie sie in der Biomedizin vorkommen, anwenden zu können, sehen sich Agentensysteme einigen Schwierigkeiten gegenüber: So müssen aus der Vielzahl hochdimensionaler Daten effiziente Repräsentationen abgeleitet werden, um Muster aus der Vergangenheit auf neue Situationen (Transfer Learning) anzuwenden. Das menschliche Gehirn scheint diese Aufgabe durch eine Mischung aus RL und hierarchischer Sensoranalyse zu lösen. Auf Ersteres weisen neuronale Daten hin, welche erhebliche Parallelen zwischen Signalen „dopaminerger“ – also auf Dopamin reagierender – Neuronen und zeitintervallbasiertem RL offenbaren. Bisher war diese Methode auf vollständig beobachtbare, niedrigdimensionale Daten beschränkt, in denen Parameter manuell gesetzt werden konnten. Heute wird Deep Learning zur Entwicklung autonomer Agentensysteme benutzt – im Sinne von aML; dieser „deep Q-Network“ genannte Ansatz optimiert die Erwartung zukünftiger Belohnungen mittels RL in einem Markov Decision Process, um erfolgreiche Handlungsrichtlinien direkt aus hochdimensionalen Daten ohne vollständiges Labeling abzuleiten [9]. Dabei kommunizieren diese Agenten bei jedem Schritt mit einem „allwissenden Orakel“. Genau dieses könnte jetzt im Sinne des iML auch durch einen (oder im Crowdsourcing: viele) menschliche(n) Agenten dargestellt bzw. zu einem Multi-Agent-Hybrid-System ergänzt werden, um in Anwendungsfeldern des iML schwere Problemstellungen zu lösen.

Preference Learning (PL)

Eine wichtige Motivation für einen präferenzbasierten Ansatz ist die Beobachtung, dass in vielen realen Domänen numerische Feedbacksignale nicht oder nur ungenügend verfügbar sind; daraus ergibt sich der Anreiz zu selektionsbasiertem RL. Ein Beispiel ist ein Modell, das einem Agenten qualitative Feedbacksignale zur Verfügung stellt. Ein solches Framework (Beispiel in [3]) kann als Generalisierung von RL gesehen werden, wobei es zur Entscheidungsfindung kurzfristig auf partielle Handlungsrichtlinien zurückgreift, ohne auf vollständige Information durch langfristige Feedbackerwartung angewiesen zu sein. Das Ziel besteht darin, RL-Agenten durch qualitative Feedbacksignale in die Lage zu versetzen, selbstständig eine Rangfolge möglicher Vorgehensweisen nach voraussichtlichem Erfolg zu erstellen und dadurch (semi-)autonom handeln zu können.

Active Preference Learning (APL)

In der Psychologie und Ökonometrie hat der Einsatz von Wahrscheinlichkeitsmodellen (Random Utility Models) eine lange Tradition und geht auf Thurstone [12] zurück.

Beispielsweise kann man Menschen M Paare von Informationsobjekten zeigen und anschließend diese nach ihren Präferenzen fragen. Daraus ergibt sich eine Menge von geordneten Paaren $\mathcal{D} = \{r_k \succ s_k; k = 1, \ldots, M\}$ (das Symbol $\succ$ bezeichnet die Präferenz von r über s). Die N Elemente der Trainingsdaten werden als $x_{1:N} = \{x_1, x_2, \ldots, x_N\}$ mit $x_i \in X \subseteq \mathbb{R}$ bezeichnet, das heißt also, r_k und s_k entsprechen zwei Elementen aus dem Vektor $x_{1:N}$. Das Ziel ist es nun, die Elemente x mit der höchsten menschlichen Präferenz – mit so wenig Vergleichen wie möglich – zu berechnen [2]. Ein solcher Ansatz kann beispielsweise verwendet werden, um das Suchverhalten von menschlichen Agenten zu erlernen [15] – auch hier könnte es vielfältige

Anwendungsmöglichkeiten für eine personalisierte Expertensuche in der Medizin geben.

Offene Fragen und zukünftige Herausforderungen

iML ist noch wenig etabliert und relativ wenig erforscht. Daher finden sich noch viele offene Fragestellungen und Evaluierungsaufgaben, die direkt mit fundamentalen Problemen der Informatik zusammenhängen, welche viel Raum zu weiterer Forschungsarbeit bieten und auch erfordern.

Machine Learning wird allgemein als Vorstufe zur künstlichen Intelligenz betrachtet. Ungeachtet des aktuellen Reifegrades dieser Technologien werden Agenten „echter Intelligenz" notwendigerweise mit ihrer Umwelt interagieren und daraus Lehren ziehen müssen. Grundlegende Einsichten in effiziente Herangehensweisen an iML bieten daher auch langfristig vielversprechende Anwendungsmöglichkeiten.

Im Verlauf der Etablierung von iML wird es notwendig, die traditionelle ML-Definition von einer „Black-Box"-Strategie zu einer „Glass-Box"-Strategie zu erweitern und dem Feature-Learning höhere Bedeutung zukommen zu lassen: Features sind ein Schlüssel zu Lernen und Verstehen. Auch eine Kombination von Domain-Ontologien mit iML-Ansätzen scheint vielversprechend, um beispielsweise durch strukturierte Metainformationen nicht nur Nicht-ML-Experten die Benutzung komplexer Algorithmen zu erlauben, sondern auch zu ermöglichen, dass die Algorithmen von den Domain-Experten, den menschlichen Agenten, lernen können.

Eines der Ziele maschinellen Lernens besteht im Entdecken unerwarteter Muster („unknown unknowns"). Dies könnte allerdings zu einem Problem bei der Involvierung menschlicher Agenten führen, da diese in der Interaktion mit einem Lernalgorithmus bereits bekannte Muster bevorzugen und somit verstärken. Mit anderen Worten kann menschliches Mitwirken ein Overfitting nicht an Labels von Trainingsdaten, sondern an ihren eigenen Erwartungen sowie Erfahrungen verursachen. Dies kann zwar in manchen Fällen gewünscht sein (subjektive Ähnlichkeiten), muss in Fällen reiner Wissensentdeckung aber vermieden werden [8].

Ein Vorschlag zur Kompensation besteht darin, die latenten Vorurteile des Benutzers während der Interaktion zu analysieren; ob und wie erfolgreich dies umsetzbar ist, stellt jedoch in sich ein iML-Experiment dar.

Danksagung

Der Autor dankt den anonymen Begutachtern dieser Arbeit für ihre Kommentare und Hinweise.

Literatur

1. Atzmüller M, Baumeister J, Puppe F (2006) Introspective Subgroup Analysis for Interactive Knowledge Refinement FLAIRS Nineteenth International Florida Artificial Intelligence Research Society Conference. AAIS press, pp 402–407
2. Brochu E, Freitas ND, Ghosh A (2007) Active Preference Learning with Discrete Choice Data. In: Platt JC, Koller D, Singer Y, Roweis ST (eds) Advances in Neural Information Processing Systems 20, NIPS 2007, pp 409–416
3. Fürnkranz J, Hüllermeier E, Cheng W, Park SH (2012) Preference-based reinforcement learning: a formal framework and a policy iteration algorithm. Machine Learning 89(1–2):123–156
4. Holzinger A (2014) Trends in Interactive Knowledge Discovery for Personalized Medicine: Cognitive Science meets Machine Learning. IEEE Intell Inform Bull 15(1):6–14
5. Hund M, Sturm W, Schreck T, Ullrich T, Keim D, Majnaric L, Holzinger A (2015) Analysis of Patient Groups and Immunization Results Based on Subspace Clustering. In: Guo Y, Friston K, Aldo F, Hill S, Peng H (eds) Brain Informatics and Health, Lecture Notes in Artificial Intelligence LNAI 9250. Springer, Heidelberg, pp 358–368
6. Kieseberg P, Schantl J, Frühwirt P, Weippl E, Holzinger A (2015) Witnesses for the Doctor in the Loop. In: Guo Y, Friston K, Aldo F, Hill S, Peng H (eds) Brain Informatics and Health, Lecture Notes in Artificial Intelligence LNAI 9250. Springer, Heidelberg, pp 369–378
7. Littman ML (2015) Reinforcement learning improves behaviour from evaluative feedback. Nature 521(7553):445–451
8. Miettinen P (2014) Interactive Data Mining Considered Harmful (If Done Wrong). ACM SIGKDD Workshop on Interactive Data Exploration and Analytics, pp 85–87
9. Mnih V, Kavukcuoglu K, Silver D, Rusu AA, Veness J, Bellemare MG, Graves A, Riedmiller M, Fidjeland AK, Ostrovski G, Petersen S, Beattie C, Sadik A, Antonoglou I, King H, Kumaran D, Wierstra D, Legg S, Hassabis D (2015) Human-level control through deep reinforcement learning. Nature 518(7540):529–533
10. Müller E, Assent I, Krieger R, Jansen T, Seidl T (2008) Morpheus: Interactive Exploration of Subspace Clustering. Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp 1089–1092
11. Samuel AL (1959) Some studies in machine learning using the game of checkers. IBM J Res Dev 3(3):210–229
12. Thurstone LL (1927) A law of comparative judgment. Psychol Rev 34(4):273–286
13. Tran-Thanh L, Stein S, Rogers A, Jennings NR (2014) Efficient crowdsourcing of unknown experts using bounded multi-armed bandits. Artif Intell 214:89–111
14. Turing AM (1950) Computing machinery and intelligence. Mind 59(236):433–460
15. Yue Y, Joachims T (2009) Interactively Optimizing Information Retrieval Systems as a Dueling Bandits Problem. Proceedings of the 26th Annual International Conference on Machine Learning (ICML), pp 1201–1208