

readme

Bulletin der UZH Alumni Informatik | Ausgabe 45 / 2021



Kalender

April – Dezember 2021

SO 18.04.

Alumni Geburtstagsbrunch
Juckerfarm, Seegräben

DI 04.05.

IfI-Vortrag von Dan Olteanu

DO 27.05.

Führung Lewa Savanne Zürich Zoo
Anschliessend Apéro, Alex Rübel (neuer
Präsident UZH Alumni) als Special Guest

DO 10.06.

Business Lunch
Outdoor

MO 23.08.

Wanderung auf den Uetliberg
Weg nach Schwierigkeitsgrad und
Grill am Ziel Uetliberg

FR 24.09.

**Alumni Sommernachtsparty
mit Special Show Act**
Mitglieder mit Partner*in
Mit Outdoormöglichkeit

DI 02.11.

Alumni Generalversammlung
ZHAW

MO 15.11.

Goldwyn Partners Group Workshop
«Executive Videotraining – Bewerbung
und Rekrutierung in Echtzeit üben!»
Europaallee 41, 8021 Zürich

DI 07.12.

Fondue Plausch
Mitglieder mit Partner*in
Sorell Hotel Zürichberg,
Orellistrasse 21, 8044 Zürich

Betreffend Kosten und Zeiten informieren wir euch noch per E-Mail und/oder auf unserer Website. Aufgrund der aktuellen Lage rund um das Coronavirus kann es zu kurzfristigen Änderungen kommen, die wir ebenfalls per E-Mail oder auf der Website kommunizieren werden. Herzlichen Dank für euer Verständnis!

Inhalt

Kalender 02

Editorial
Christian Schneider 03

Vorstellung Marc-André Pradervand
Marc-André Pradervand 03

Aus dem Präsidium
Dr. Brigitte Bailer 04

Neues aus dem IfI
Prof. Dr. Renato Pajarola 05

Deep Learning – Fluch und Segen
Prof. Dr. Manuel Günther 08

Skalierungsgesetze von künstlichen neuronalen Netzwerken
Marc Stampfli 11

Big Data und Deep Learning: Rechtliche Stolpersteine
Roland Mathys, Dr. Samuel Klaus und Claudia Jung 14

Geburtstagsbrunch
Marcel Bühler 16

Sommernachtsparty
David Habegger 18

Cyber Security in der RS
Dr. Brigitte Bailer 18

Unsere Sponsoren und Partner 19

Impressum 19

Editorial

Von Christian Schneider

Liebe Alumni

Noch lebhaft kann ich mich an einen Kurs aus meinem Master in Wirtschaftsinformatik erinnern, den ich als freies Wahlmodul bei den Kollegen aus der Computer Linguistik belegt habe. Nebst Maschineller Übersetzung aus einer Sprache in eine andere, wurden dort Aspekte des Deep Learning als technischen Ansatz für die Maschinelle Übersetzung angeschnitten. Von den vielseitigen Einsatzgebieten des Deep Learning, die weit über die Computer Linguistik hinausreichen, war ich beeindruckt. Umso mehr freut es mich, dass wir für dieses readme drei Experten aus Academia und Praxis gewinnen konnten, die aus unterschiedlichen Domänen über ihre Erkenntnisse und Erfahrungen mit Deep Learning – Chancen und Risiken – berichten.

Auch für mich, einen jungen Alumnus, ist dies eine Thematik mit viel Neuheitsgehalt. Euch, liebe Community, erwarten Beiträge von Prof. Dr. Manuel Günther, der uns aufzeigt, wo Deep Learning ein Enabler sein kann und wo Vorsicht geboten ist, Marc Stampfli, der über Skalierungsgesetze von künstlichen neuronalen Netzwerken berichtet. Einen juristischen Blick auf die Thematik geben uns Roland Mathys, Dr. Samuel Klaus und Claudia Jung.

Dieses readme ist die erste Ausgabe, die ich redaktionell begleiten darf. Gerne möchte ich deshalb die Gelegenheit nutzen, um mich vorzustellen: Mein Name ist Christian Schneider. 2018 habe ich als einer der letzten Studierenden in der Studienordnung 2006 meinen Master in Wirtschaftsinformatik abgeschlossen. Mit Begeisterung habe ich Ende 2020 die Vakanz im Vorstand des Alumni Informatik (Ressort readme) übernommen. Beruflich bin ich in der Parametrierung und im Solution Design im Financial Service Bereich tätig. Ich freue mich, mit euch in Kontakt zu bleiben, und wünsche euch gute Lektüre.

Mit besten Grüßen aus der readme Redaktion
Christian



Christian Schneider

ist seit 2020 bei der LGT Bank als Business IT Specialist tätig. Dort arbeitet er in der Parametrierung der Core Banking Plattform. Er hat mehrere Jahre Erfahrung als IT Consultant mit den Schwerpunkten Solution Design, Implementierung und Test Engineering. Christian schloss 2018 seinen Master in Wirtschaftsinformatik an der Universität Zürich ab und übernahm 2020 die Redaktion des readme im Alumni Informatik.

► christian.schneider@alumni.ch

Vorstellung Marc-André Pradervand

Von Marc-André Pradervand

Seit der Generalversammlung im vergangenen November darf ich als neues Vorstandsmitglied unsere Alumni-Organisation unterstützen. Als ich von unserer Präsidentin Brigitte Bailer, mit der ich schon während meiner Dissertation bei Professor Bauknecht in der gleichen Forschungsgruppe am Institut für Informatik engagiert war, für die Aufgabe angefragt wurde, war dies für mich nicht einfach eine Anfrage nach einer (weiteren) ehrenamtlichen Tätigkeit. Da ich schon bei der Gründungsversammlung unserer Alumni im Jahr 1997 dabei sein durfte, war und ist diese Aufgabe für mich vor allem eine Herzensangelegenheit.

Mein beruflicher Weg hat mich in den letzten 20 Jahren von der klassischen Wirtschaftsinformatiker-Karriere in die Non-Profit-Welt geführt, wo ich zwar auch immer wieder in Informatik-Projekte involviert bin, mich aber vor allem mit Fundraising und Sponsoring für gemeinnützige Zwecke beschäftige. Dies einerseits als Berater und Interim-Manager und andererseits auch als Referent und Dozent. Und so freut es mich besonders, unseren Vorstand im Bereich Sponsorenmanagement zu ergänzen, damit wir weiterhin genügend Firmenpartner und Sponsoren finden, um unseren bald 800 Alumni-Mitgliedern attraktive Angebote bieten zu können.



Dr. Marc-André Pradervand

hat 1995 als Doktorand am Institut für Informatik promoviert. Nach diversen Stationen in der Privatwirtschaft ist er seit über 20 Jahren in der Non-Profit-Welt tätig, einerseits als Interim-Manager und andererseits als Berater für Fundraising und CRM-Systeme. Seit dem Herbst 2020 ist er im Vorstand der UZH Alumni Informatik für das Ressort Sponsorenmanagement zuständig.

► marc.pradervand@alumni.ch

Aus dem Präsidium

Von Dr. Brigitte Bailer

Liebe Alumna, Lieber Alumnus

Du hältst eine Kurzversion des neuen readme in den Händen. Oder bist du gleich in die Online-Ausgabe eingetaucht? Wie auch immer, unser readme 45/2021 feiert in zweifacher Hinsicht Premiere:

Erstens wurde es erstmals nach 14 Jahren von unserem neuen Vorstandsmitglied Christian Schneider organisiert, redigiert und verantwortet. Christian hat damit die Nachfolge von Kornel definitiv angetreten. Ihr werdet nach dem Sichten des neuen readme mit mir einig sein: Es ist ihm hervorragend gelungen. Das neue readme präsentiert sich im frischen Design der Jubiläumsausgabe des letzten Jahres, die Inhalte sind hochaktuell, interdisziplinär und zeigen das hohe Niveau unserer Ausbildung und was man daraus machen kann. Parallel dazu kommt auch der Einblick in unser Vereinsleben nicht zu kurz.

Die zweite Neuerung betrifft die Form der Publikation. Erreichen wir unsere Mitglieder, wenn wir nur noch eine Email mit dem Hinweis auf die Online-Version versenden? Oder braucht es noch einen Eyecatcher? Wir haben uns als Pilot für einen Eyecatcher mit vier Schnupperseiten in gedruckter Form entschieden. Auf der Titelseite findest du den QR-Code mit Link zur Onlineversion - einfach ein- und weiterlesen.

Und was gibt es sonst zu berichten?

Ein Rückblick auf das letzte Jahr muss sein. Wir alle wissen es: Es war ein schwieriges Jahr. Für viele vielleicht das anspruchsvollste ihres bisherigen Lebens. Unsere Alumni konnte doch 60% der Anlässe wie geplant durchführen. Unsere Eventmanager*in aus dem Vorstand haben das mit ihrem grossem Einsatz ermöglicht. Wir haben euch dazu gelungene Review-Beiträge in diesem readme zusammengetragen.

Ein wichtiger Moment war sicher die Wahl unserer beiden neuen Vorstandsmitglieder anlässlich der schriftlich durchgeführten GV 2020. Neben Christian Schneider ist auch Marc-André Prader vand zu uns gestossen – ein Voll-Profi in Sachen Sponsoring. Beide lernt ihr in diesem readme besser kennen. Anja Cavigilli ihrerseits hat das Aktuariat übernommen.

Auch für das laufende Jahr haben wir uns auf volatile Zeiten eingestellt. Unsere Devise für die wärmere Jahreszeit wird aber nicht «UZH Alumni Informatik goes Online», sondern «UZH Alumni Informatik goes Outdoor» lauten. Alle unsere Events von April bis Oktober sind «Outdoor» angelegt. Davor sind wir Online, danach sehen wir weiter. Sobald wir also wieder physisch dürfen, legen wir draussen los. Schau dir also die Agenda genau durch, es ist wieder für jede*n etwas dabei.

Und zum Schluss noch dies: Unsere Studierenden haben es in Homeoffice-Zeiten nicht immer leicht, Kontakte herzustellen und ihren Platz zu finden. Ein gutes Netzwerk kann da Halt bieten. Der UZH Alumni Informatik bittet euch deshalb: Wenn ihr in eurer Umgebung eine Möglichkeit für ein Praktikum seht, meldet euch beim Ifl oder bei unserem Ifl-Vorstandsmitglied Nathan Labhart.

Herzliche Grüsse
Eure Präsidentin
Brigitte



Dr. Brigitte Bailer

Dr. Brigitte Bailer ist Mitinhaberin und Geschäftsleiterin der Basec Software AG. Sie berät seit vielen Jahren Unternehmen in der Gestaltung ihrer Wertschöpfungskette unter optimalem Einsatz der Informatik, ist aktuell Verwaltungsrätin der Enea-Gruppe für Landschaftsarchitektur und Stiftungsrätin bei der Swiss Life. Seit 2018 präsidiert sie den UZH Alumni Informatik
► brigitte.bailer@alumni.ch

Neues aus dem IfI

Von Prof. Dr. Renato Pajarola

Liebe Alumnae, liebe Alumni

Wir sind so ins Frühlingsemester 2021 gestartet, wie wir das letzte Herbstsemester beendet haben: nämlich digital und online. Weiterhin heisst es, geduldig bleiben. Jedoch konnte ich in den letzten Monaten beobachten, wie sich Dozierende und Studierende rapide auf die veränderten Umstände einstellten. Darum bin ich sehr zuversichtlich bezüglich der zukünftigen Lehre und Forschung am IfI.

Gemeinsames Feiern hingegen ist schwierig, in physischer Form weiterhin unmöglich. Unser 50-jähriges Jubiläum hatten wir wegen der Corona-Pandemie von Herbst 2020 auf Frühling 2021 verschoben. Anstatt euch nun auf ein neues Datum zu vertragen, möchte ich nur dies ankündigen: gefeiert wird später!

Unsere traditionelle IfI-Weihnachtsfeier wurde ganz untraditionell in Zoom durchgeführt, wobei nach den üblichen Ansprachen einige Aktivitäten angeboten wurden wie Buchdiskussionen oder das «Great IfI Pub Quiz», welches für viele Lacher sorgte. Auch fürs leibliche Wohl wurde gesorgt: Wer sich zur Weihnachtsfeier anmeldete, konnte sich Essen nach Hause liefern lassen.

Dass wir in der digitalen Lehre gut unterwegs sind, zeigt unter anderem die UZH-Würdigung der «Teachers of the Hour», die wir am IfI gleich dreifach erhielten. Im November 2020 konnten Studierende jene Dozierende nominieren, die kreative Wege gefunden hatten, trotz Distanz Interaktion herzustellen oder die einen ausserordentlichen Einsatz für ihre Studierenden zeigten.

Michael Böhlen, Sven Seuken und ich selber wurden als «Teachers of the Hour» ausgezeichnet.

Wir freuen uns sehr, dass Prof. Dr. Alberto Bacchelli im Oktober 2020 zum ausserordentlichen Professor ad personam für Empirical Software Engineering ernannt wurde (<https://www.ifi.uzh.ch/en/zest/team/bacchelli.html>). Nur ein paar Monate zuvor war er mit dem «Ric Holt Early Career Achievement Award» ausgezeichnet worden. Dieser Award würdigt Nachwuchsforschende, die in der Anfangsphase ihrer Karriere herausragende Beiträge auf dem Gebiet von «Mining Software Repositories» geleistet haben.

Auch erfreulich ist, dass wir am IfI zwei neue Assistenzprofessuren besetzen konnten. Seit Juli 2020 ist Prof. Dr. Manuel Günther Assistenzprofessor für Künstliche Intelligenz und Maschinelles Lernen (www.ifi.uzh.ch/en/aiml/people/guenther.html) und seit September 2020 ist Prof. Dr. Jürgen Bernard Assistenzprofessor für Interacting with Data (www.ifi.uzh.ch/en/ivda/team/bernard.html).

Diese Ernennungen werden bestimmt einen positiven Einfluss haben auf die Weiterentwicklung unseres Instituts. Da wir uns in nächster Zeit weiterhin virtuell begegnen, wäre es schön, wenn ihr von Zeit zu Zeit auf Social Media reinschaut! Oder folgt uns auf Facebook und Instagram. Bleibt gesund!

Mit besten Wünschen
Euer Renato Pajarola



Prof. Dr. Renato Pajarola

Renato Pajarola studierte an der ETH Zürich Informatik und absolvierte dort auch sein Doktorat, welches er 1998 abschloss. Anschliessend war er für ein Jahr Postdoc am Georgia Institute of Technology und ab 1999 Assistenzprofessor an der University of California Irvine. Seit 2005 ist er Professor am Institut für Informatik an der Universität Zürich, wo er seit dem 1. August nun auch Institutsdirektor ist. Renato Pajarolas Forschungsinteressen liegen in den Bereichen Visual Computing, 3D Computergrafik, interaktive Datenvisualisierung und Geometry Processing.

► pajarola@ifi.uzh.ch





Big Data und Deep Learning: Chancen und Risiken

08 | Deep Learning – Fluch und Segen
*Enabler für intelligente Produkte,
aber Vorsicht vor blindem Vertrauen*

Von Manuel Günther

**11 | Skalierungsgesetze von künstlichen
neuronalen Netzwerken**
*Mehr Daten, grössere Modelle, neuere
Architekturen, bessere Resultate*

Von Marc Stampfli

**14 | Big Data und Deep Learning:
Rechtliche Stolpersteine**
Vertrauen, Normen und Haftung

Von Roland Mathys, Samuel Klaus, Claudia Jung

Deep Learning – Fluch und Segen

Von Prof. Dr. Manuel Günther

Die Entwicklung neuer Technologien ist in den letzten Jahren rasant angestiegen. Dies ist nicht zuletzt dem Deep Learning zuzuschreiben, welches es ermöglicht, riesige Datenmengen automatisch zu analysieren und eigene Schlüsse zu ziehen. Doch obwohl das Deep Learning riesige Sprünge in der Wissenschaft erlaubt und auch einige neue Applikationen für den Endbenutzer basierend auf Deep Learning entwickelt wurden, gibt es einige Risiken des Deep Learning, die ich in diesem Artikel zusammenfassen möchte.

Einsatz von Regelwerken

Doch bevor wir uns den Chancen und Risiken des Deep Learning widmen, möchte ich einen kurzen Überblick über traditionelle Herangehensweisen erläutern. Erste Ansätze zur Automatisierung von einigen Anwendungsgebieten basierten auf Regelwerken. Ein Beispiel einer solchen Anwendung ist die automatische Vereinfachung mathematischer Gleichungen, dessen Regelwerk auf mathematischen Gesetzen beruht. Mithilfe dieses Regelwerkes ist es möglich, auch komplexere Gleichungen zu analysieren und bei der Beweisführung zu helfen. Solche Systeme sind auch heutzutage noch im Einsatz, allerdings sind die Anwendungsgebiete sehr spezifisch.

Automatische Lernverfahren

Ein vollkommen anderer Ansatz zur Automatisierung ist das Lernen von Regeln aus Beispielen. Als ein Anwendungsfall wäre die automatische Übersetzung von Texten aus einer Sprache in eine andere zu sehen. Durch die hohe Komplexität einzelner Sprachen sind regelbasierte Verfahren zum Scheitern verurteilt, da es unmöglich ist, jeden Spezialfall mit einer Regel abzubilden. Daher ist es nötig, andere Verfahren zu entwickeln, die dies ermöglichen. Automatische Lernverfahren, besser bekannt unter dem Namen «Künstliche Intelligenz» oder dem Englischen «Artificial Intelligence (AI)», besitzen die Möglichkeit, selbständig Informationen und auch Handlungsanweisungen aus Daten zu extrahieren.

Traditionell besteht ein solches Lernverfahren aus zwei verschiedenen Komponenten. Als erstens werden bestimmte Merkmale aus den Daten extrahiert, die möglichst viele relevante Informationen beinhalten, während nicht relevante Informationen ausgeschlossen werden. In der automatischen Gesichtserkennung zum Beispiel werden zuerst das Gesicht und einige Landmarken wie Nase, Mund, Augen etc. im Gesicht detektiert (meist auch durch beispiel-basierte Lernverfahren).

Nur an diesen Landmarken werden Informationen aus dem Bild extrahiert, nicht jedoch aus dem Hintergrund oder den Haaren, welche sich als zu schwierig herausgestellt hatten. Als zweite Komponente wird ein Verfahren entwickelt, das anhand der extrahierten Merkmale höhere Informationen extrahiert, in unserem Beispiel, ob die Person im Bild gerade lächelt, oder welche Person in dem Bild zu sehen ist. Diese Verfahren verwenden meist statistische Informationen, die sie aus einer Menge von Beispielbildern extrahiert haben, welche vorher präzise gelabelt sein müssen. Das Problem mit diesen traditionellen Zwei-Komponenten-Verfahren ist, dass die zu extrahierenden Merkmale meist nur auf wenigen Anwendungsgebieten erfolgreich sind, und die Lernverfahren speziell auf die verwendeten Merkmale abgestimmt sein müssen. Des Weiteren können diese statistischen Verfahren nur auf einer begrenzten Anzahl von Beispielen trainiert werden. Allerdings gibt es seit einigen Jahren eine riesige verfügbare digitale Datenmenge, die nur darauf wartet, analysiert zu werden.

Deep Learning und seine Chancen

Das einzige momentan bekannte Lernverfahren, dass grundsätzlich mit solch riesigen Datenmengen arbeiten kann, ist das Deep Learning. Beim Deep Learning wird (in den meisten Fällen) auf die separate Extraktion von Merkmalen aus den Rohdaten verzichtet. Stattdessen lernt das Verfahren, die höheren Informationen direkt aus den Eingabedaten zu extrahieren. Dies spart nicht nur den Aufwand, sich für jedes Problem die geeigneten Merkmale zu definieren, es funktioniert auch noch viel besser. Seitdem im Jahre 2014 das erste Deep-Learning-Verfahren alle anderen bekannten Verfahren in den Schatten gestellt hatte, indem es die ILSVRC gewann, hält der Boom des Deep Learnings an. Die Entwicklung von open-source Deep Learning Frameworks und der dazu benötigten Hardware, die Weiterentwicklung immer tieferen Lernens und die Bereitstellung von immer mehr Daten ermöglichen es heutzutage, Ergebnisse zu erzielen, von denen man vor 10 Jahren noch nicht einmal zu träumen gewagt hat. Und durch die universelle Handhabung hat Deep Learning in so ziemlich jedes Gebiet der Wissenschaft Einzug gehalten -- regelmäßige Leser der Readme werden in den letzten Ausgaben schon mehrere Artikel gefunden haben, in denen Deep Learning in verschiedensten Gebieten eingesetzt wurden. Weiterhin wurden viele täglich verwendete Applikationen entwickelt, wie zum Beispiel intelligente Lautsprecher, die auf Sprachbefehle reagieren, personalisierte

Empfehlungen von Inhalten, oder auch das Entsperren des Smartphones mit dem Gesicht, um nur einige wenige Anwendungsgebiete zu nennen.

Vorsicht beim Einsatz von Deep Learning

Doch ist Vorsicht geboten. Während Wissenschaftler die traditionellen Lernverfahren noch bis ins Detail verstanden haben, ist dies beim Deep Learning nicht mehr der Fall. Als Experte weiss ich zwar, wie ein solches Deep Learning Verfahren zu trainieren ist, aber auch ich habe keine Ahnung, was genau dieses Verfahren lernt. Durch die Komplexität der verwendeten Modelle ist eine Analyse sehr schwer bis unmöglich. Daher verwundert es nicht, dass die Deep-Learning-Verfahren, sowie auch andere statistische Lernverfahren, einige Schwächen haben, die erst nach und nach zu Tage treten.

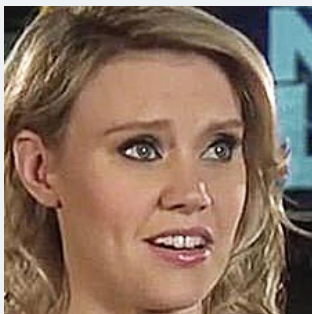
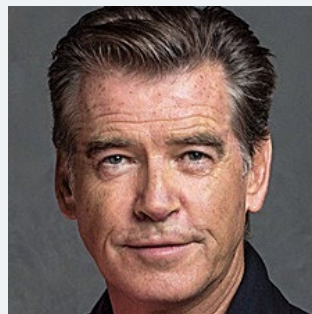
Eine Schwäche von Deep Learning ist die Existenz von sogenannten «adversarial samples». Dies sind Testbeispiele, die nur minimal verändert wurden, und trotzdem eine falsche Reaktion des Deep-Learning-Systems hervorrufen. Wenn wir bei dem Beispiel der Bildklassifikation (ILSVRC) bleiben, wird ein

korrekt klassifiziertes Bild gezielt, aber für das menschliche Auge unsichtbar, manipuliert, um eine falsche Klassifikation hervorzurufen. Neue Verfahren der Manipulation können selbst die Klasse bestimmen, die das Verfahren klassifizieren soll, sodass man zum Beispiel auch Gesichtserkennungssysteme attackieren kann (siehe Abbildung 1). Es wurde letztsens auch gezeigt, dass es möglich ist, die Reaktion autonomer Fahrzeuge zu manipulieren, indem Schilder am Strassenrand aufgestellt werden, die für den menschlichen Betrachter wie Werbeplakate aussehen.

Ein weiteres Problem maschineller Lernverfahren sind systematische Fehler in den Trainingsdaten, die sich auf die Anwendung auswirken können. Zum Beispiel ging durch die Medien, dass Amazon eine Software entwickelt hatte, die grundsätzlich alle weiblichen Bewerber abgelehnt hatte, die sich bei Technologiefirmen beworben hatten, nur weil die meisten erfolgreichen Bewerber Männer waren. Ein anderes Beispiel wäre, dass die Bank jemandem Kredite verweigert, weil ein Deep-Learning-Verfahren gelernt hat, dass Menschen aus einem gewissen Stadtteil häufiger dazu neigen, Kredite nicht zurück zu bezahlen.



Abbildung 1:
8 der 9 Bilder sind so manipuliert, dass ein Deep-Learning-Verfahren sie für die 9. Person hält. Schon erraten, welche? Das Originalbild ist unten links, alle anderen Gesichter sind für das attackierte Deep-Learning-Verfahren ähnlich genug, um ein Smartphone zu entsperren. Für das menschliche Auge sind die attackierten Bilder kaum von ihren Originalen zu unterscheiden, nur wenige, naturnahe Fältchen sind hinzugekommen.



Das Problem hierbei besteht darin, dass am Ende nur die Entscheidung des Deep-Learning-Verfahrens steht, man aber nicht mehr nachvollziehen kann, welche Gründe zu dieser falschen Entscheidung geführt haben.

Unbekannte Eingaben

Eine Schwachstelle von Deep Learning, die ich mit meiner Forschung versuche, etwas deutlicher in den Vordergrund zu stellen, ist die Behandlung von unbekannten Eingaben. Nehmen wir einmal an, ein Deep-Learning-System hat gelernt, Pferde von Kühen und Hunden zu unterscheiden. Doch was passiert, wenn man dem System nun eine Bild eines Elefanten vorlegt? Momentan hat ein solches System nur drei verschiedene Antwortmöglichkeiten, von denen aber keine richtig ist (Siehe Abbildung 2). Die korrekte Antwort wäre «Ich weiss es nicht». Erste Ansätze zeigen zwar, dass eine solche Entscheidung möglich ist, auch wenn das System noch nie Beispiele von dieser unbekannten Klasse gesehen hat. Aber bis zur Marktreife ist es noch ein weiter Weg.

Zum Schluss sollte sich jeder Mensch, der maschinelle Lernverfahren einsetzt, bewusst sein, dass diese Verfahren noch nicht ausgereift sind und Fehler machen können, die man als Mensch nicht machen würde. Es wurde von Fällen berichtet, dass amerikanische Polizisten eine Frau mit vorgehaltener Waffe aus dem Auto gezwungen haben, nur weil die Software zur Erkennung des Nummernschildes einen Fehler gemacht hat. Auch wurde berichtet, dass eine Person inhaftiert wurde, weil ein automatisches Gesichtserkennungssystem eine Person aus einer Verbrecherdatenbank wiedererkannt zu haben schien. Jedoch sahen sich die beiden Personen nicht einmal ähnlich, sodass eine sorgfältigere Prüfung eine Inhaftierung hätte verhindern können.

Fazit

Deep-Learning-Verfahren haben die Wissenschaft revolutioniert und bringen ungeahnte Möglichkeiten, aber mit dem Nachteil, dass man autonom getroffene Entscheidungen nicht mehr nachvollziehen kann. Daher sollten bis auf Weiteres keine komplett autonom handelnden Maschinen ungeprüft eingesetzt werden, sondern Deep Learning sollte nur als Unterstützung für den Menschen angesehen werden.



Prof. Dr. Manuel Günther

ist seit Juli 2020 Assistenzprofessor für Artificial Intelligence und Machine Learning am Institut für Informatik. Dort leitet er die gleichnamige Forschungsgruppe, die sich insbesondere mit drei Themenbereichen auseinandersetzt: Automatische Gesichtserkennung, Adversarial Examples und der Frage, wie ein

Klassifikator zu einer Aussage «ich weiss nicht» trainiert werden kann. Manuel Günther studierte Informatik mit Nebenfach Mathematik an der TU Ilmenau. Schon in seiner Diplomarbeit im Jahre 2004 befasste er sich mit der Gesichtserkennung, ein Thema, das ihn bis heute nicht wieder losgelassen hat. Seine Doktorarbeit fertigte er bis 2011 an der Ruhr-Universität Bochum an. Von 2012 bis 2015 war er Postdoc am Idiap Research Institute, Martigny, wo er unter anderem an der Open-Source Bibliothek «Bob» arbeitete. Danach fand man ihn als Associate Researcher an der University of Colorado Colorado Springs, wo er sich unter anderem in das Thema der Open-Set Klassifikation und der Adversarial Examples vertiefte. Nach einer kurzen Episode in der Industrie, genauer gesagt in der trinamiX GmbH Ludwigshafen, hat er den Ruf als Assistenzprofessor an der Universität Zürich angenommen.

► guenther@ifi.uzh.ch

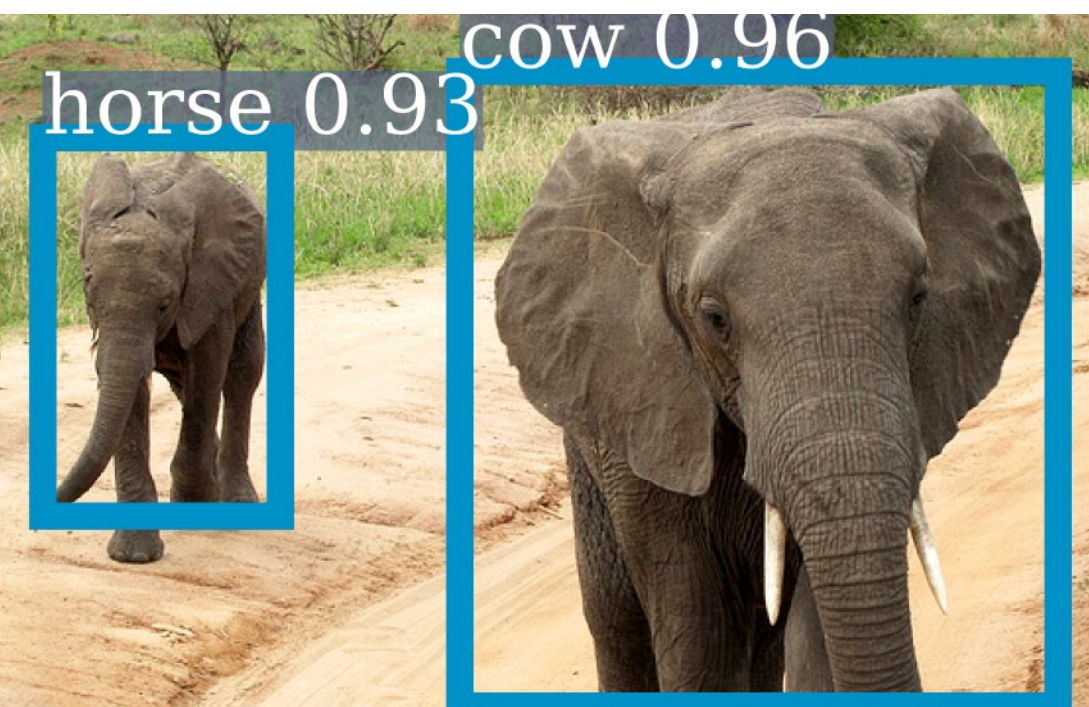


Abbildung 2:

Ein Deep-Learning-Verfahren ist darauf trainiert, 20 verschiedene Objekte wie Pferde und Kühe zu detektieren und zu benennen, allerdings keine Elefanten. Wenn man nun trotzdem ein Bild zweier Elefanten zeigt, werden sie zwar richtig detektiert, aber falsch benannt, und dies mit sehr hoher Konfidenz. Den Algorithmen die richtige Antwort: «Ich weiss nicht» beizubringen, ist einer von Manuels Forschungszweigen.



Skalierungsgesetze von künstlichen neuronalen Netzwerken

Von Marc Stampfli

Beitrag 11

Mehr Daten, grössere Modelle, neuere Architekturen, bessere Resultate

Daten, mehr Daten – «Big Data»

Viele Firmen, welche moderne künstliche Intelligenz mit Deep Learning zum ersten Mal einzusetzen, versuchen, die Verwendung von grossen Datensätzen zu vermeiden. Man versucht meist, zuerst die Datenqualität zu verbessern, zu strukturieren und erwartet damit, die Datensätze minimieren zu können. Als nächstes wird dann das komplexe Problem, das ein neuronales Netzwerk lösen soll, so vereinfacht, dass zwar ein Resultat erreicht wird, dieses jedoch nicht mehr dem ursprünglichen Ziel entspricht oder man gibt sich mit minimaler Genauigkeit der zu lösenden Aufgabe zufrieden.

Kürzlich war ich bei einem Finanzkunden, der gerade mit neuen Deep Learning Modellen für Risikoberechnungen experimentiert. Aufgrund der Erfahrung mit ähnlichen Kunden war mir bewusst, dass dazu sehr grosse Datensätze, sprich «Big Data» und grosse Modelle benötigt werden, um genaue Resultate zu erhalten. Beim ersten Gespräch wurde mir jedoch vom Verantwortlichen versichert, dass alle ihre Probleme nur «Small Data» benötigen. Erst beim Workshop mit den Datenwissenschaftlern

konnte ich die Situation klären. Es konnten nur weniger als 7% der Datenmengen verwendet werden, da sonst die grossen Datenmengen schlicht nicht verarbeitet werden konnten. Also hat man das Modell verkleinert und die Anforderungen einfach an die zu geringe Datenmenge angepasst, sodass es vermeintlich genügte. Dieses Datenparadox finde ich bei den meisten Firmen, welche mit Deep Learning beginnen.

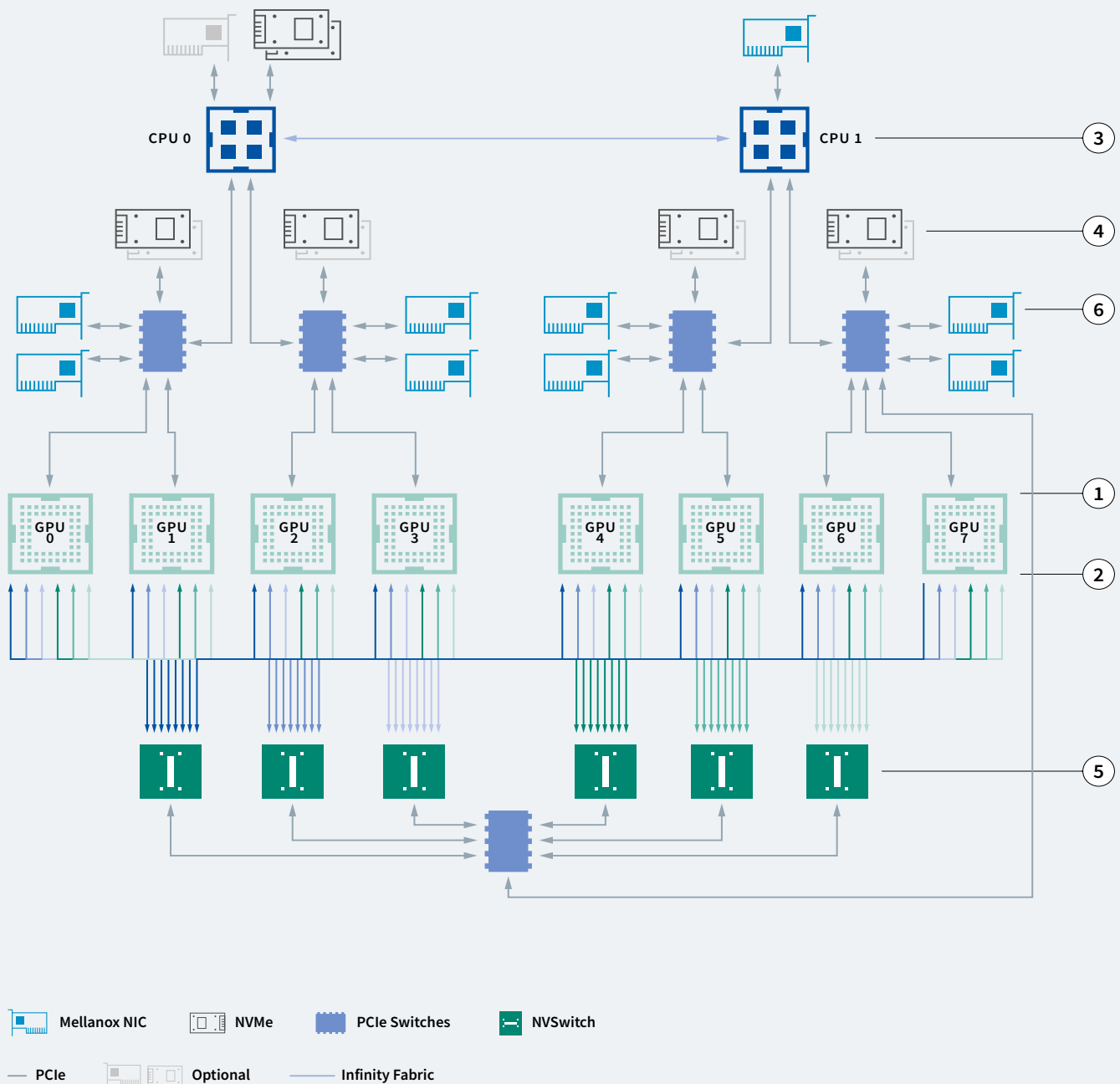
Wissenschaftlich ist es jedoch erwiesen, dass mehr Daten und grössere neuronale Netzwerk Modelle bessere Resultate liefern¹, da kein oder ein sehr später Plateau-Effekt entsteht, im Gegensatz zu vielen reinen mathematischen Methoden. Der Grund: Grosse neuronale Netzwerke nutzen die grossen Datenmengen effizienter². Je mehr Daten verfügbar, «Big Data», desto grössere Modelle müssen eingesetzt werden, um effizient zu sein.

Die besten Modelle für NLP³ (Bert-Large, Megatron-LM, GPT3), Computer Vision⁴ (BiT-M-ResNet152x4) und Recommendation⁵ Systemen (Bert4Rec) sind inzwischen sehr gross, aber bezüglich Resultate auch hervorragend geworden.

Mehr Hardware, nicht einfach mehr Performance

Sobald man akzeptiert hat, dass für eine entsprechende Genauigkeit eines neuronalen Netzwerkes genügend Datensätze und moderne grosse neuronale Netzwerke benötigt werden,

Referenzarchitektur NVIDIA DGX A100 Server



versuchen Firmen oft, das Problem mit bestehender Hardware zu lösen. Doch eigentlich handelt es sich um ein High-Performance-Computing (HPC) Problem. Zur effizienten Verarbeitung wird eine komplett andere Hard- und Softwarearchitektur benötigt als viele Firmen im Rechenzentrum haben oder an vielen Universitäten traditionell gelehrt wird.

Oft behilft man sich dann damit, dass mehrere günstige GPU Karten gekauft werden, welche man in einen bestehenden Server einbaut. Und es funktioniert vermeintlich, die Software scheint ja zu laufen, aber irgendwie doch nicht so richtig. Denn die Performance für das Training und Inferencing des neuronalen Netz-

werkes sollte doch viel höher sein bei so vielen GPU Karten. Dieses Hardware-Paradox trifft ich leider viel zu oft an.

Für Deep Learning Systeme sind andere Architekturen erforderlich als man sie sonst kennt, und mehr Karten bringen ohne entsprechende balancierte Architektur nicht einfach mehr Leistung. Der Grund ist einfach: Jedes neuronale Netzwerk mit mehr als 1,3 Milliarden Parametern passt nicht in einen einzigen GPU (selbst einer mit 32 GB Speicher). Somit muss das Modell selbst parallelisiert oder in Teile zerlegt und über mehrere GPUs verteilt werden. Dies erfordert Anpassungen an die Architektur, um überhaupt effizient zu sein.

Neue Hard- und Softwarearchitektur bringen Performance für Deep Learning

Beim Trainieren eines neuronalen Netzwerkes werden vor allem Vektoroperationen verwendet, welche parallelisiert werden können. Ausserdem müssen zwischen den verschiedenen GPUs aufgrund begrenztem VRAM pro GPU die Gradienten und Aktivierungen ausgetauscht werden. Dies ist bei traditionellen Architekturen schlicht nicht effizient umsetzbar. Ausserdem gibt es weitere Flaschenhälse wie CPU, RAM, Festplattenspeicher und Netzwerk.

Folgende Punkte zeigen eine Referenzarchitektur auf, welche die oben besprochenen Probleme löst und die Performance für neuronale Netzwerke optimiert (vgl. graphisches Architektur Schema):

- 1 GPU Parallelprozessor, welcher Vektoroperationen massiv parallelisiert ausführen kann (Tensor Cores)
- 2 Hoch performantes, möglichst grosser VRAM mit sehr hoher Memorybandbreite für den Datendurchsatz zwischen den GPUs, aber auch direkt zum Festspeicher (HBM2e, 80 Gb).
- 3 Hoch performante CPUs, um die GPUs mit der Datenverarbeitung auszulasten und keine Wartezeiten aufgrund der CPU zu erzeugen (AMD Epyc 772).
- 4 Dedizierte Speichertechnologie (NVME), um den hohen Datenbedarf und das Zugriffsmuster beim Trainieren und Ausführen von neuronalen Netzwerken optimal zu unterstützen unter Umgehung des CPUs und RAMs (GPU Direct Storage).
- 5 Bei mehreren GPUs braucht es einen Leistungsstarken Bus (NVSwitch), der es ermöglicht, Gradienten und Aktivierungen mit minimaler Latenz zwischen den GPUs auszutauschen ohne Einsatz von PCIe. Der PCIe Bus ist zu langsam und schnell überlastet. Das ist einer der Gründe, warum das einfache Hinzufügen einer zusätzlichen GPU Karte nicht skaliert.
- 6 Bei Multi-Node Training braucht es ein Netzwerkverbindung mit möglichst hoher Bandbreite und tiefer Latenz, sowie direktem Zugriff auf den GPU unter Umgehung der CPU. (200 Gb/s HDR Infiniband, GPU Direct RDMA)

Doch damit sind erst die Hardwaregrundlagen für ein optimiertes System für Deep Learning gelegt. Immerhin, ein solches System skaliert fast linear über mehrere Nodes hinweg, benötigt aber noch entsprechende Softwareunterstützung.

Für die Kommunikation zwischen den GPUs wird eine Softwareschnittstelle benötigt, welche Multi-GPU- und Multi-Node-Kommunikationsprimitive implementiert, die für GPUs und -Netzwerke optimiert sind (NCCL). Dies erlaubt die effiziente Kommunikation zwischen den GPUs und das VRAM kann transparent als ein grosser Speicher angesehen werden. Bei der obigen Referenzarchitektur wären es 640 Gb pro Node (8x80 Gb VRAM), welche für grosse neuronale Netzwerkmodelle und grosse Datensätze benutzt werden können - beliebig skalierbar über mehrere Nodes.

Der letzte Schritt ist die Implementierung einer optimierten Softwareschnittstelle für die bekanntesten und zukünftigen Deep Learning Frameworks wie PyTorch, MXNet, Tensorflow, Keras, etc., welche die mathematischen Operationen durch GPU Operationen ersetzt (CUDA, CUDNN). Eine sorgfältige Softwareoptimierung bringt neben Hardwarebeschleunigung eine zusätzliche Verbesserung um den Faktor 3-10x.

Ein optimiertes System zu entwickeln, welche grosse Datenmengen für Deep Learning verarbeiten kann, ist keine einfache Aufgabe, aber heute effizient und ökonomisch lösbar. Es braucht dazu keine traditionellen Supercomputer mehr. Anhand der Referenzarchitektur wurde aufgezeigt, wo Ansatzpunkte sind für die Optimierung, getrieben durch die aktuellen Entwicklungen für grössere neuronale Netzwerke.

Sollte dennoch jemand an die Grenzen des Machbaren mit Deep Learning und «Big Data» vorstossen, so bin ich überzeugt, man kann Vieles mit intelligenten Hard- und Softwarearchitektonischen Ansätzen lösen. Ich würde mich freuen, davon zu hören.



Marc Stampfli

Marc Stampfli arbeitete nach seinem Studiumabschluss bei Technologiefirmen wie Oracle, IBM, Colt Technologie Services und NVIDIA. Seit 2017 ist er bei NVIDIA verantwortlich für das Schweizer Geschäft. Der Hauptfokus liegt dabei auf High Performance Computing, künstliche Intelligenz (Machine Learning/Deep Learning) und Grafikbeschleunigung.
► mstampfli@nvidia.com

¹ Hestness, J., Narang, S., Ardalani, N., Diamos, G., Jun, H., Kianinejad, H., ... & Zhou, Y. (2017). Deep Learning Scaling is Predictable, Empirically. arXiv preprint arXiv:1712.00409.

² Shoenybi, M., Patwary, M., Puri, R., LeGresley, P., Casper, J., & Catanzaro, B. (2019). Megatron lm : Training multi billion parameter language models using gpu model parallelism. arXiv preprint arXiv:1909.08053

³ Kaplan, J., McCandlish, S., Henighan, T., Brown, T. B., Chess, B., Child, R., ... & Amodei, D. (2020). Scaling Laws for Neural Language Models. arXivpreprint arXiv:2001.08361.

⁴ Big Transfer (BiT): General Visual Representation Learning

⁵ Sun, F., Liu, J., Wu, J., Pei, C., Lin, X., Ou, W., & Jiang, P. (2019, November). BERT4Rec: Sequential recommendation with bidirectional encoder representations from transformer. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management (pp. 1441-1450).



Big Data und Deep Learning: Rechtliche Stolpersteine

Von Roland Mathys, Dr. Samuel Klaus und Claudia Jung

Deep Learning – und damit Künstliche Intelligenz (KI) – setzt Big Data voraus: Nur wenn ein Algorithmus bzw. ein neuronales Netz von Algorithmen mit genügend vorbestehenden Daten trainiert und parametrisiert wird, kann dieses erfolgreich für einen bestimmten Zweck eingesetzt werden. Bei Big Data stellt sich unabhängig vom Inhalt der Daten die Frage nach dem Berechtigten: Wer darf was mit diesen Daten machen? Enthält eine Datensammlung zudem Personendaten, so sind die datenschutzrechtlichen Vorgaben zu beachten.

Ist die KI-Anwendung erfolgreich parametrisiert, so können damit kognitive Fähigkeiten simuliert und letztlich Entscheide getroffen werden. Wieviel Vertrauen aber haben Anwender in solche automatisierten Entscheide – und wer haftet für fehlerhafte Ergebnisse?

Kein Big Data ohne Daten

An Daten gibt es kein Eigentum, aber vertragliche Rechte. Diese sind entscheidend dafür, was mit einer Big Data Datensammlung gemacht werden darf. Werden solche Datensammlungen somit nicht selbst erstellt, sondern von Dritten bezogen (z.B. unter einer Lizenz), so muss darauf geachtet werden, dass man sich die nötigen Rechte einräumen lässt. Das gleiche gilt – wenn auch mit umgekehrten Vorzeichen – wenn man eigene Datenbestände kommerzialisieren will: Hier ist darauf zu achten, dass man einem Abnehmer nicht mehr Rechte an diesen Daten einräumt, als nötig – und sich allfällige spätere Verwendungen dieser Daten für eigene Zwecke freihält.

Big Data, KI und Datenschutz

Sind bei Big Data nicht nur technische oder faktische Daten (Sachdaten) betroffen, sondern Daten, die sich auf bestimmte oder bestimmbar Personen beziehen (Personendaten), so sind nebst vertraglichen Rechten auch die datenschutzrechtlichen Vorgaben zu beachten: Wer anderen Personendaten liefert, muss sicherstellen, dass dies die Rechte der betroffenen Personen nicht verletzt; und wer Personendaten verwendet, muss sicher sein (und sich absichern), dass er dies für den fraglichen Zweck auch darf.

Der Datenschutz verhindert KI-Anwendungen keineswegs, stellt aber hohe Anforderungen an sämtliche Beteiligten: Wer Personendaten sammelt und zusammenstellt, muss dies transparent tun und Betroffene entsprechend informieren. Wer Personendaten anderen zur Verfügung stellt, darf dies nur im Einklang mit den Betroffenen. Und wer mittels KI aufgrund von Personendaten automatisierte Einzelentscheidungen fällt, muss unter dem neuen Datenschutzgesetz (voraussichtlich ab 2022) in gewissen Fällen die Betroffenen informieren, ihnen Gelegenheit geben, den eigenen Standpunkt darzulegen, und die automatisiert getroffene Entscheidung allenfalls von einem Mensch überprüfen lassen.

Vertrauen, Normen und Haftung

KI-Anwendungen auf Basis von Big Data und Deep Learning setzen rein statistische Auswahlmethoden in Entscheidungen um. Vielen Anwendern fehlt (zurzeit) aber noch das Vertrauen in solche rein maschinellen Entscheidungen. Durch Normen und

Standards soll hier Vertrauenswürdigkeit geschaffen werden. So sind die Internationale Organisation für Normung (ISO), das US National Institute of Standards and Technology (NIST) wie auch das Deutsche Institut für Normung (DIN) daran, Spezifikationen und Qualitätsmodelle für KI-Systeme zu entwickeln. Langfristiges Ziel ist, eine Zertifizierung von KI-Systemen zu erlauben, ähnlich wie dies heute mit einem ISO-9001-Zertifikat für das Qualitätsmanagement in einem Unternehmen möglich ist.

Auch Qualitätsstandards können Fehler und Schäden nicht gänzlich verhindern. Die Frage ist dann, wer dafür haftet. Für ein KI-System haftet das einsetzende Unternehmen – wie für jedes andere eingesetzte Hilfsmittel. Unter Umständen kann es aber Rückgriff nehmen, falls das Deep Learning durch Dritte (mangelhaft) ausgeführt wurde oder auf ungeeigneten (oder ungenügend aufbereiteten) Daten beruhte, die durch Dritte geliefert wurden. Ob ein solcher Rückgriff möglich ist, entscheidet sich aufgrund der Verträge mit diesen Dritten. Ein Unternehmen, das KI-Systeme auf Grundlage von Big Data und Deep Learning einsetzt, sollte sich deshalb entlang seiner Lieferkette für solche KI-Komponenten absichern.



Roland Mathys, LL.M. (LSE)

Roland Mathys ist Partner und Leiter von Schellenberg Wittmers Information and Communication (ICT) and Data Law Group.

► roland.mathys@swlegal.ch



Dr. Samuel Klaus, LL.M. (Berkeley)

Samuel Klaus ist Partner in der ICT / Data Law Group mit Fokus auf Digitalisierung und neue Technologien.

► samuel.klaus@swlegal.ch



Claudia Jung

Claudia Jung ist Associate in der ICT / Data Law Group mit Fokus auf Datenschutzrecht, insbesondere im Finanzbereich.

► claudia.jung@swlegal.ch

Geburtstags-brunch

Von Marcel Bühler

Man könnte meinen, ein «Geburtstagsbrunch» sei ein ruhiger, festlicher Anlass, ohne tückische Gefahren. Dies ist jedoch weit gefehlt. Wenn du wissen möchtest, was an einem regnerischen August-Tag alles geschehen kann, dann lies weiter.

Zu Beginn schien alles wie immer. Wir wurden von Esther und Brigitte herzlich begrüsst und schon bald wurden die ersten Platten aufgetragen: frisches Brot und Gipfeli, Joghurt, Früchte, Lachs, Käse. Alles war vorhanden und es schien alles friedlich und sicher. Wer hätte gedacht, dass wir bereits nach kurzer Zeit im Urwald um unser Überleben kämpfen mussten?

Hindernis-Parcour mit Krokodilen

Nachdem sich die ersten Leckereien etwas gesetzt hatten, begann die Survival-Challenge, aka das Plauschturnier. Dafür bildeten wir Teams von 4–6 Teilnehmern, die zu allem bereit waren. Zu unser aller Entsetzen wurde uns mitgeteilt, das sei heute der «Gummistiefel-Brunch», und deshalb solle man sich a) warm und b) wasserfest anziehen. Von wegen ein friedlicher Sonntagmorgen Brunch! Das schien eher eine Art Bootcamp zu werden.

In der Tat war bereits bei der ersten Aufgabe höchste Konzentration und extreme Balance gefordert: ein Ei sollte möglichst schnell durch einen Hindernis-Parcours transportiert werden. Nun ja, anstatt durch Wasserfälle und 100 Meter tiefe Schluchten bewegten wir uns auf dem Tennisfeld und anstatt um Krokodile rannten wir um Slalomstangen. Aber hey, die Fantasie macht ja auch mit.

Als ob wir bei der ersten Aufgabe nicht schon genug geschwitzt hätten, kam die zweite wie ein Hammerschlag. Es ging darum, auf kleinen, holzigen Pedalos zu fahren und so den Urwald, bzw. das Tennis-Feld, zu überqueren. Es fehlte nicht viel, und wir hätten dabei ein Teammitglied an wilde Tiere verloren. Aber dank unserem unschlagbaren Team-Spirit überstanden wir diese Challenge.

Aliens erobern Zürich

Danach war höchste Präzision gefragt. Wann hast du das letzte Mal einen Fussball passgenau in der oberen linken Ecke eines Tores platziert? Wie sieht es mit deinen Hockey-Skills aus? Wir schlugen uns leidlich und konnten den Ball zumindest beim Hockey einmal versenken. Danke, Herbert! Nachdem wir über die Hälfte des anspruchsvollen Parcours geschafft hatten, ging es nach draussen in die Wildnis. Es stürmte wild und der Wind drohte, sogar die dicksten Bäume auszureissen. Wir blieben trotzdem draussen, mutig unter dem Dach, und schossen auf wilde Aliens, die den Kanton Zürich erobern wollten. Damit sind natürlich Blechbüchsen gemeint.





Knack die Nuss

Der letzte Posten war der unbestritten schwierigste, gefährlichste und lauteste. Stell dir vor, du bist in der tiefsten Wildnis, der Regen prasselt und du hast schon seit drei Tagen und Nächten nicht das Geringste gegessen. In diesem Stadium siehst du nun einen Baum mit Nüssen, deine letzte Hoffnung!

Du schüttelst den Baum und die Nüsse fallen durch ein komplexes System von teilweise durchsichtigen Röhren. Am unteren Ende war ein Loch, in dem die Nüsse auf Nimmerwiedersehen verschwanden. Die einzige Chance, eine Nuss zu treffen (und damit sich vom Verhungern zu retten), war das Knacken der Nuss in der Bewegung mit einem Hammer. Wir versuchten alles, aber es war nicht zu schaffen. Keine einzige Nuss liess sich von uns treffen.

Zum wohlverdienten Buffet

Mit letzter Kraft schleppten wir uns durch die Sintflut zurück in die Blockhütte. Da wurden unsere Mühe und all die Gefahren belohnt: der Brunch wurde ergänzt mit Braten, Schinken und Kartoffel-Auflauf. Wie froh waren wir, dass wir trotz unseres Fehlschlages beim Nussknacker nun doch etwas zu Essen bekamen. Nicht nur das: Nach kurzer Zeit erschien sogar noch ein reichliches Dessertbuffet mit gebrannter Creme, Schokoladenmousse und Zitronenkuchen.



Wohl genährt, schon ziemlich rund, aber mit einem glücklichen Lächeln auf dem Gesicht machten wir uns wieder auf den Heimweg. Sogar der Sturm hatte sich in der Zwischenzeit etwas gelegt und die Sonne blinzelte hinter den Wolken hervor. Beim Auto angekommen, stiegen wir ein und fuhren dem Regenbogen entgegen.

The End

PS: Herzlichen Dank an Esther Rölly und Brigitte Bailer für die tolle Organisation.



Sommernachtsparty

Von David Habegger



Unpassend zum Sommernachtsfest, welches im Herbst stattfand, blies ein winterlicher Wind auf der Terrasse des Uni-Turms, welcher einige Damen in frühlingshaften Cocktailkleidern erzittern liess. Nichtsdestotrotz liessen wir uns draussen mit Apéritotellerchen vom Feinsten verwöhnen und studierten die städtebauliche Entwicklung von Zürich.

Der Berner Remo/Reto Zumstein (Schweizermeister 2016 im Poetry Slam) erklärte uns humorvoll den Verschreiber seines Namens in der Einladung und abstimmungsaktuell das Fehlen

eines Vaterschaftsurlaubes. Remo bescherte uns einen gelungenen Werbespot für das Wirtschaftsinformatik-Studium, der hier aufgrund des breiten berndeutschen Dialekts des Autors besser nur in phonetischer Schrift wiederzugeben sei: [Maltli: i'd ITi: !].

Die episch kniffligen Fragen des altbewährten Quiz, führten dieses Mal die erfolgsverwöhnten Suchmaschinen-Bediener ins Leere. Charmant durften die Organisatorin Esther Rölly und die Präsidentin Brigitte Bailer die italienischen Geschenkkörbe an die besten Wahrscheinlichkeits-Theoretiker übergeben.

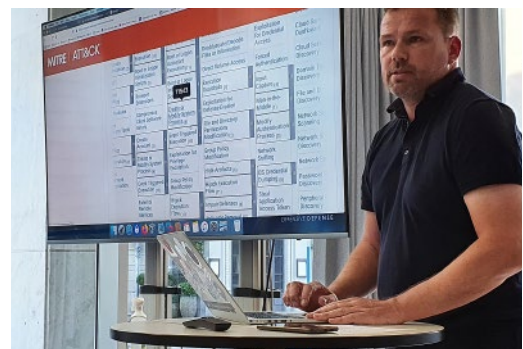
Persönliches Learning-Nugget

- Immer wieder spannend, welche interessante Gespräche – oft schon generationenübergreifend – zwischen Wirtschaftsinformatik-Alumni aus mittlerweile ganz verschiedenen Berufszweigen entstehen.
- Wer die immer wieder grandios unterhaltsamen, kulinarisch hochfliegenden Sommernachtsparties verpasst, ist selber schuld! Ein grosses Dankeschön auch an den Sponsor NSM Engineering AG, der diese Anlässe grosszügig unterstützt.

Cyber Security in der RS

Von Dr. Brigitte Bailer

Die heisseste Veranstaltung des Jahres 2020 war der Abendvortrag im August mit Ivan Bütler, CEO von Compass Security. Seine Ausführungen zum Thema Cyber Security und wie die Schweizer Armee damit beginnt, Rekruten gezielt auf diese Herausforderung vorzubereiten, war enorm lehrreich. Was man im Internet alles über die eigene Person innert kürzester Zeit finden kann, darüber sollte man Bescheid wissen. Für das grosse Ganze, also das Schweizer Sicherheitsdispositiv, sind die Cyber Attacken eine grosse Herausforderung. Der neu aufgegleiste Bachelor für Cyber Security hat uns Ivan inklusive Aufgabengebiet nähergebracht. Die Diskussionen danach waren so intensiv, dass der Abend erst lange nach Ende des Vortrages ein Ende fand. Herzlichen Dank Ivan für diesen hervorragenden Einblick in die Welt der Cyber-Security-Profis.



Unsere Sponsoren und Partner

Das vielfältige Angebot der UZH Alumni Informatik wäre ohne die tatkräftige Unterstützung unserer Sponsoren und Partner nicht möglich. Ihre Unterstützung erlaubt uns, unsere Aktivitäten frühzeitig zu planen und mit attraktivem Inhalt durchzuführen. Sie inserieren, leisten Beiträge an Events oder nutzen unseren E-Mail-Versand für die Suche nach Mitarbeitenden u.w.m.

Weitere Informationen zu einer Partnerschaft oder einem Sponsoring finden sich auf unserer Website www.alumni.ch unter der Rubrik «Sponsoren & Partner».

ADNOVUM

 **ausbildung-
weiterbildung.ch**
Das Schweizer Bildungsportal

avalog
essential for banking

 **GOLDWYN PARTNERS GROUP**

NSM
Engineering AG

 **PROACADEMICSAG**

Impressum

readme Nr. 45 / 2021

Herausgeberin
UZH Alumni Informatik

Redaktion
Christian Schneider (Lead Redaktion),
Brigitte Bailer, Anja Cavigilli,
Esther Röllli, Marc Pradervand,
Nathan Labhart, Nicola Fantini

Adresse
UZH Alumni Informatik
Schönberggasse 15a, 8000 Zürich
www.alumni.ch

Redaktionsadresse
readme@alumni.ch

Bildnachweise
www.shutterstock.com
Portraitfotos: www.alumni.ch
Beiträge: privat

Grafikdesign
Vera Grönegress

connecting the world
with best sources
for over 15 years

NEARSHORING

AT ITS

BEST