The Dark Secret at the Heart of AI

Thursday, May 25, 2017 2:04 PM

- Applications
  - Siri, Google Assistant
  - Object classifications in photograph: i.e. Google Lens
  - Self-driving cars
- Neural Network
  - Shape, color, features to tell certain things
  - The more complex the image is: the harder for developer to tell why program created the certain output
- NVIDIA's Self Driving Cars
  - Does not follow any instructions
  - Learns how to drive by looking at how normal people drive everyday
  - Concerns: not sure how car made decision
    - what if one day it makes a bad decision: stops somewhere
    - Neural network so complicated
- AI on Medical Field
  - Mount Sinai Hospital, New York
  - Trained using 700,00 indiv data
  - Better than existing methods
  - Works well on predicting psychiatric disorders

Universal Perturbations

Thursday, May 25, 2017 2:12 PM

- Background: Deep Machine Learning
  - Like human brain
  - Translate data through layers and make a decision
  - Like when you show someone a pic they know what it is
- Univ. Pert.
  - Modifies an image but humans can't tell
  - Adds noise so machines can't tell --> wrong decision in telling what it is
  - Can train machines to tell its wrong but still gets it wrong majority
    - independent of neural network and image chosen
- Reasons
  - Decision Boundaries: decision A on left decision B on right
  - Applications
    - being anonymous in connected society
    - Hacking: potential application to semantic segmentation
- Applications:
  - face paint: but can tell
  - tshirts: not overt but it can work
  - Semantic Segmentations: hacking
    - use UP to remove all people from image
- What is the future?
  - Security issues
  - Maintaining privacy

VR Games for Rehabilitation of Stroke Patients

Thursday, May 25, 2017 2:23 PM

- 800,000 people in US have strokes
    - result from clots that stop blood from flowing to part of the brain
- Disabilities and Rehabilitation
    - Speech therapy
    - Physical
        - Hemiparesis - paralysis of half of your body
    - Occupation therapy
        - Daily activities
- How VR Devices Work
    - Rehab req consistant exercises (cerebral plasticity)
- Ex. Become a Dolphin
    - John Krakaur
    - Study app that relies on non task based tasks
    - Similar to hungry shots but played with robotic arm
    - Advantages
        - Stroke patients learning ABCs in new enviornment --> explore new movement and not hindered by thoughts
        - Natural tendency for storke patients to use limbs that were unaffected but now forced to use affected limbs
- How effective
    - Ping pong game
        - After 10 hours of training - patient has more improvement
        - Show improvement in functional skills
    - Types of VR Devices
        - UCLA uses xbox Kinect, mech arm
- Commercialization
    - Tej Tadi -> Mind Maze
    - Develop hardware and software platform that create human Vr

Splinter: New System for

Thursday, May 25, 2017 2:33 PM

- Database queries: reveal info about users who make them (metadata)
  - Ip, and other stuff
- Problems
  - Websites can take advantage of consumers with info they receive (Airlines)
    - Or patents, and other stuff
  - User queries can be leaked both intentionally (google or Facebook) or accident (AOL)
  - Can Hide using Tor: requires trust and they don't protect against leaks
- Splinter
  - New Encryption that disguises uq
  - Better to work with TOR not just by itself
- Works
  - Splits query up and distributes across copies of the same database on multiple servers
    - At least one that can be trusted
- Competitors
  - Generlaly not acieved performances because they use expensive primitives and protocals
- Secret Sharing
  - 10x faster for disguising database queries in past
  - DQ conver into set of cmplemntary math functions
    - Each server

My Project

Saturday, May 27, 2017 10:07 AM

- Overview
  - Mobile Payments: Apple and Android Pay
    - Available for everything from gas to groceries to restaurants
  - Slow adoption rate in UK -> security concerns and fear of theft
    - This focuses on the security concern
- Security concern
  - "Eavesdropping"
    - Very similar to what humans do when listening to other people's conversation
      - This is where hackers intercept the data sent by consumers and know what is being transmitted
  - Android and Apple Pay both use NFC
    - NFC inherently cannot protect itself against eavesdropping
      - There are some add ons that help provide security such as establishing a secure channel using a symmetric key like 3DES or AES
      - Hackers though can still get in if they know the key
  - Can't detect eavesdropping
- Solution
  - Quantum technolgy: Oxford University collaboration, including Dr. Iris Choi, along wigh Nokia and Bay Photonics
  - sends mlions of single particles of light to send encryption keys
    - Can detect activities like eavesdropping and shut down the system to prevent hacking
- How it works
  - Usses moveable mirrors and ultrafast LEDs to send a secret pin-code at rate of 30 kb.s
  - 6 pairs of LEDS that are polarized differently and at different positions
    - The circularly polarized LED is the main key
    - Others used to check the security and correct any errors in transmission
- How does it provide greater secuity

    - Quantum key is long: preents hackers from figuring out the key pattern randomly
    - Innovative Steering system: prevents hackers from cracking code
        - The lights have to go at an exact position - even if they get moved a little bit the system fails
        - If hacker gets the code, they alter the quantum signal and makes the code now unusable
    - Humans have natural motion in their hand even when completely still
        - Research team found the exact measurements of this movement first
        - Used to optimise the design of the steering system
- Prototype
    - Handheld
    - Constructed using ordinary materials rather than custom
- Future
    - System can be shrunk down and become a part in the phone
        - As with most technologies: it is very difficult to do this and still have it work the same as the prototypes
        - Also be used for secure connections for NFC and Wifi networks
    - Higher adoption rate for mobile payments and increased public trust

[2] Apple Pay security and privacy overview: 2017. https://support.apple.com/en-us/HT203027. Accessed: 2017-05-29.

VR Techniques

Tuesday, May 30, 2017 2:00 PM

- Visual auditory and tactile methods
- Visual
    - Users use a headwt to receive the display - use convex lens
    - Problems: Display Lagging
        - Difference between motion of users head and the display in the headset
        - If lag is longer than 20 ms there will be dizziness
    - How to reduce lag
        - Time-crit computing: trades computation time for accuracy
        - Multi processor to parellize
- Auditory
    - Need convincing sound - 3d audio formats
    - Multichannel
        - Loud speakers
        - Each channel is one speaker
        - Sound created by mixing the channels
        - More channels more spacing
    - Object
        - Sound is made by mixing the sound softs?
    - Ambisonics
        - Doesn’t rely on speakers or objects
        - Covers sound sources above and below listener
        - Most VR uses it
- Tactile
    - Hand controller
        - Two cameras that capture the diameter of ball
        - Can track motion of ball
        - PS move
    - Gloves
        - Detect a person's presence
        - Record motion of fingers
        - More pressure changes the resistance

        more pressure changes the resistance

- Conclusion
    - Ethical: desensitation
        - Personn no longer affected by extreme acts of behavior or uncompassion
- Future Guess
    - Make a dynamic floor that changes the landform based on player's legs
    - No longer rely on buttons

Predict Supreme Court Decisions: Machine Learning

Tuesday, May 30, 2017 2:21 PM

- SCOTUS
    - Appeals form lower cours
        - Writs of certiori (certs)
    - Original jurisdiction: sue federal gov
- To Predict
    - Use previous cases, public opinion
- Previous Research
    - Generality: create models for 1 set of 9 justices
        - Can't apply to more than 1 set
    - Consistency
        - Doesn't work for diff time periods
    - Out of sample applicability
        - If they try to add in new justice: data screwed up
- Feature Engineering
    - Take qualitivie features
    - Case and behavioral features
        - Case: issue, reason for cert
        - Turn into 13 different variables
    - Feature Binary encoding: cert ==> 13 indicator variables
    - Feature extraction or generation/extraction
        - Coarsen or collapse
        - Arithmethicallu derived fuatres
- Modeling
    - Training feature set is matrix D_T
        - Rows docket votes
        - Column: featrues
- Learning Algorithm
    - Random forest clasification
        - Subsets of Decision trees
        - Create a whole bunch of decisions and generate average decision
        - Many weak learners => strong learners
        - Forest of statitically diverse decision trees

        - Forest of statitically diverse decision trees
    - Growing Forest
        - Fresh forest (Accuracy) vs growing (effieency)
        - Natuaral court change => retrain all trees or some
        - 5 new trees per term
- Results
    - Baseloin/null models
        - Optimized finite memory (M=10)
            - Last 10 years and look at court reversals
        - Infinite memeory
        - Always guess reverse
    - Leveles of Predition
        - Left case 71.9%
        - Right: justince 70.2%
- Implications
    - "Court observors, litigants, citizens and markets"
    - Baseline model
    - Any application of predictive analytics
    - Matters to big companies: know if they can win
        - Profits are on the line

AlphaGo Defeats Chinese Go Master

Tuesday, May 30, 2017 2:36 PM

- What is AlphaGO
    - AI program developed by Google DeepMind in London
    - Surround a larger total area of the board han the opponet
        - More complex than chess: innumerour more possibilities
- How does it Work
    - Monte Carlo tree search: finds moves based on knowledge previously learned by machine learnong (deep learning)
    - Based on playouts: select moves at random and assigns weights to the moves on nodes of treee
    1. Section: cjppsog cjold nodes hat let tree expand towards most promising moves
    2. Expansion: Unless game ends, create additional child nodes
    3. Simulation: play random playout from specific node
    4. Back propagation: use rsult to update information in node on current path
- How is it diffierent
    - Previous AI was Deep Blue- designed for chess
        - Deep Blue worked in more traditional manner -> consider all possible moves
    - Alpha Go aplies to neural network where evaluation heuristics are not hard coded by humnas but are learned through past Go matches and matches played against itself
    - Not even developer teamm is capable of pointing out next move
- Results
    - First tested AlphaGo against Lee Sedol, Korean
        - One of the bes in world
        - Beat him 4 games to 1
    - Second test Ke Jie, Chinese National go player
        - AG won first game
- Lessons/Applications
    - Can develop software that perform better than humans can
        - i.e self driving car, legal documents
    - Consider milesone towards creating human-level AO softwar

        - Creat machines with humanlike capabilities
- Possibility: AI takeover
    - AI becomes too smart and humans will be under their control
- What's next
    - Start prep for genral purpose intelligent machines
    - Companies: like Facebook and DeepZenGo are working on developing AI algorithms

Internet of Things: Smart Cities

Thursday, June 1, 2017 2:03 PM

- Internetworking of physical deices with sensors, softwate and network coenecivty to allow devices to talk to each other
- Overview
    - Smart City: Urban development vission to integrate IOT in a secure fashion to managw a city's assent
    - Goals:
        - Make bettr use of public resources
        - Increase quality of services to citizens
        - Reduce operating cost
    - 100 million market
- Current Implementations
    - Smart Governance: noise management
    - Mobility: traffic
    - Waste Management
        - Detect when they are full and optimize collection route
        - Reduce cost of waste collection and improves recycling quality
    - Noise monitoring
        - Having microphones that can tell law enforcement if someplace is too louad
        - Offers promise in recognizing glass crashes, gunshots, and fights in public places
            - Allows for automation of police dispatc
    - Traffic congestion
        - Reads cellphone location data to sense wwhere cars are and give realtime traffic data
        - Allows city planners to intelligently plan out routes
    - Architecture
        - IOT as Web Services
            - Representational State TranswferVery simila to traditional web sevices
        - Transport layers: HTTP/TCP too complex
        - Use COAP

- Link Layer
  - Wifi, Ethernet, Fiber optic are overkill
  - More suitable: Bluetotth, IEEE 802.11 low power, PLC, NFC, RFID
- Backend
  - Servers aren't necessary in principle
    - Fundamental for urban though" facilitate access and open data
  - Database management systems
    - Store info produces by IOT peripheral nodes
    - As sensors/info scale, databases must be able to scale their storage

- Case Study: Padova Smart City
  - Uni of Padova and Patavina Tech partnership
  - Current system
    - Monitor enviornmental parameters
    - Control street lights and feed inforation to admins
    - Need to use ipV6: handles billions and billons of devices
- What's Next
  - More widespread rollout of IOT
  - More intelligent neural networks to interpret data
  - Bigger database

CS 35L Final Review

Tuesday, June 6, 2017 1:59 PM

- Tips
    - Only focus on the slides and the assignments
    - Print some supplement materials, especially cheat sheers
- Week 1 Basic Concepts
        - History of OS
    - Components of Linux
        - Kernel: know the 4 main function
            - Core of operating sstems
            - Allocates
    - Know the functions, usage, options of command line utilities'
- How do I find where files are on systems
    - find
- When is a file a file and when is it a process
    - ps
- Absolute vs Relative Path
    - Absolute: start at root and relative is whatever point you define
- Sample W: CHMOD hello
- ^\(?[2-9][0-9]{2}\)?(|-|\.)[0-9]{3}(|-|\.)[0-9]{4}
    - ^ : occurs at beginning of line
    - {2}: there has to be 2 instances of [0-9]
    - (|-|\.) : Delimiter can be none, -, .
- Build Process
    - Configure
        - Check if environment is compatible or not
    - Make
    - Make install

Git

Head: pointer specifies which branch you are working on
Git init: initalize empty repository and creates .git
Git clone: initialize repo but is filled with existing git

Git status, git diff answer to Week 9 Q1

Git status, git diff answer to Week 3 Q1
PART 2
Diff thread share a heap and different stack

Malloc: initialize
Realloc: deallocate og memory and reallcate new data,
Calloc: initialzed to memory: I.e int* to 0
Free: frees the memory

Malloc() and free

Int** arr = malloc(sizeof(int*) *100);

Iterate through array of pointers and allocate 200 times size of int for element of array pointers

To free: for loop - free inner parts then int**

Don't have access to array element if you get rid of array

Can get segmentation fault: dereference a null pointer, use memory that doesn't exist, go out of array index

Week 4 sample Q:
A,B,C

Week 5 sample Q
Fopen is library (buffered io), open is system
Trap is only used in the beginning
Library function make less system calls compared to system calls alone

Time
Real: actual time on wall
User: CPU time spent in user mode
Sys: CPU spent in kernel mode

Sys+user should = Real

Digital signature: check integrity
Encryption: only targted person can read it

sed 's/[^0-9]*//g'	delete non numbers
sed -i 's/ //g'	delete leading blank space
sed 's/[[:blank:]]*$//'	delete trailing whitespace
sed -r 's/\s+//g'	remove all white space
tr -d '\n'	remove new lines
sed '/^$/d'	Remove empty lines
sed 's/[^0-9]*//g'	remove non numbers

Common Sed Commands

Sunday, June 11, 2017 8:46 PM

tr -c 'A-Za-z' '[\n*]' < assign2.html : After running this, all non all non letter characters were replaced with a new line. So, if there are multiple non letter characters in a row then there will be multiple new lines.

tr -cs 'A-Za-z' '[\n*]' < assign2.html : After running this command, it outputs a similar to the previous command except that if there are multiple non letter characters in a row, they are replaced with only one new line. There is no blank lines between lines with text.

tr -cs 'A-Za-z' '[\n*]' < assign2.html | sort : The output of this command has the same characteristics of the previous command, but now the output is sorted alphabetically. I initially put < assign2.html at the end, but the terminal somewhat froze and I had to use C-c to exit. Putting it before piping to sort fixed the issue.

tr -cs 'A-Za-z' '[\n*]' < assign2.html | sort -u : This outputted the same result as the previous command, but using the -u option removed any duplicate words that are spelled using the same characters. If, there are different characters used to spell the same word they are kept. For example, for all, All, and ALL, none of the words are deleted, but if it was all, all, and all, only one of the all words is kept.

tr -cs 'A-Za-z' '[\n*]' < assign2.html | sort -u | comm - words : This command outputs 3 columns.

The first column outputs the words that only appear in assign2.html. The second outputs the words that only appear in words, and the third column outputs the words that are in both files.

tr -cs 'A-Za-z' '[\n*]' < assign2.html | sort -u | comm -23 - words : This command outputs only the words that are unique to assign2.html. the -23 in the comm command suppresses the 2nd and 3rd columns, so they are not shown.

grep '<td>.*</td>' $1 | : This command searches for all the lines containing the English and Hawaiian words. These are between <td> and </td>. Initially, I did not put the . before the * and only lines that were <td></td> were outputted. Adding the * fixed it. The $1 is the file passed in to be changed.

sed 's/<[^>]>//g' | : This command deletes all the HTML tags from the text.

sed "s/\`/\'/g" | : This command replaces the okina with a comma. When trying to come up with the command, the " were initially ', but this caused the terminal to no longer let me enter commands. Also, I initially did not put \`. It did not have the \ before the `, causing the terminal to again freeze up.

sed 's/^ *//g' | : This command deletes all the leading spaces for each line. Initially, I used sed 's/^\t*//g' to delete the spaces since I thought it was a tab rather than just a space. Also, I thought if I added [] around the \t it would work, but it did not either. Thus, I just had the command look for a space at the beginning of the line and delete it.

sed 's/[,[:space:]]/\n/g' | : This command finds all the commas and spaces and changes them to new lines. This allows the words separated by a comma or space to be treated as multiple words. Initially, I used [,\s], but it would replace some spaces with newlines and it would not for others. Making it [,[:space:]] allowed the command to work.

sed '/^\s*$/d' | : This command gets rid of all the empty lines sed '/^\s*$/d' | : This command gets rid of all the empty lines. Initially, I used the command, sed 's/^\s*$//g' and nothing happened. It seemed to replace the empty line with another empty line. By using the delete function with d, the empty lines were replaced.

tr '[:upper:]' '[:lower:]' | : This changes the uppercase letters into lowercase letters

sed "/[^pk'mnwlhaeiou]/d" | : This deletes any line that does not contain the Hawaiian letters. The ^ inside the brackets makes it so the sed command deletes the characters that are not in the set listed.

sort -u : This sorts the word list alphabetically and removes duplicates. Then, it saves the output into hwords.