MUNI
ICS

3. Počítače a počítání

Aleš Křenek
ljocha@ics.muni.cz

Ústav výpočetní techniky, MU

2. 10. 2023

Proč má počítač počítat?

- To, co chceme na počítači vidět, slyšet, …zpravidla nějak souvisí se světem a lidmi
- Lidské poznání světa popisují vědy (humanitní i přírodní)
- Matematika je nástrojem k preciznímu vyjádření vědeckého poznatku
- Aritmetika je konkrétním, praktickým uchopením matematiky

Proč má počítač počítat?

- To, co chceme na počítači vidět, slyšet, …zpravidla nějak souvisí se světem a lidmi
- Lidské poznání světa popisují vědy (humanitní i přírodní)
- Matematika je nástrojem k preciznímu vyjádření vědeckého poznatku
- Aritmetika je konkrétním, praktickým uchopením matematiky
- Počítače jsou v aritmetice velmi dobré
  - desítky miliard operací za vteřinu na jednom jádru CPU
- K tomu přidávají paměť
  - Encyclopaedia Britannica: 32 tis. stran – řádově desítky až stovky MB informace
  - běžný mobil – desítky GB úložiště (1000× více)

Angry Birds

- https://www.youtube.com/watch?v=Km0UUVEQKpI (1:45)
- Jednoduchá hra, chová se v souladu s očekáváním na základě zkušenosti
- Platí v ní běžné fyzikální zákony, jsou výpočetně simulovány

$$F = ma \qquad v = at \qquad s = vt$$

- Kompletní simulaci jednoduché scény zvládne mobil

Angry Birds

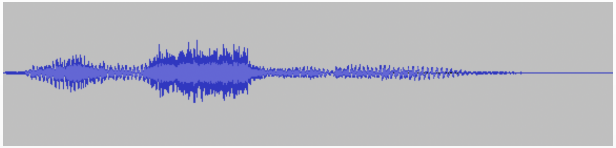
- https://www.youtube.com/watch?v=Km0UUVEQKpI (1:45)
- Jednoduchá hra, chová se v souladu s očekáváním na základě zkušenosti
- Platí v ní běžné fyzikální zákony, jsou výpočetně simulovány

$$F = ma \qquad v = at \qquad s = vt$$

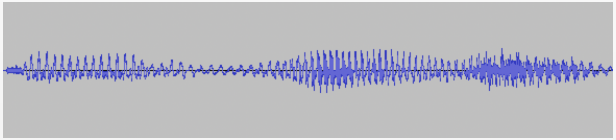
- Kompletní simulaci jednoduché scény zvládne mobil
- Simulace chování viru je totéž pro miliony atomů současně a miliardy kroků výpočtu https://youtu.be/7AhQ19m2ok4

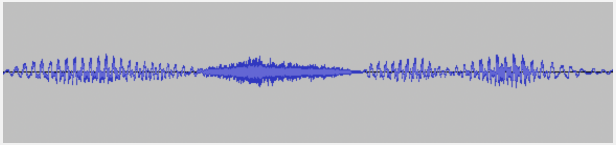
Hey, Siri!

- Referenční záznam „Hey, Siri!“



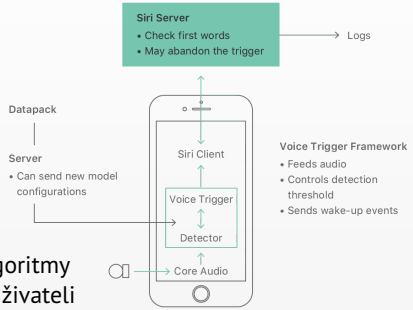
- „Hey, Siri!“ a jiná podobně dlouhá věta (jiný člověk)





Hey, Siri!

- Mobil zaznamená a analyzuje zvuk
- Specializovaný hardware
  - např. Apple „Neural Engine“
  - dopředu nacvičený rozpoznat klíčovou větu
  - postupně se přizpůsobuje konkrétnímu uživateli
- Záznam putuje do cloudu
- Transformace hlasu na text a analýza významu
  - vzájemně provázané, komplikované modely a algoritmy
  - globální znalost i přizpůsobení se konkrétnímu uživateli
- Zpravidla komplikované neuronové sítě (umělá inteligence)
- V důsledku miliardy aritmetických operací
- `https://machinelearning.apple.com/research/hey-siri`



Facebook, Youtube, Instagram, TikTok, ...

- raději nevědět ...

Facebook, Youtube, Instagram, TikTok, ...

- raději nevědět ...
- „jednoduché“ analýzy à la Cambridge Analytica
- očekávané zpracování (konverze formátu videa)
- porozumění textu i obrazu (detekce závadného obsahu)
  - `https://ai.facebook.com/blog/how-facebook-uses-super-efficient-ai-models-to-detect-hate-speech/`
  - `https://www.theverge.com/2019/7/3/20681231/facebook-outage-image-tags-captions-ai-machine-learning-revealed`
  - „Content ID claim“ na Youtube
- kombinace výpočetní síly a obrovského množství dat

Facebook a Cambgridge Analytica

- Skandál s pravděpodobným ovlivněním voleb v USA 2016
- Kvíz charakteristik osobnosti a politických preferencí
  - Odměna $2–5 za vyplnění
  - 320 tis. respondentů v USA
- Sběr dat o aktivitě na FB („lajky“, skupiny, …)
  - matice „lajků“, dekompozice na singulární hodnoty, korelace, …
- Přes „přátele“ expanze na dalších 50–90 milionů lidí
- Predikce osobnosti a politických preferencí, možnost cílené politické reklamy
- Zjednodušená rekonstrukce `http://doi.org/10.1073/pnas.1218772110`

Kódování zvuku a videa

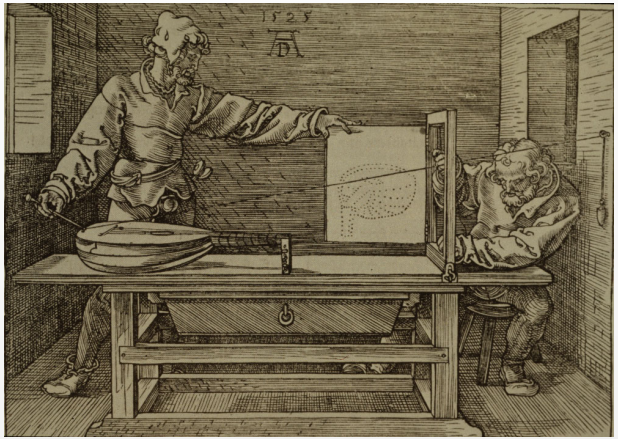
- Připomenutí předchozí přednášky
  - digitální obraz je složen z několika milionů bodů
  - pro každý bod zpravidla 3 čísla (R,G,B)
  - tolik dat neuložíme ani nepřeneseme, nezbytná komprese
- Velký počet aritmetických operací, musí se stihnout včas

Střílečky a animáky

- „Makro“ fyzika (viz Angry Birds)

Střílečky a animáky

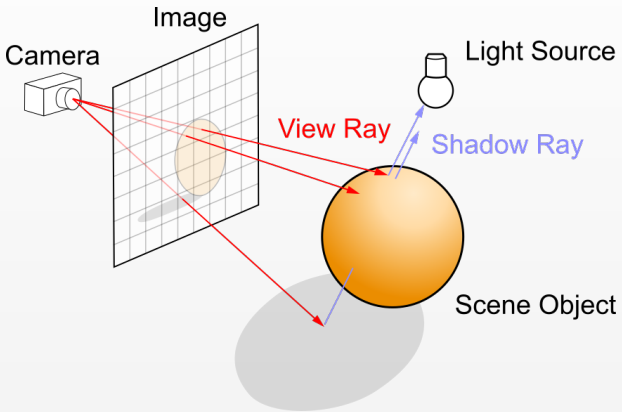
- „Makro“ fyzika (viz Angry Birds)
- Optika – realistický obraz, např. sledování paprsku



(Albrecht Dürer, 1525)

Střílečky a animáky

- V počítačové verzi



- Provedeme 60× za vteřinu pro každý z 8 milionů bodů obrazu …

Střílečky a animáky

- umělá inteligence (jednání postav, …)

Střílečky a animáky

- umělá inteligence (jednání postav, …)

- konvenční – vše je modelováno na lokálním zařízení
- tradiční síťové – lokální pohled na herní svět modelujeme u sebe, interakce na serveru
- cloudové – uživatelské zařízení je jen příjemce videostreamu
  - optimalizace hardware (výdrž na baterie, cena, …)

Těžba kryptoměn

- Principem těžby Bitcoinu je hledání *noncí* („příležitost“):
  - úloha podobná „uhodni číslo, které po vynásobení 1115693994938935442811052828725345276943 27 má šestou a sedmou cifru 42“
- Použité algoritmy (SHA-2) zaručují, že se musí hádat, nelze vypočítat lépe
- Mechanismus těžby zaručuje produkci stabilní 6.25 BTC / 10 min
  - zvyšuje náročnost těžby při zapojení dalších těžařů

Těžba kryptoměn

- Principem těžby Bitcoinu je hledání *noncí* („příležitost“):
  - úloha podobná „uhodni číslo, které po vynásobení 1115693994938935442811052828725345276943 27 má šestou a sedmou cifru 42“
- Použité algoritmy (SHA-2) zaručují, že se musí hádat, nelze vypočítat lépe
- Mechanismus těžby zaručuje produkci stabilní 6.25 BTC / 10 min
  - zvyšuje náročnost těžby při zapojení dalších těžařů

- Hrubý výpočet ze statistik: alespoň 10^{25} aritmetických operací na jeden BTC
  - výkon sítě $\sim$100 EH/s
  - každý hash alespoň tisíce aritmetických operací
  - potvrzení bloku každých 10 min, vygeneruje 6.25 BTC, tj. 100s/BTC

Těžba kryptoměn

- Principem těžby Bitcoinu je hledání *noncí* („příležitost“):
  - úloha podobná „uhodni číslo, které po vynásobení 1115693994938935442811052828725345276943 27 má šestou a sedmou cifru 42“
- Použité algoritmy (SHA-2) zaručují, že se musí hádat, nelze vypočítat lépe
- Mechanismus těžby zaručuje produkci stabilní 6.25 BTC / 10 min
  - zvyšuje náročnost těžby při zapojení dalších těžařů

- Hrubý výpočet ze statistik: alespoň 10^{25} aritmetických operací na jeden BTC
  - výkon sítě ∼100 EH/s
  - každý hash alespoň tisíce aritmetických operací
  - potvrzení bloku každých 10 min, vygeneruje 6.25 BTC, tj. 100s/BTC

- `https://www.lrb.co.uk/the-paper/v41/n08/donald-mackenzie/pick-a-nonce-and-try-a-hash`

Digitální modely a dvojčata

- 90. léta, Boeing 777 jako první důsledný
  - miliony součástí
  - každá popsána desítkami až stovkami čísel (souřadnice rohů, …)
  - správná rotace a umístění – transformace souřadnic
  - K. Sabbagh, 21st-Century Jet: The Making and Marketing of the Boeing 777, New York: Scribner, 1996

Digitální modely a dvojčata

- 90. léta, Boeing 777 jako první důsledný
  - miliony součástí
  - každá popsána desítkami až stovkami čísel (souřadnice rohů, …)
  - správná rotace a umístění – transformace souřadnic
  - K. Sabbagh, 21st-Century Jet: The Making and Marketing of the Boeing 777, New York: Scribner, 1996
- Dvojčata unikátních zařízení
  - kosmická loď, turbína v Temelíně, …
  - „dvojče“ sleduje chování fyzického zařízení: matematický model a data ze senzorů
  - včasná detekce problémů, opotřebení, …
  - simulace scénářů „co se stane, když …“
  - složitá zařízení $\Rightarrow$ mnoho dat a náročný výpočet

Aplikace ve vědě

- Předpověď počasí
  - 1950, první významná numerická aplikace
  - `https://maths.ucd.ie/~plynch/Publications/ENIAC-BAMS-08.pdf`

Aplikace ve vědě

- Předpověď počasí
  - 1950, první významná numerická aplikace
  - `https://maths.ucd.ie/~plynch/Publications/ENIAC-BAMS-08.pdf`
- SETI@home (1999 – 2020)
  - signály z radioteleskopů, rozděleny na malé části a distribuovány „uživatelům“ (1.8 M)
  - detekce vzorů, které by mohly mít nepřirozený, mimozemský původ
  - software jako „šetřič obrazovky“, využití zahálejících počítačů

Aplikace ve vědě

- Předpověď počasí
  - 1950, první významná numerická aplikace
  - `https://maths.ucd.ie/~plynch/Publications/ENIAC-BAMS-08.pdf`
- SETI@home (1999 – 2020)
  - signály z radioteleskopů, rozděleny na malé části a distribuovány „uživatelům“ (1.8 M)
  - detekce vzorů, které by mohly mít nepřirozený, mimozemský původ
  - software jako „šetřič obrazovky“, využití zahálejících počítačů
- Hledání tvaru proteinů
  - Folding@home – stejný vzor
  - AlphaFold (2020) – masivní užití umělé inteligence

Aplikace ve vědě

- Higgsův bosson a další
  - urychlovač částit LHC (CERN)
  - od cca. roku 2000 bylo jasné, že objem dat a potřeba výpočtů bude enormní
  - nepřetržitý tok „událostí“ (kolize částic a jejich detekce), filtrování smysluplných
  - simulace možného chování, srovnávání s výsledkem experimentů

Aplikace ve vědě

- Higgsův bosson a další
  - urychlovač částit LHC (CERN)
  - od cca. roku 2000 bylo jasné, že objem dat a potřeba výpočtů bude enormní
  - nepřetržitý tok „událostí“ (kolize částic a jejich detekce), filtrování smysluplných
  - simulace možného chování, srovnávání s výsledkem experimentů
- biologie na molekulární úrovni
  - genetická informace – sekvenování
  - struktura biomolekul – krystalografie, NMR, CryoEM, …
  - analýzy vzorků – hmotnostní spektrometrie
  - data z tisíců laboratoří, potenciálně citlivá

Aplikace ve vědě

- Higgsův bosson a další
  - urychlovač částit LHC (CERN)
  - od cca. roku 2000 bylo jasné, že objem dat a potřeba výpočtů bude enormní
  - nepřetržitý tok „událostí“ (kolize částic a jejich detekce), filtrování smysluplných
  - simulace možného chování, srovnávání s výsledkem experimentů
- biologie na molekulární úrovni
  - genetická informace – sekvenování
  - struktura biomolekul – krystalografie, NMR, CryoEM, …
  - analýzy vzorků – hmotnostní spektrometrie
  - data z tisíců laboratoří, potenciálně citlivá
- COVID-19
  - zjištění struktury viru a jeho proteinů
  - simulace chování léčiv
  - návrhy vakcín

Velké jazykové modely

- *Model* si „přečte“ velké množství textu
  - řádově více, než jeden člověk za celý život
- Získaná znalost je v něm *nějak* reprezentována
  - pouze omezeně rozumíme, co se uvnitř děje
- Pozorované schopnosti blížící se člověku
  - překlad mezi jazyky, konverzace, generování textu na dané téma …

Chceme ještě lepší počítače

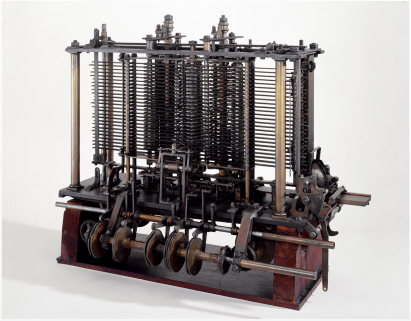
- S lepší technologií jsme toho zvládli více
- Víme, že s ještě lepší technologií to půjde dál
- Tlak na další vylepšování technologie … a pořád dokola
- Moorův zákon
  - Za stejné peníze dostaneme za 18–24 měsíců dvojnásobný výkon
- exponenciální růst
- platí cca. od roku 1975

Technologie a jejich rozvoj

- Máme data, kam s nimi?
- Jak se k datům dostaneme?
- Jak data zpracujeme?

Trocha historie

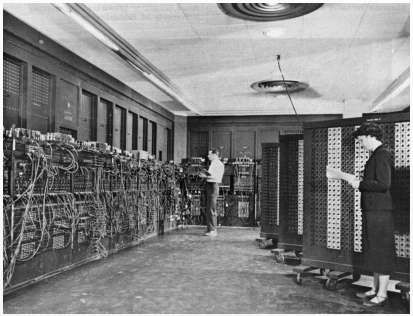
- Analytical Engine (Charles Babbage, 1837)



- 16 kB paměti, aritmetické operace včetně $\sqrt{\ }$, čísla s přesností až 50 míst
- Gausova eliminace, řešení polynomů …
- Pouze kvantitativně odlišné od počítačů 21. století

Trocha historie

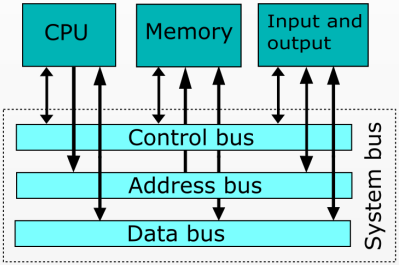
- Electronic Numerical Integrator and Computer (1945)



- Elektronky, relé, …
- 5 mil. ručně pájených spojů
- 150 kW, 500 FLOPS
- Výpočty vodíkové bomby

Od mobilu k superpočítači

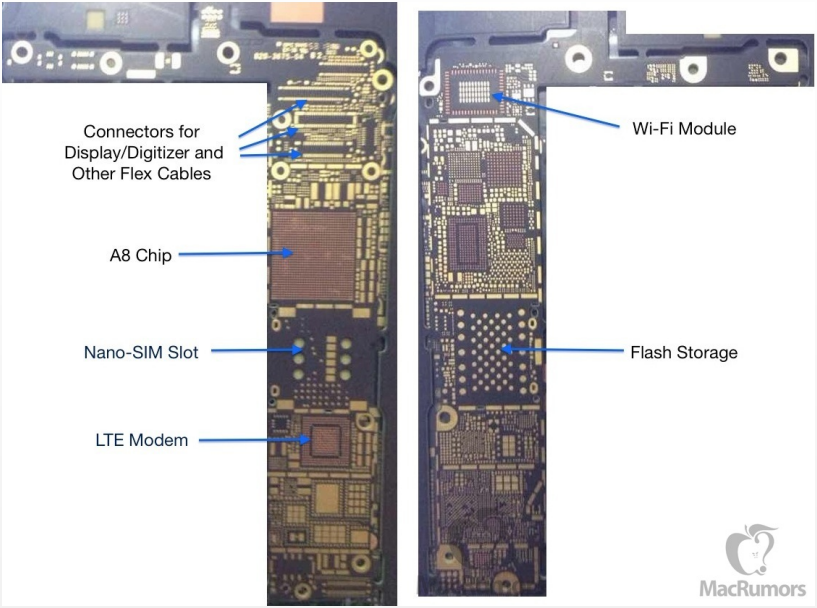
- Základní architektura je u všech stejná
- Sběrnice pro veškerou komunikaci
- CPU („mozek“) a paměť
- Vstupy a výstupy
  - úložiště (disk, SSD)
  - grafika
  - klávesnice/myš/dotykový displej
  - komunikace (síť, wifi, LTE, …)
- Výrazné rozdíly v hlavním účelu, a tedy i ve výkonu a kapacitě



Mobil a tablet

- zvuk, fotky, video, komunikace, méně náročné hry
- relativně velký špičkový výkon (neliší se od desktopu), jen velmi krátký čas
- specializované akcelerátory (kodeky, AI)

Mobil a tablet



Počítač domácí a kancelářský, notebook

- + kancelářská práce, náročnější hry, menší výpočty
- stavěný na dlouhodobější zátěž ve vyšším výkonu
- výkonná grafická karta

Servery v datacentrech

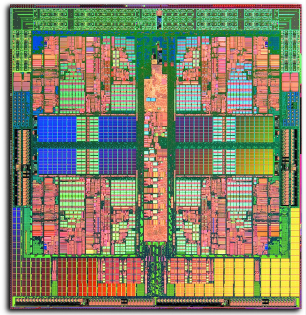
- dostupné služby a sdílení mnoha uživateli vs. intenzivní výpočty
- více jader, větší RAM, rychlejší síť
- serverové disky a SSD, výpočetní GPU
- provedení do racku, dlouhodobá vysoká zátěž
- hot-swap komponenty, chlazení
- `https://my.matterport.com/show/?m=ao36A4WHbuf`

Superpočítače

- totéž ve velkém
- jak udržet tak velký systém naživu?
  - při riziku selhání jedné komponenty 1:10000 selže systém o 1000 komponentách s pravděpodobností 10 %
  - největší superpočítač na světě má 160 tis. procesorů
- jak donutit tak velký systém řešit jednu úlohu?

CPU a operační paměť

- Stejné základní architektura a srovnatelný špičkový výkon od mobilu po superpočítač
- Rozdíly v reálně dosažitelném výkonu (napájení, chlazení)
- V současnosti téměř vždy více *jader*
  - zjednodušeně více (téměř) nezávislých procesorů na jednom čipu



- Paměť (RAM) jednotky GB až jednotky TB
  - jeden bit = jeden tranzistor
  - potřebuje napájení a pravidelnou obnovu
  - hierarchie: cena $=$ kapacita $\times$ rychlost

Datová úložiště

- tradiční rotační disky: $\sim$20 TB
- SSD: jednotky TB
- mobil: 16–64 GB SSD

- Apple TV 4k HDR $>$40 Mbit/s – 18 GB/h
- Netflix 4k HDR ve špičkách 20 Mbit/s, průměrně cca. 8 Mbit/s, 3.6 GB/h

Datová úložiště

- SSD – semiconductor storage device – jednotky TB
  - komplikovaná kvantová fyzika, náboj se „objeví“ na izolované části, kam by se „normálně“ vůbec neměl dostat, a zůstane tam i bez napájení
  - zařízení se díky tomu opotřebovává
- disky, magnetický princip – $\sim$20 TB

Datová úložiště

- RAID – Redundant Array of Inexpensive Disks
  (jednotky až desítky PB)
  - zvýšení rychlosti
  - snažší správa (jeden velký „disk“ místo desítek menších)
  - nezbytná ochrana proti selhání

Datová úložiště

- Páskové knihovny (více než 1 EB)

Datová úložiště

- Souborový systém – jednotky PB
  - hierarchie adresářů (složek), soubory v nich
  - složitější sekundární struktura – symbolické linky (zástupci)
  - k souborům lze přistupovat po částech
- Objektové úložiště
  - uloženy jsou pouze „objekty“ – kus dat nějaké velikosti
  - žádná hierarchie
  - někdy lze přiřazovat metadata („popisky“) a podle nich hledat
  - k objektům se přistupuje vcelku (uložit celý, stáhnout celý)

Síťové připojení

- EDGE 200 kbit/s, LTE (4G) 1 Gbit/s, 5G 0.4–4 Gbit/s
- WiFi 2 Mbit/s (802.11), 3.5 Gbit/s (802.11ac), 10 Gbit/s (802.11ax)
- kancelářský Ethernet 1 Gbit/s, serverový 10, 20 Gbit/s (100 Gbit se objevuje)
- Infiniband (lokální propojení serverů) 40 Gbit/s – 4.8 Tbit/s
- páteřní sítě (optické) běžně stovky Gbit/s, očekáváme Tbit/s

Akcelerátory

- specializované určení, výšší výkon, menší relativní spotřeba
- GPU nejen na grafiku, specializované, až 1000× výkonnější proti CPU
- podpora kódování zvuku a videa v mobilech
- Apple Neural Engine: teoreticky 10 GFLOP/s (1/3 NVIDIA 3090)
- ASIC pro těžbu kryptoměn: 1 000 000× výkonnější proti GPU

Fyzikální limity konstrukce počítačů

- Vzdálenost vs. rychlost světla
  - takt procesoru 3 GHz – 10 cm

Fyzikální limity konstrukce počítačů

- Vzdálenost vs. rychlost světla
  - takt procesoru 3 GHz – 10 cm
- Teplo a chlazení
  - až stovky wattů na jednom čipu

Fyzikální limity konstrukce počítačů

- Vzdálenost vs. rychlost světla
  - takt procesoru 3 GHz – 10 cm
- Teplo a chlazení
  - až stovky wattů na jednom čipu
- Velikost atomu
  - velikost tranzistoru – jednotky nm
  - vzdálenost mezi atomy – desetiny nm

Fyzikální limity konstrukce počítačů

- Vzdálenost vs. rychlost světla
  - takt procesoru 3 GHz – 10 cm
- Teplo a chlazení
  - až stovky wattů na jednom čipu
- Velikost atomu
  - velikost tranzistoru – jednotky nm
  - vzdálenost mezi atomy – desetiny nm
- Kosmické záření
  - https://asset-pdf.scinapse.io/prod/48011110/48011110.pdf
  - v jednom paměťovém čipu nastane chyba každé dva roky

Sdílená a distribuovaná paměť

- Výkon jednoho procesoru (jádra) už nelze příliš zvyšovat
- Celkový výkon navýšíme pouze spoluprací více (mnoha) procesorů

Sdílená a distribuovaná paměť

- Výkon jednoho procesoru (jádra) už nelze příliš zvyšovat
- Celkový výkon navýšíme pouze spoluprací více (mnoha) procesorů
- Skládání puzzle ve skupině
  - všichni vidí vše, mohou přispět kdekoli
  - omezený počet míst u stolu, soupeření o díly puzzle
  - nelze rozdělit mezi lidi předem

Sdílená a distribuovaná paměť

- Výkon jednoho procesoru (jádra) už nelze příliš zvyšovat
- Celkový výkon navýšíme pouze spoluprací více (mnoha) procesorů
- Skládání puzzle ve skupině
  - všichni vidí vše, mohou přispět kdekoli
  - omezený počet míst u stolu, soupeření o díly puzzle
  - nelze rozdělit mezi lidi předem
- Stavba stanového tábora
  - rozdělení materiálu a určení míst ke stavbě předem
  - poté samostatná práce s minimální synchronizací
  - s dostatkem lidí postavíme (téměř) libovolně velký tábor ve stejném čase

Superpočítače v ČR a ve světě

- 1995: první instalace na 5 VŠ v ČR
  - výkonem a kapacitou srovnatelné s dnešním mobilem
  - tři různé architektury, nic z toho současný Intel/AMD nebo ARM

Superpočítače v ČR a ve světě

- 2022 v ČR: Kar0l1na, superpočítačové centrum IT4Innovations
  - 800+ uzlů, 100 000+ jader, 576 akcelerátorů NVidia A100
  - 15 PFLOPS, 79. místo v TOP500

Superpočítače v ČR a ve světě

- Žebříček TOP500 `http://top500.org/`
- 1. Frontier, 136 409 uzlů, AMD EPYC + 4x MI250X, 1 686 PFLOPS
- 2. Fugaku, 158 976 uzlů, Fujitsu ARM, 537 PFLOPS
- 3. LUMI, 17 346 uzlů, AMD EPYC + 4x MI250X, 429 PFLOPS
- 4. Leonardo, 4 992 uzlů,Intel Xeon Platinum 8358 + NVidia A100, 304 PFLOPS
- 5. Summit, 4 600 uzlů, IBM Power9 + NVidia V100, 200 PFLOPS
- 7. Sunway TaihuLight - Sunway MPP, 126 PFLOPS

  ...
- 10. Tianhe-2A, Intel, 100 PFLOPS

Superpočítače v ČR a ve světě

- Žebříček TOP500 `http://top500.org/`
- 1. Frontier, 136 409 uzlů, AMD EPYC + 4x MI250X, 1 686 PFLOPS
- 2. Fugaku, 158 976 uzlů, Fujitsu ARM, 537 PFLOPS
- 3. LUMI, 17 346 uzlů, AMD EPYC + 4x MI250X, 429 PFLOPS
- 4. Leonardo, 4 992 uzlů,Intel Xeon Platinum 8358 + NVidia A100, 304 PFLOPS
- 5. Summit, 4 600 uzlů, IBM Power9 + NVidia V100, 200 PFLOPS
- 7. Sunway TaihuLight - Sunway MPP, 126 PFLOPS

  ...
- 10. Tianhe-2A, Intel, 100 PFLOPS
- Příklady aplikací (Fugaku)

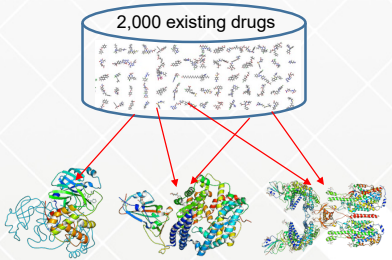
Fugaku

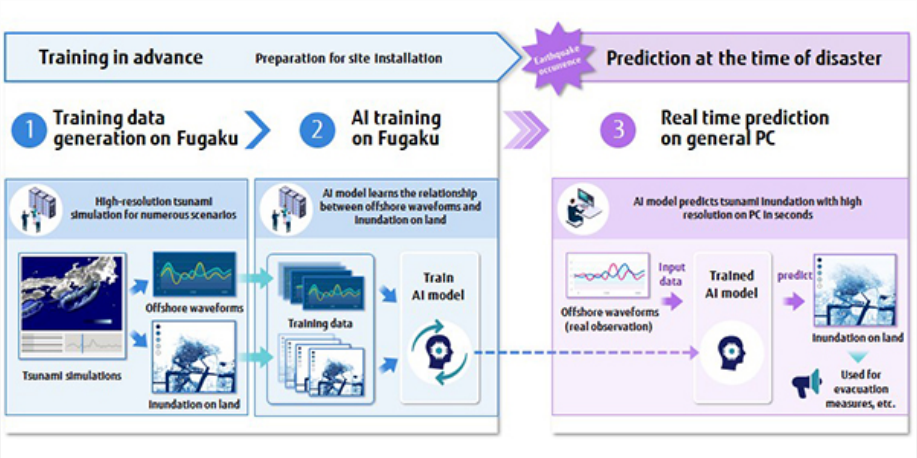
Exploring new drug candidates for COVID-19 by "Fugaku"

RIKEN / Kyoto University Yasushi OKUNO, Prof. PhD.

Research content:
Currently, clinical trials are underway in Japan and overseas to confirm the effects of existing drugs on COVID-19. Some reports have shown that the drug has shown efficacy through these clinical trials, but the number of cases has been small, and no effective therapeutic drug has yet been identified. Furthermore, due to the small number of drugs being tested, it is possible that none of the drugs have a definite effect.
Therefore, in this study, we performe molecular dynamics calculations using "Fugaku" to search and identify therapeutic drug candidates showing high affinity for the target proteins of COVID-19 from approximately 2,000 existing drugs that are not limited to existing antiviral drugs targeted in clinical trials.

Expected results:
- ✓ New therapeutic drug candidates other than those currently undergoing clinical trials can be discovered.
- ✓ Combination effects of multiple drugs can be estimated
- ✓ The molecular action mechanism of existing drugs currently undergoing clinical trials will be elucidated. In addition, these findings provide a clear direction for developing new drugs that go beyond the existing drugs.




Training in advance
Preparation for site installation
Earthquake occurrence
Prediction at the time of disaster
1 Training data generation on Fugaku
2 AI training on Fugaku
3 Real time prediction on general PC
High-resolution tsunami simulation for numerous scenarios
Tsunami simulations
Offshore waveforms
Inundation on land
AI model learns the relationship between offshore waveforms and inundation on land
Training data
Train AI model
AI model predicts tsunami inundation with high resolution on PC in seconds
Offshore waveforms (real observation)
Input data
Trained AI model
predict
Inundation on land
Used for evacuation measures, etc.

Co je to ten cloud?

- Počítače někde jinde, které patří někomu jinému
  - ten je koupil, platí elektřinu a péči o ně
  - služby „zdarma“ se mu musí nějakým způsobem vyplácet
- Analogie banky
  - jednomu konkrétnímu uživateli se kapacita cloudu jeví neomezená
- Úroveň abstrakce služby vhodná pro koncového uživatele
  - neřeší kam uložit video, v jakém kódování, jakým programem ho přehrát, …
- Nalezení správného modelu na začátku 21. století přispělo k masovému rozšíření IT

Co je to ten cloud?

- Historická synergie trendů:
  - virtualizace (technický)
  - „grid“ vedle superpočítačů (politický)
  - nadbytečná kapacita (finanční)

Co je to ten cloud?

- Historická synergie trendů:
  - virtualizace (technický)
  - „grid“ vedle superpočítačů (politický)
  - nadbytečná kapacita (finanční)
- Služby pro koncové uživatele
  - Facebook, Google, Microsoft, …
- Služby pro „experty“
  - Infrastructure/Platform/Software as a Service
- Obchodní modely
  - zdarma s reklamou, drobný poplatek (Apple), full-cost (Amazon)

Bez křemíku

- Křemík je snadno dostupný a snadno zpracovatelný; proto převládá
- Alternativní polovodiče (GaN, BAs, …)
  - o něco lepší vlastnosti (rychlost, teplo, …), náročnější zpracování
- Grafenové nanotrubičky
  - „dobrá“ kontrola nad vlastnostmi materiálu, potenciálně menší, efektivnější, …
- Molekulární „obvody“
  - malé i větší organické molekuly, reakce na chemický podnět (ion, pH, …)
- DNA
  - problém zakódován do sekvence DNA, masivně paralelní „výpočet“

Kvantové počítače

- Elementární jednotkou klasického počítače je **bit**
  - 1 bit má hodnotu 0 nebo 1
  - „slovo“ velikosti n bitů reprezentuje jedno číslo $0–2^n$
  - ke zpracování takového slova je třeba jednotka velikosti n
- Mnoho zajímavých problému vyžaduje 2^n operací
  - pro větší n už je to moc – zásadní **limit použitelnosti** klasických počítačů

Kvantové počítače

- Elementární jednotkou klasického počítače je **bit**
  - 1 bit má hodnotu 0 nebo 1
  - „slovo“ velikosti n bitů reprezentuje jedno číslo $0–2^n$
  - ke zpracování takového slova je třeba jednotka velikosti n
- Mnoho zajímavých problému vyžaduje 2^n operací
  - pro větší n už je to moc – zásadní **limit použitelnosti** klasických počítačů
- Jeden příklad za všechny: autorizace bankovní transakce
  - se znalostí klíče (velikosti např. $n = 2048$) stačí k ověření transakce vykonat kn operací (s rozumně malým k)
  - aby se za vás útočník mohl vydávat, musel by provést 2^n operací, a to už je nezvladatelné
  - tak jsou záměrně stavěné šifrovací algoritmy

Kvantové počítače

- Kvantovou fyzikou inspirovaný teoretický koncept
  - potenciálně velmi zajímavé schopnosti
  - spolehlivou technickou realizaci ještě nemáme, není nemyslitelná

Kvantové počítače

- Kvantovou fyzikou inspirovaný teoretický koncept
  - potenciálně velmi zajímavé schopnosti
  - spolehlivou technickou realizaci ještě nemáme, není nemyslitelná
- Jednotkou kvantového počítače je **qubit**
  - qubit má hodnotu „něco mezi 0 a 1“

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{kde } \alpha, \beta \text{ jsou komplexní}$$

  - k popisu stavu qubitu potřebujeme dvě čísla
  - $|\alpha|^2$ je pravděpodobnost, že pozorováním ψ zjistím 0

Kvantové počítače

- Skládání stavů více qubitů je komplikovanější, k popisu stavu n qubitů je třeba 2^n čísel

$$|\psi_1\psi_2\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- Na zpracování 2^n čísel současně stačí kvantový počítač velikosti n
  - při troše štěstí, není to tak jednoduché
  - zejména je problém takový algoritmus naformulovat

Kvantové počítače

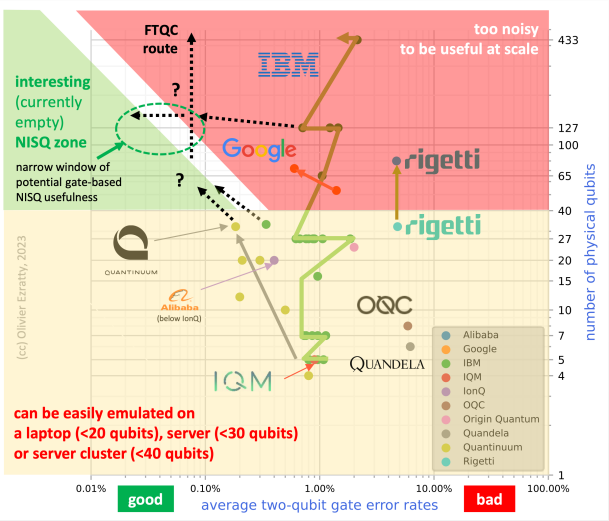
- Skládání stavů více qubitů je komplikovanější, k popisu stavu n qubitů je třeba 2^n čísel

$$|\psi_1\psi_2\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- Na zpracování 2^n čísel současně stačí kvantový počítač velikosti n
  - při troše štěstí, není to tak jednoduché
  - zejména je problém takový algoritmus naformulovat
- Kvantové počítače mají teoretickou schopnost řešit exponenciální algoritmy
  - spousty užitečných aplikací
  - a také likvidace elektronického bankovnictví (a jiné …)
- `https://doi.org/10.58729/1941-6679.1410`

Kvantové počítače

Technická realita



https://arxiv.org/ftp/arxiv/papers/2305/2305.09518.pdf

Shrnutí

- Úložná kapacita, přenosová rychlost sítí, a výpočetní výkon v posledních dekádách narostly enormně
- Zpracování velkého objemu dat a rozsáhlé výpočetní simulace pronikají do většiny odvětví lidské činnosti
- Zejména cloudové modely použití (to hlavní se děje „někde jinde“) přispěly k masovému rozšíření
- To vytváří tlak na další růst výkonu
- Výkon jednoho počítače naráží na fyzikální limity, musí se řešit „chytřeji“ (spoluprací), případně radikální změnou technologie