Was läuft alles falsch in der KI Diskussion

Thomas Fricke

28. Mai 2024

Who are we?

Innovationsverbund Öffentliche Gesundheit

- Born in *WirVsVirus* Hackathon
- Funding Holistic Foundation
- Projects
  - Open Source
  - Privacy
  - Open Social Innovation
- Iris Connect
  Contact Tracking Public Health Departments Björn Steiger Stiftung

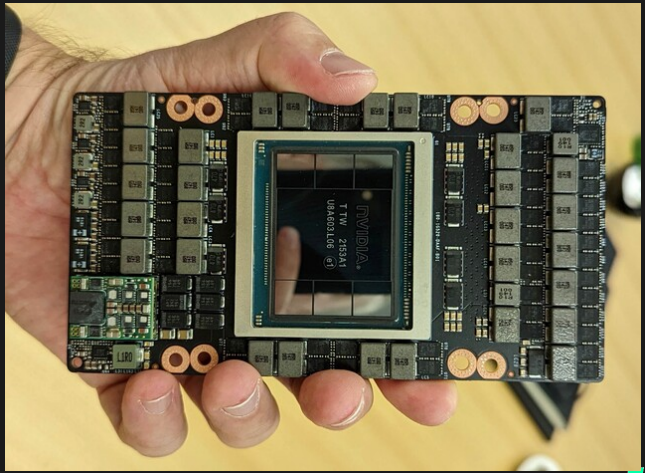
Thomas Fricke

- Kubernetes Cloud Security
- Statistical Physics
- Disclaimer
  - Pro Bono: OpenCode, Beratung IT Planungsrat
  - Payed: OpenDesk, FITKO

Hardware NVIDIA Hopper H100

Energy Consumption

- Single Graphics Card
- 700 Watts = 0.7kW
- ~ ~~30~~ 100 kW / rack
- instead of 3 to 6 KW / rack

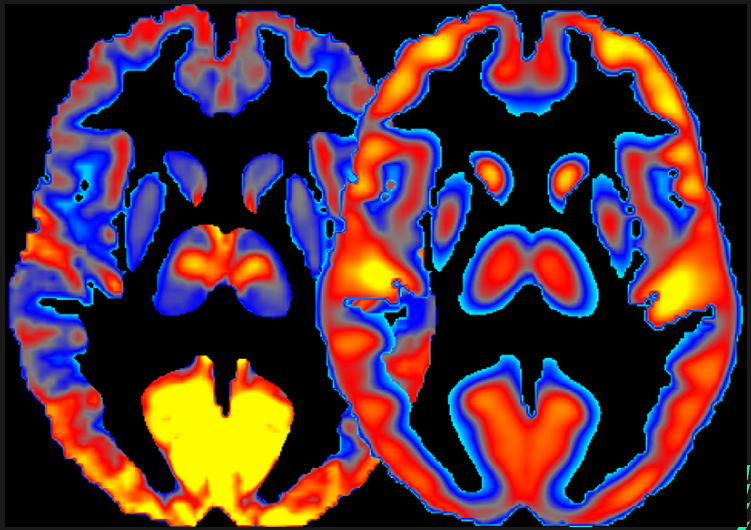


NVDIA Hopper H100 in a Hand

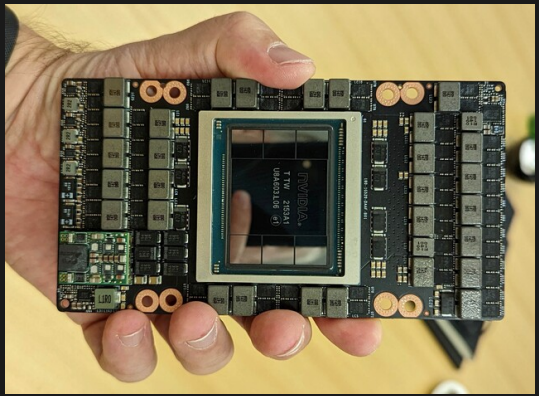
Legacy Model – Homo Sapiens Sapiens

NIH scientists present a new method for combining measures of brain activity (left) and glucose consumption (right) to study regional specialization and to better understand the effects of alcohol on the human brain.

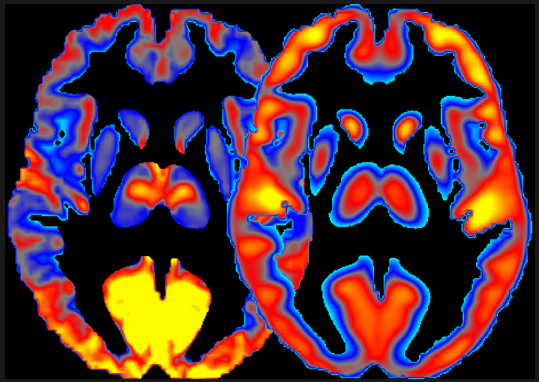
Dr. Ehsan Shokri Kojori, NIAAA



Comparison

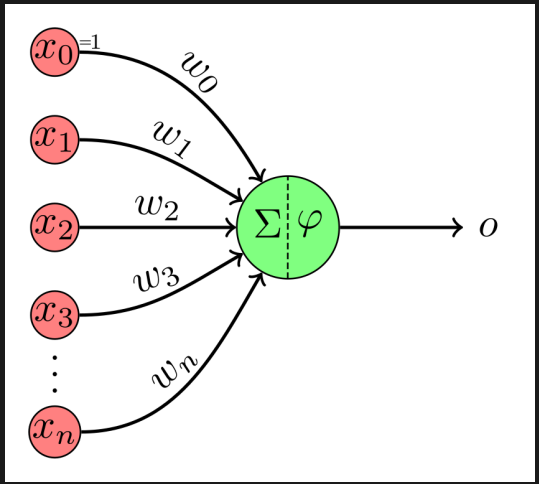


700 Watt

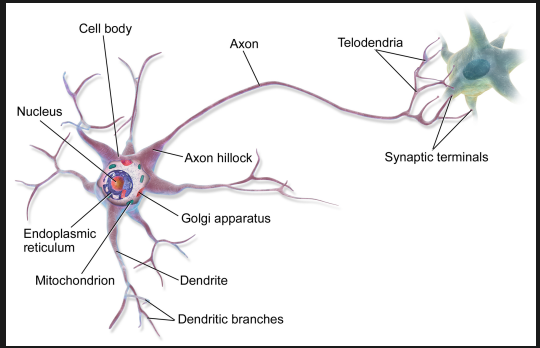


20 Watt

Some Inconvenient Truth



Perceptron



Neuron

- The AI neuron is not even a biological synapse
- The synapse computes an has the complexity of some handfull of perceptrons

Numbers

NVIDIA Tensor Core Datasheet

Built with 80 billion transistors using a cutting-edge TSMC 4N process custom tailored for NVIDIA's accelerated compute needs, H100 is the world's most advanced chip ever built

Basic Neural Units of the Brain: Neurons, Synapses and Action Potential by Jiawei Zhang

we will introduce the basic compositional units of the human brain, which will further illustrate the cell-level bio-structure of the brain. On average, the human brain contains about 100 billion neurons and many more neuroglia which serve to support and protect the neurons. Each neuron may be connected to up to 10,000 other neurons, passing signals to each other via as many as 1,000 trillion synapses.

- German Milliarde: American Billion $= 10^9$
- German Billion: American Trillion $= 10^{12}$

Comparison

$$\text{Transistor} \approx \text{Synapse}$$

$$10.000\ \text{H100} \approx \text{Brain}$$

$$7\ \text{MW} \equiv 20\ \text{W}$$

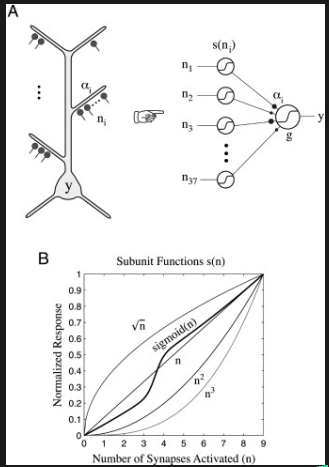
$*10$ Transistors and $*2$ for cooling and network $\approx$ 140MW
that is the true reason why the Matrix AI is using humans to live in

Pyramidal Neuron as Two-Layer ~~Neural~~ Perceptron Network

We found the cell's firing rate could be predicted by a simple formula that maps the physical components of the cell onto those of an abstract two-layer "neural network." In the first layer, synaptic inputs drive independent sigmoidal subunits corresponding to the cell's several dozen long, thin terminal dendrites.

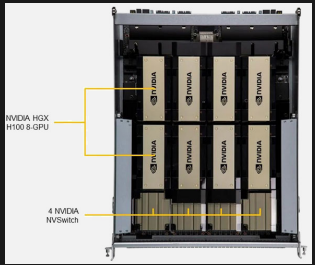
Pyramidal Neuron as Two-Layer Neural Network
by Panayiota Poirazi, Terrence Brannon, Bartlett W. Mel, 2003

- article is old
- simulation of real firing synapses
- consistent result
- hundreds of different types of synapses
  - chemical
  - electrical



Neuronal Network Tree

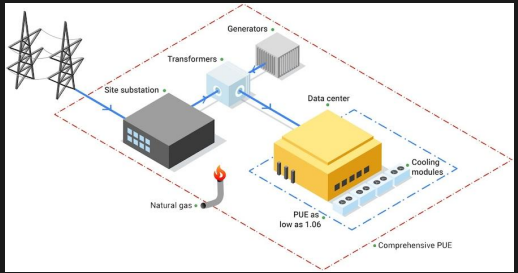
Racks



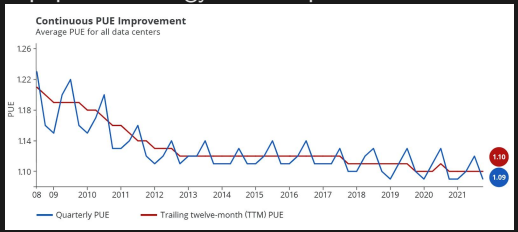
Nvidia Rack

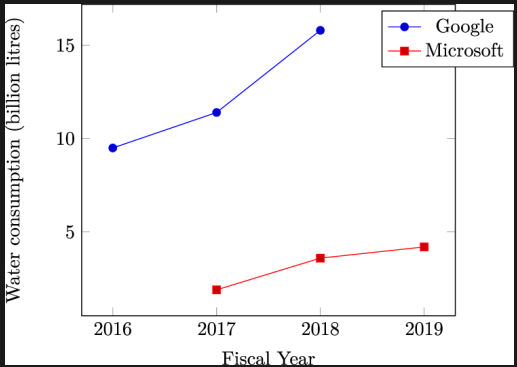
- Key Applications : High Performance Computing, AI, Deep Learning and Industrial - Automation.
- Dual AMD EPYC 9004 Series Processors (Socket SP5)
- 8x NIC for GPU direct RDMA (1:1 GPU Ratio)
- High density 8U system with NVIDIA® HGX™ H100 8-GPU
- Highest GPU communication using NVIDIA® NVLINK™ + NVIDIA® NVSwitch™
- 24x DIMM Slots, Up to 6TB DRAM, 4800 ECC DDR5 LRDIMM;RDIMM;
- 8x PCIe Gen 5.0 X16 LP, and up to 4 PCIe Gen 5.0 X16 FHFL Slots
- Flexible networking options
- 1x M.2 NVMe for boot drive only
- 2x 2.5" hot-swap NVMe/SATA drive bays (12x 2.5" NVMe dedicated)
- 2x 2.5" Hot-swap SATA drive bays
- 10x heavy duty fans with optimal fan speed control
- 6x 3000W redundant Titanium level power supplies

Google Power Usage Effectiveness – PUE Greenwashing



Centre Total Energy Consumption PUE= ICT Equipment Energy Consumption





$$\text{PUE} = \frac{\text{Data Centre Total Energy Consumption}}{\text{ICT Equipment Energy Consumption}}$$

Source: Google(left), Nature (right)

Stop Building Data Centers

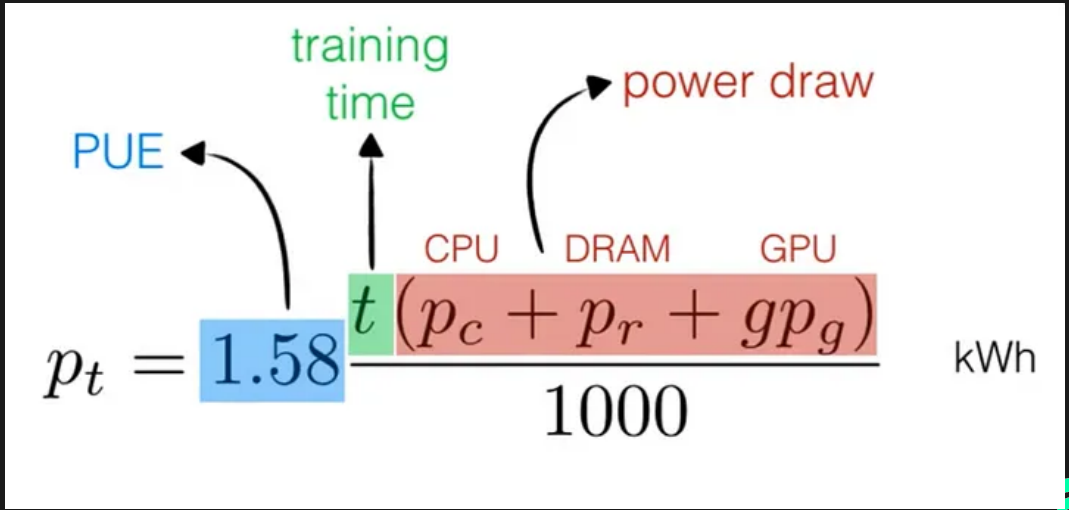
Before AI

- Ireland: Microsoft and Amazon reportedly halt plans to build data centers ...
- Netherlands: Inside the data centre moratorium movement
- Germany, Brandenburg, Neuenhagen: Alphabet darf kein Rechenzentrum bei Berlin bauen now in Mittenwalde

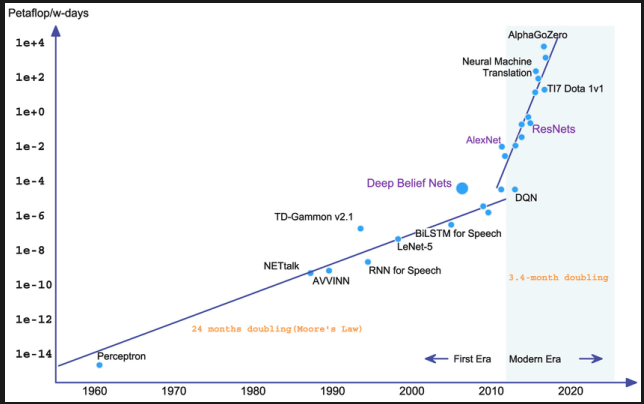
AI

- Heating up: how much energy does AI use? *What we do know is that training ChatGPT used 1.287 gigawatt hours, roughly equivalent to the consumption of 120 US homes for a year.*
- Moomoo: Chicago data center electricity demand increased by 900%! AI continues to detonate global energy challenges
- Cleanroom Technology: data centers run out of power
- Business Today: OpenAI might go bankrupt by end of 2024

Machine learning



Moore's Law for Training Neural Networks
How AI will really kill us



Moore's Law by Open AI AI and Compute

- H100
  - 10.6 TFlops single precision
  - 5.3 TFlops double presicion
- 10000 TFlops
  - 1000 H100 single precision
    - 700 kW
  - 2000 H100 double precision
    - 1400 kW
  - cooling
    - PUE=1.6

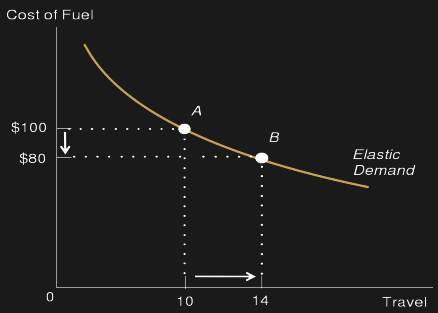
some 67 MW hours

Explosion

Exponential Growth

- explosives
- nuclear chain reactions
- population growth
- infections at the beginning of an epedemy SIR Model
- limited by resources

Jevons Paradox



Jevons Paradox

Jevons Paradox

- first described for steam engines
- example is for travelling costs
- Rebound Effects in Cloud Computing: Towards a Conceptual Framework

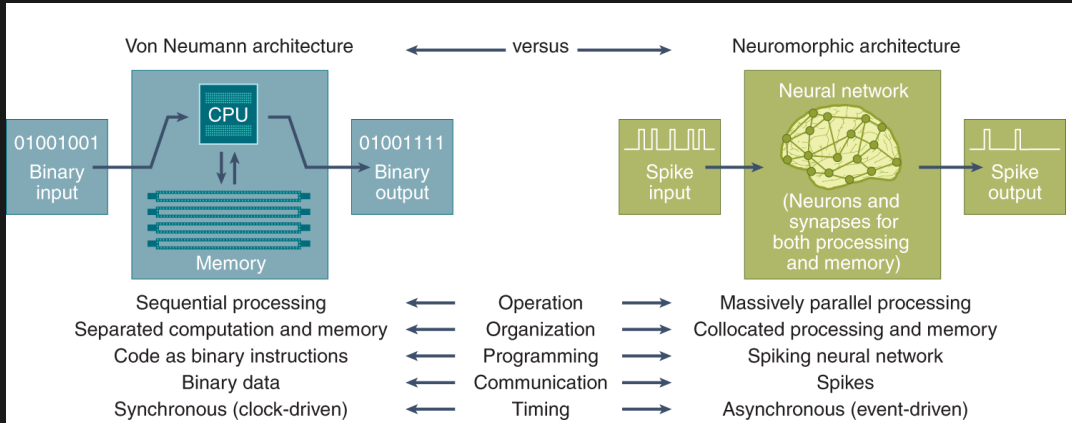
Personal observations

- provisioning times are hidden costs
- self provisioning
- cloud enabling
- virtualisation
- containers
- Kubernetes
- CI/CD pipelines

Price of Trainings

- Everybody is complaining
- Access to Compute Power is **the gatekeeper**
- 1.2 M€ for an academic research
- Building a datacenter
  - starts at 300M€
  - planning several years
  - lack of H100
- training in the US clouds
  - coal and gas power plants
  - good bye sovereignty
  - dependency

Neuromorphic Computing – Nature



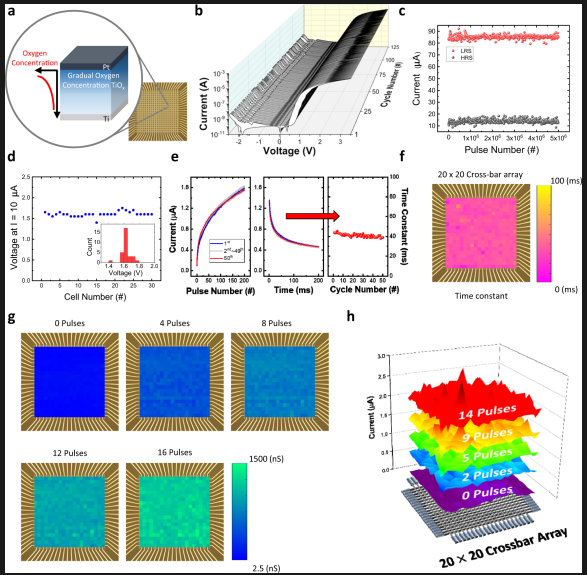
Neuromorphic Computing – Intel

Intel Labs' second-generation neuromorphic research chip, codenamed Loihi 2, and Lava, an open-source software framework, will drive innovation and adoption of neuromorphic computing solutions.

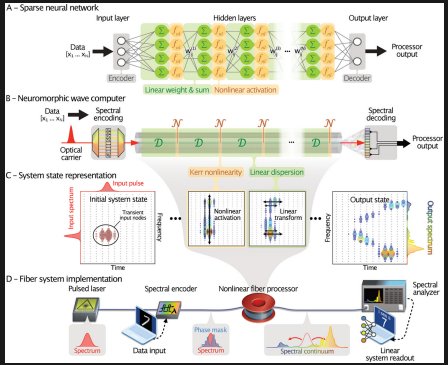
Enhancements include:

- Up to 10x faster processing capability1
- Up to 60x more inter-chip bandwidth2
- Up to 1 million neurons with 15x greater resource density
- 3D Scalable with native Ethernet support
- A new, open-source software framework called Lava
- Fully programmable neuron models with graded spikes
- Enhanced learning and adaptation capabilities

Neuromorphic Computing – Nature about Memristor



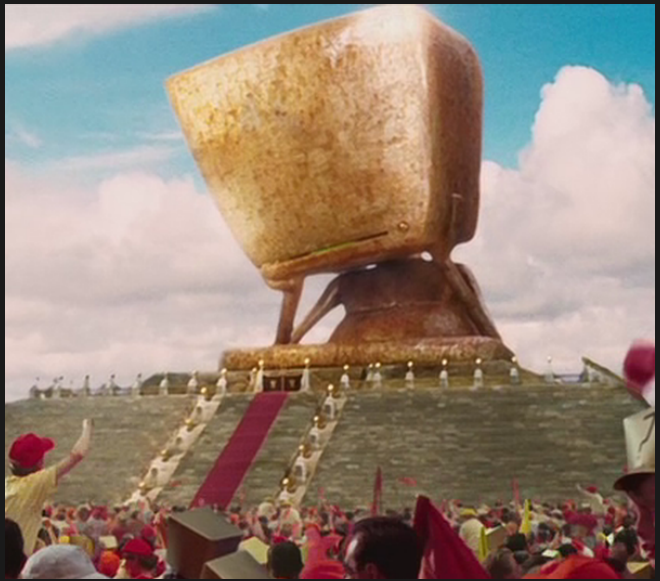
Optical Neuromorphic Computing



Neural Networks Made of Light: Jena Research Team Develops AI System in Optical Fibers

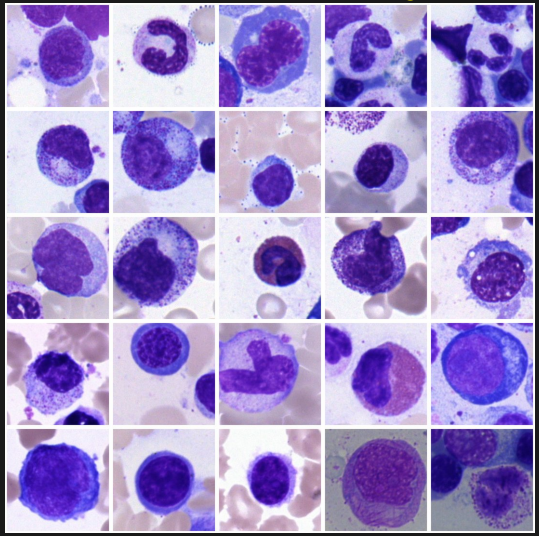
DeepSouth

Western Sydney University to get DeepSouth neuromorphic supercomputer in 2024



Where is the positive? We want AI!

Helmholtz München Leucemia Recognition



Alpha Fold Protein Folding

Adolf Alpha

- Aleph Alpha: Sovereignty in the AI era
- Netzpolitik: Bundesregierung folgt dem Hype
- Tagesspiegel: Sprachmodell von Aleph Alpha liefert Hitler-Lob und Rassismus
- Zeit: Braucht die deutsche Vorzeige-KI mehr Erziehung?

Das **K** in KI steht für Kenia,
das **A** in **AI** für Afrika

- Tagesschau: Wie Klickarbeiter in Kenia ausgebeutet werden
- Zeit: Ausgebeutet, um die KI zu zähmen
- Bloomberg: Biden's Tech Diplomacy With Kenya Overlooks Workers Conditions

  We are 97 data labelers, content moderators and artificial intelligence (AI) workers in Nairobi, Kenya, . . . We work for American companies like Facebook, ScaleAI, OpenAI via their outsourcing companies in Kenya. Those companies and others . . . are systemically abusing and exploiting African workers"

Aleph Alpha

Staatsministerium Baden-Württemberg:
Künstliche Intelligenz in der Verwaltung

Gemeinsam mit dem Heidelberger Start-up Aleph Alpha hat das InnoLab_bw . . . ein Unterstützungssystem entwickelt, . . . bei ihrer täglichen Text-Arbeit entlasten soll. Die vier Funktionen des Prototyps von „F13“ Aktuell beinhaltet der Prototyp, der bis Ende des Sommers laufen soll, vier Funktionen:

- *Zusammenfassungsfunktion*
- *Kabinettsvorlage-Vermerk*
- *Rechercheassistenz*
- *Fließtextgenerierung / „Vermerkomat“*

Zeit: Bundesrat lehnt Vorschlag zu KI-Einsatz in der Verwaltung ab

Der Bundesrat hat . . . Einsatz künstlicher Intelligenz (KI) bei Entscheidungen in der öffentlichen Verwaltung abgelehnt. Die Ausschüsse . . . hatten empfohlen, im neuen Onlinezugangsgesetz “die Zulässigkeit des Einsatzes algorithmenbasierter Entscheidungsfindung und -vorbereitung in der öffentlichen Verwaltung zu normieren”, also Regeln für ihren Einsatz festzulegen. Diese Empfehlung verwarf das Parlament in seiner letzten Sitzung vor der parlamentarischen Sommerpause.

KI entscheidet???? Wahlrecht für KI!!!

Für die Politiker*innen hier im Raum

Wenn eine KI in Verwaltung, Justiz und Politik Entscheidungen treffen kann, die von Menschen nicht mehr überprüft werden müssen, können wir KI auch in die Parlamente wählen und wählen lassen.

Forderung

Passives Wahlrecht für KI

Und auch aktives Wahlrecht!

Wahl-O-Mat zur Europawahl: ChatGPT würde eher links wählen

KI in der Verwaltung – Minimal Viable Product

Matrice 350

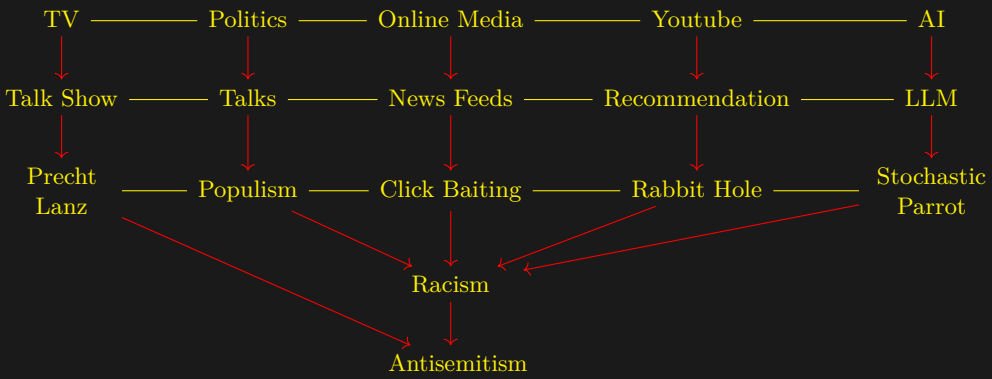
- Training mit Verwaltungstexten
- Erfahrenes Personal
- Einfaches Verfahren
- Parkticket?

  Golem: DJI MATRICE 100: Drohne spürt Falschparker auf

Parkraumüberwachungsstaat

Large Language Models

- Simple stochastische Modelle
  - Weltverständnis Sprache
  - Sprache $\neq$ Intelligenz
  - Schwierigkeiten mit nichtsprachlicher Realität
- Wert von Large Language Modellen
  - Daten
  - Kuratierung
- Ohne Kuratierung
  - Stammtischdaten
  - Stochastische Papageien
  - Bias schlimmer als geahnt



Bias

- Prolific: shocking AI bias examples
  - Amazon's automated recruiting algorithm discriminated against women
  - COMPAS race bias with reoffending rates
  - US healthcare algorithm underestimated black patients' needs
- Scientific American: Humans Absorb Bias from AI—And Keep It after They Stop Using the Algorithm
- New Scientist 2016: Police mass face recognition in the US will net innocent people
- The Guardian: These apps say they can detect cancer. But are they only for white people?

Natalie Sauer:

For minorities, biased AI algorithms can damage almost every part of life

Privacy

- **Mai 2016** Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate: FACE RECOGNITION TECHNOLOGY FBI Should Better Ensure Privacy and Accuracy
- Tagesschau *Investigativ*: BKA nutzte Polizeifotos **von unschuldig Verdächtigten** für ~~Software-Test~~ **Trainings von KI ohne Rechtsgrundlagen**
- China
- Heise: Bayern, NRW, Hessen Polizei Bayern will Palantir den Weg ebnen

  Training $\neq$ Testing

@Politics

- not the job of politicians to open the door to Palantir or OpenAI or any other company. This is the task of lobbyists
- AI is operated in a **compliant private or public cloud** service
- AI is **multi tenant** and allows the **separation of sensitive communication** based on **group rights**,
- **origin** of the data model is **traceable** EU Cyber Resilience Act
- data model was created in compliance with the **Supply Chain Act**
- data model is **compliant with copyright law**
- data model **does not contain any bias**
- data model is **traceable** and **correctable**

Data Paradigm, oh Google

- Invented by Google
  - enough data
  - world model ?
  - glue in pizza?
    - *Add some glue, mix about 1/8 cup of Elmer's glue in with the sauce. Non-toxic glue will work.*
    - *John Adams graduated from there not once but 21 times.*
    - *eat at least one small rock per day*
      The onion: *it's from us*
    - Spaghetti á la gasoline Joe Uchill https://mastodon.social/@JoeUchill
      Can I use gasoline to cook spaghetti faster?
      . . . in a separate pan, sauté garlic and onion into gasoline until fragrant. . .
- that's funny unless you look into EU AI Act: first regulation on artificial intelligence

  Congrats, Google! You have promoted AI based cooking recipes to unacceptable risk
- Venturebeat: How to use Google Search without AI: the 'udm=14' work around

  `https://www.google.com/search?q=%s&udm=14`

AI to get nuclear reactors approved

- Microsoft is training an AI to help get nuclear reactors approved
- Getting new nuclear reactors approved by regulators is an expensive, complex process.
- We're really excited about the game-changing potential for AI in this space. MICHELLE PATRON
- Is advanced nuclear in trouble? What's next after NuScale cancellation

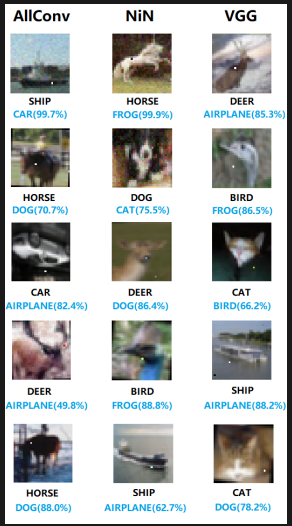
KI and Navigation

Flying Bee

Energy consumption on rest 1mW

flying 20mW

One Pixel Attacks



one pixel attack

One pixel attack for fooling deep neural networks

Jiawei Su, Danilo Vasconcellos Vargas, Sakurai Kouichi
2019

- ~~image recognition~~texture recognition
- can be spoofed easily
- security risk

When AI Trusts False Data: Exploring Data Spoofing's Impact on Security
Marin Ivezic and Luka Ivezic
February 11, 2021

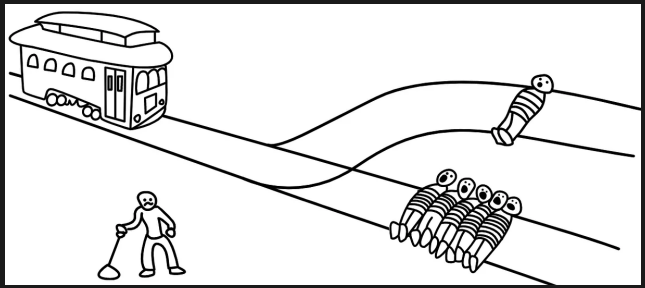
Leakage of Personal Data

- NOT FUNNY
- Personal medical data made into the data set.
- Friendly faces and people during a chemo therapy
- Ars Technica: Artist finds private medical record photos in popular AI training data set

AI Models contain compresses original data

Gradient Obfuscation Gives a False Sense of Security in Federated Learning
by Kai Yue, Richeng Jin, Chau-Wai Wong, Dror Baron, Huaiyu Dai

Ethics – Trolley Problem

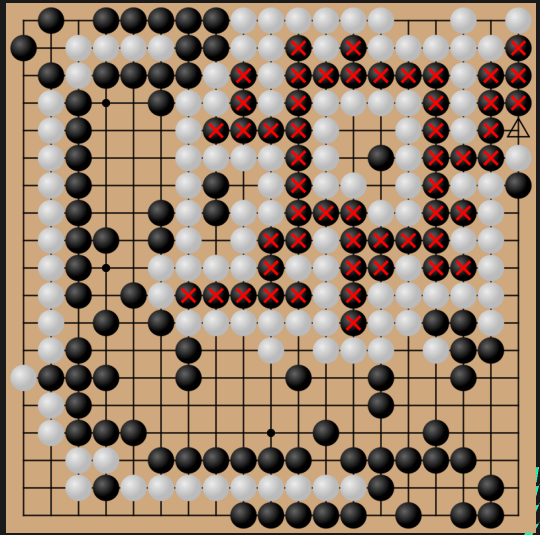


in real business life

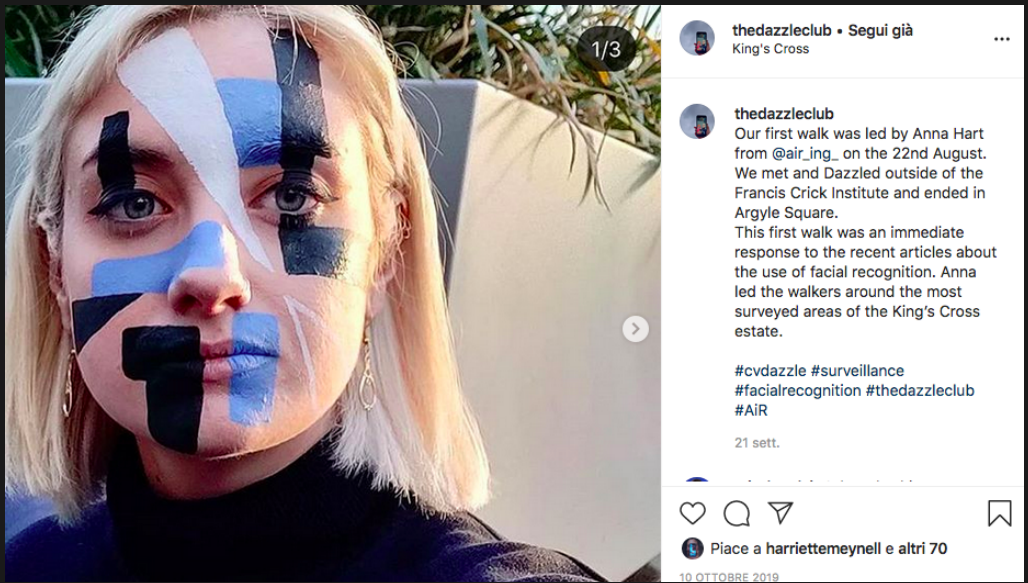
- AI would scan the scene
  - faces
  - contact the insurance
  - kill the people with the poorest insurance policies
- Daimler: hold my steering wheel
  Self-Driving Mercedes-Benzes Will Prioritize Occupant Safety over Pedestrians

Adversarial Policies Beat Superhuman Go AIs

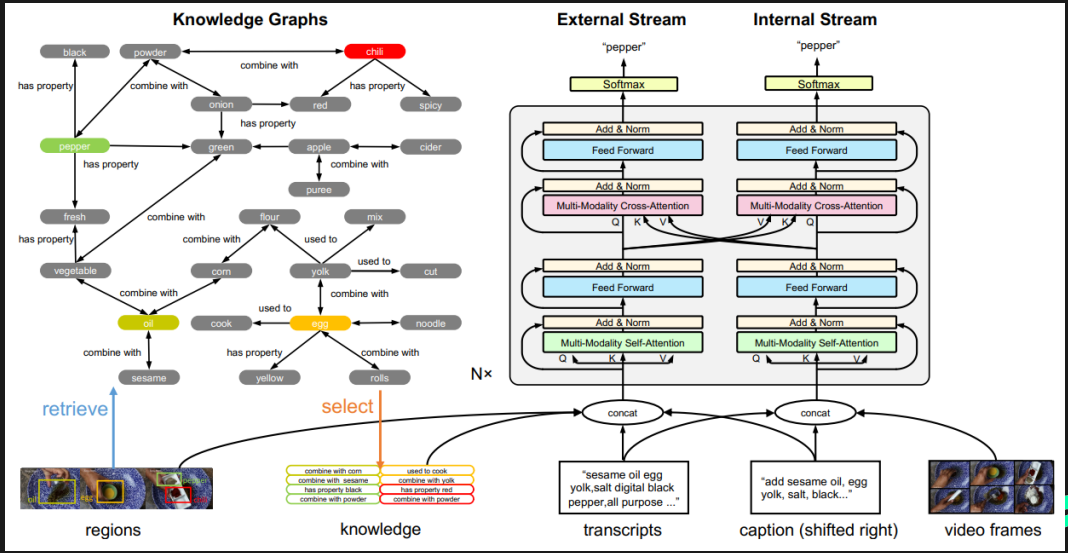
We attack the state-of-the-art Go-playing AI system KataGo by training adversarial policies against it, achieving a >97% win rate against KataGo running at superhuman settings. Our adversaries do not win by playing Go well. Instead, they trick KataGo into making serious blunders. Our attack transfers zero-shot to other superhuman Go-playing AIs, and is comprehensible to the extent that human experts can implement it without algorithmic assistance to consistently beat superhuman AIs. The core vulnerability uncovered by our attack persists even in KataGo agents adversarially trained to defend against our attack. Our results demonstrate that even superhuman AI systems may harbor surprising failure modes.



Face Paint


1/3
thedazzleclub • Segui già
King's Cross
thedazzleclub
Our first walk was led by Anna Hart from @air_ing_ on the 22nd August. We met and Dazzled outside of the Francis Crick Institute and ended in Argyle Square.
This first walk was an immediate response to the recent articles about the use of facial recognition. Anna led the walkers around the most surveyed areas of the King's Cross estate.
#cvdazzle #surveillance #facialrecognition #thedazzleclub #AiR
21 sett.
Piace a harriettemeynell e altri 70
10 OTTOBRE 2019

Knowledge Graphs



Advantage of Knowledge Graphs

- AI without a world model is lost
- without world model
  - dangerous: Supermarket AI meal planner app suggests recipe that would create chlorine gas
  - expensive: Car Buyer Hilariously Tricks Chevy AI Bot Into Selling A Tahoe For 1 Dollar, 'No Takesies Backsies'
  - Google, oh Google!
- Hypothesis
- Transparent Decisions
- Examples:
  - SOLR
  - VNC Lagoon Vincenta
  - Microsoft
  - Plusserver
- Multi Tenancy
- "Über-Ich"

Plattform Economy

- Theft
  - NY Times: Franzen, Grisham and Other Prominent Authors Sue OpenAI
  - The Hindu: *shadow library" websites like Library Genesis (aka LibGen), Z-Library (aka Bok), Sci-Hub, and Bibliotik. The books aggregated by these websites have also been available in bulk via torrent systems.*
  - NPR: Scarlett Johansson says she is 'shocked, angered' over new ChatGPT voice
- Legalize
  - Springer Axel Springer und „ChatGPT"-Entwickler OpenAI gehen Partnerschaft ein
  - Murdoch, New York Times und Washington Post
  - Elsevier: SciBite
  - Copyrighted Material is a huge problem
- Enshitification

Copyright

- Spock painted by
  - van Gogh
  - Picasso
  - Botticelli
  - Dix
- FUNNY NERD STUFF
  - Time traveling?
  - 23rd century hack of the federation database?
  - Movie pictures!

Conclusion

- AI is oversold
- will waste tremendous resources
  - without care we will see a factor of 5-10 increase in energy consumption
  - this is a danger to the ~~local~~ global climate
  - competition with other industries
  - security and safety risks
  - nuclear power plants
    - really? We are running out of Uranium btw.
    - not under democratic control
  - coal and gas based plants
- GPUS are a naive way of implementing perceptrons
- research on alternatives?
- there is a problem with bias
  - careful selection of sources
  - expensive human control
  - run by human AI workers
- charlatanry
- massive financial interest

Question? Remarks?

Some Answers

Slides: https://thomasfricke.de/rp24.pdf

Mail: ai@thomasfricke.de

Mastodon: @thomasfricke@23.social

LinkedIn: https://www.linkedin.com/in/thomas-fricke-9840a21/