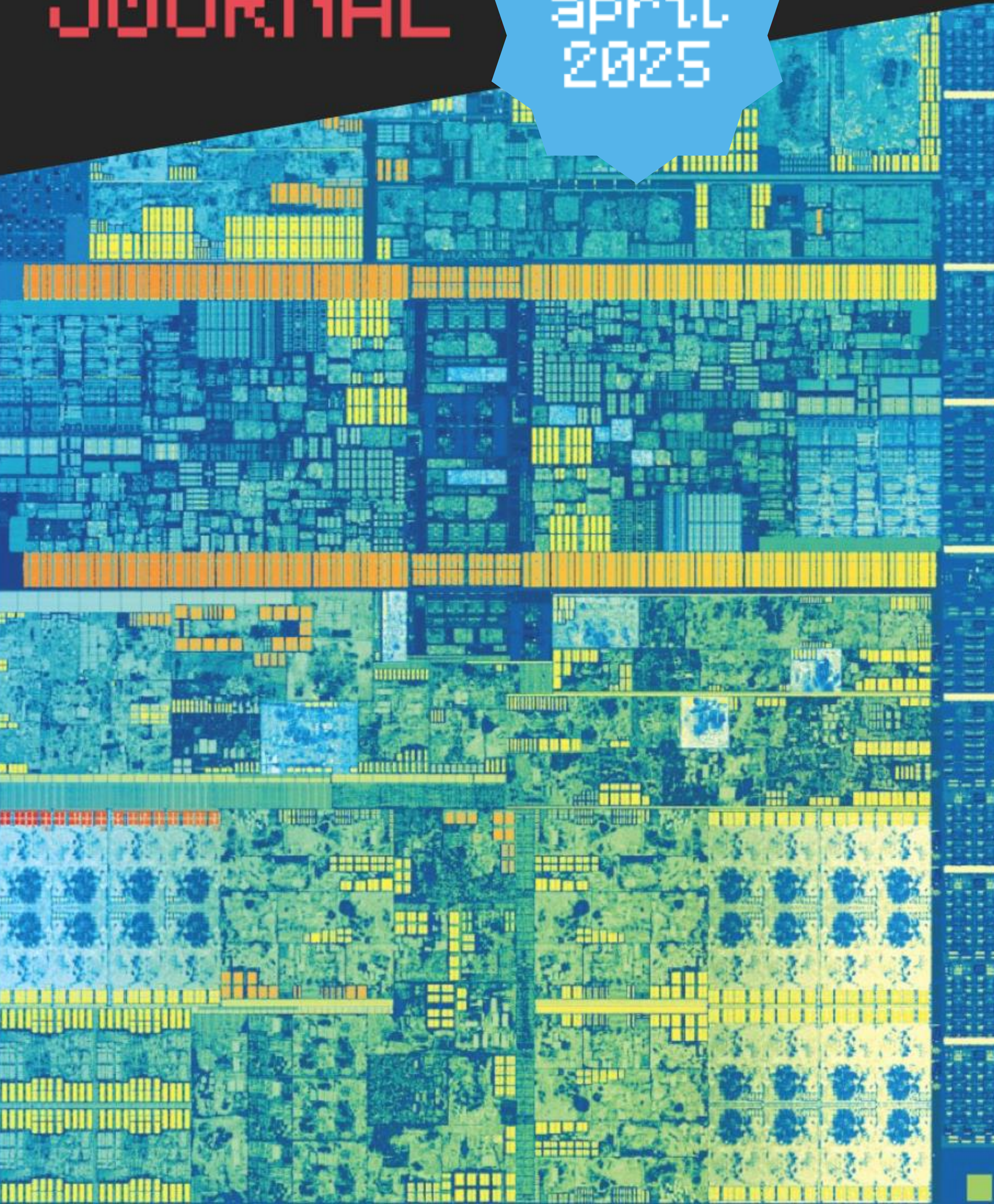
COMPUTER SCIENCE JOURNAL

april 2025



Contents

Editor's Note

After a long wait, we are proud to finally present the completed April 2025 edition of Newstead's Computer Science Journal, featuring contributions from students throughout the school looking at a variety of fields and ideas in computer science.

The journal has a total of 28 articles to offer, discussing a wide range of topics such as the benefits and disadvantages of AI, the latest advancements in quantum computing, the applications of computer science in various fields and much more. With so many articles, there's something for everyone to read and learn from. There are also several puzzles scattered throughout the journal for you to find and attempt to solve.

The front and back covers of the journal feature die shots of two different CPU cores from Intel – Kaby Lake and Penryn. The images of these cores and many others can be found on https://happytrees.org/dieshots/Main_Page. The backgrounds for each article were made using a dithering filter from https://doodad.dev/dither-me-this/.

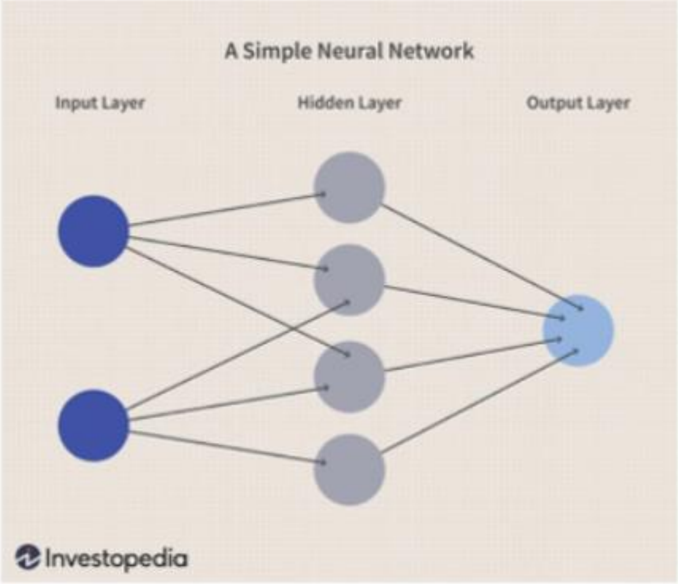
Thank you to everyone who contributed. We hope you enjoy reading the journal!
The Journal Editors –
Nithika and Leo

Neural Networks in Machine Learning

By Anna

Over the past few years, Artificial Intelligence (AI) has been an integral part of everyday life for most people. From smart speakers to chatbots, AI aids people all over the world. That brings the inevitable question, how does AI learn? The answer to this is that there are many ways, but one of the most common methods is by using artificial neural networks, a complex system that models the human brain to do various tasks. This article will explore what a neural network is and some of their various uses.

How does a Neural Network work?



Neural networks are made up of nodes/neurons that are organised into 3 main layers:

The input layer - This layer can take any input value, as long as it can be represented numerically. Videos, photos and text are a few examples of valid inputs.

Hidden layers – These layers do a large number of calculations, based on certain features of the input to determine what the input is.

The output layer – This is where a prediction is outputted, based on the calculations from the hidden layers. The output can be in various forms such as a probability from 0-1 or the binary 1 or 0.

The neural network goes through iterations to adjust the weights of certain nodes so that there is a more accurate final classification. This is commonly done via a process called backpropagation, where the algorithm goes back through itself to calculate the loss (the difference between the prediction and target), then adjusts the weights for the optimum output.

Example: Hand-drawn Digit Recognition

This image is part of a set of 10,000 hand-drawn digits made for digit recognition by MNIST. While the human brain can easily recognise this as the number 8, a computer cannot, so researchers can use this training data to test a neural network made for digit recognition. Ideally the neural network would have these layers:

The input layer –The input is the 28x28 pixel image. The computer only sees a numerical value for each pixel, based on the greyscale value, and this would make up the 784 input neurons.

Hidden layers - The hidden layers would include nodes that break down the number into distinct shapes and lines and determine the number of certain shapes such as circles. These nodes would “fire” when a certain threshold has been met (e.g. at least 2 circles) and this determines what nodes in the next layer will be fired and ultimately decides the final output. These thresholds are changed by the weights and through iteration the computer decides the best weight for the most accurate result.

The output layer - This would output what number the drawing is most likely to be.

Uses of Neural Networks

Finance - Neural Networks are commonly used in financial predictions for stock rates. They are particularly good at this as they can adapt to the changing stock-market. They are also used to detect fraudulent purchases by finding anomalies in purchase history.

Healthcare - Neural Networks have been used in healthcare for several decades. They can be used to recognise patterns indicating disease in various aspects of healthcare including blood tests, MRI scans and X-Rays. This level of precision is difficult to achieve by a human and reduces diagnosing times.

The Good and Harm of Artificial Intelligence: A Double-Edged Sword

By Ruth

Artificial Intelligence (AI) has arguably greatly transformed the globe at a probably higher velocity than any other innovation in recent times: changing industries, optimising efficiency, but upsetting daily life. AI enables an optimised self-driving car or even complicated medical diagnoses to solve the very abstract problem whose solution eludes human beings-enlarging their capabilities. But the higher values incurred confront extreme cases for job displacements, privacy issues, and ethical concerns. As the technology progresses, should people be able to develop at all the advantages of the change and consider the likelihood of these disadvantages concerning artificial intelligence?

One of the significant advantages of AI is its ability to increase productivity and efficiency. Through AI, the industry can get involved in activities that require less human intervention, such as financial, manufacturing, and customer service tasks, for example, which then reduces the human workload while reducing errors. Medicine: it can help with the diagnosis of diseases as well as predicting outcomes for patients while also performing robotic surgery. This reduces the time taken; diminishes the overhead; and improves the quality of life.

It performs an incredibly significant role-ensure safety. The state-of-the-art in artificial intelligence approach to cybersecurity is composed of platform-independent, real-time threat identification and neutralisation: citizens are better protected, and businesses safeguarded. It ensures that the technology behind autonomous vehicles will make road travel safer by reducing errors which otherwise might be caused by human factors. In fact, AI is also used in the prediction of disasters and climate science, allowing scientists to fight such global ills, including climate change and natural calamities.

AI brings about challenges that are gargantuan. The real problem is there are many lower hanging fruits-job displacement by labour, where robots substitute human labour in various industries. However, there could be a challenge in adopting it-age old habits die hard-which may lead to the economic inequality since AI would also tend to create new opportunities that may be challenging for some labour force to adapt. Other than that, AI algorithms learn biases from data, like pregnancy or dark skin-tones, which are already incorporated into their learning testified by the training data.

The Rise of Quantum Computing

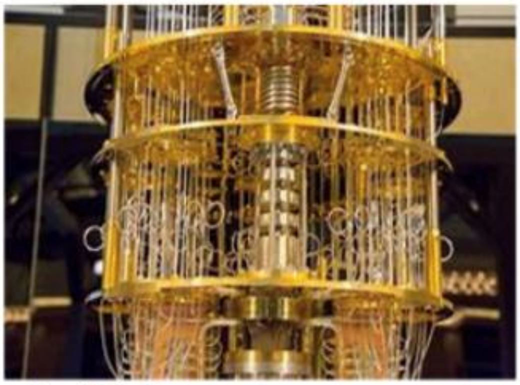
By Mannat

Computer science is pushing the limits of what we currently have, since what started as simple mechanical calculators quickly evolved into the supercomputers we can't live without today. Now, a new technology known as quantum computing is about to change the way we think about solving problems. Quantum computers, unlike normal computers, apply the strange, theoretical rules of quantum mechanics to solve problems beyond the capabilities of current systems. Outcomes of this ground-breaking tech could even have a noticeable impact on sectors such as cryptography or medicine.

What is quantum computing?

Quantum computing is a field of computer science (still in development) that would be able to solve complex problems that even modern supercomputers aren't able to solve and solve them much faster. The reason for this is that quantum computers use qubits (quantum bits) instead of bits, made from some of the smallest parts of the physical universe, like photons and electrons.

Developments in quantum computing

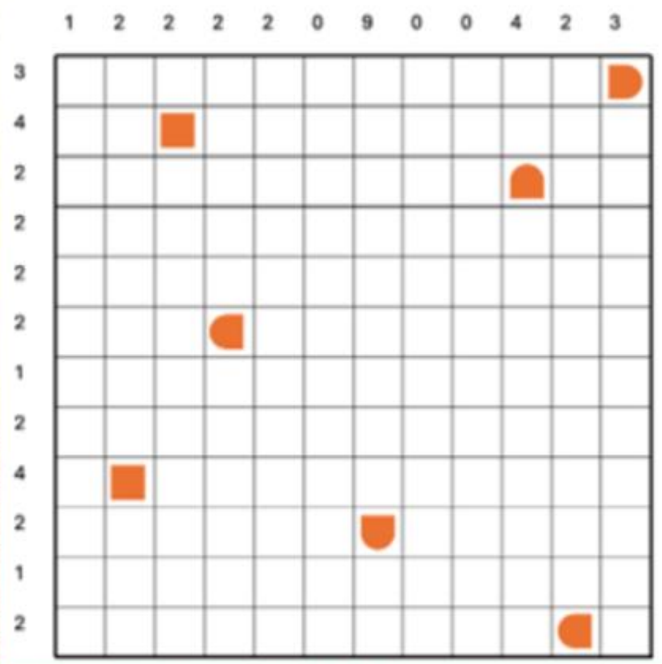


An IBM quantum computer (London)

The quantum realm is extremely difficult to make use of; quantum chips can often degrade information very quickly if not transported correctly and must be stored in freezing temperatures. This means that, although scientists and engineers have attempted to develop complex quantum computers for over 20 years, it has been extraordinarily difficult to create something more than a quantum computer with simple microchips. However, in the last decade, new information has been discovered that could help create these machines.

Prof Hensinger's team at the Sussex Centre of Quantum Computing made a breakthrough – finding a method to transfer information between quantum chips with a reliability of 99.999993%, at record speed. This is incredibly important as it shows that complex quantum computers *can* be achieved – if enough quantum chips are slotted together, extremely powerful supercomputers could be made. The only problem now is engineering – being able to scale up these machines to a size where they can quickly do realistic, useful calculations is incredibly hard to engineer, especially with the volatile nature of the chips. Despite this, the potential for quantum computing is exciting and immense – it could simulate chemical reactions almost instantly, designing new, useful drugs, or be used in encrypting data worldwide. The barriers for creating practical quantum computers are nearly all down – it is finally feasible.

Puzzle #1 - Battleship Solitaire



Battleship solitaire is a variation on the original guessing game of Battleship. It was first created in Argentina by Jaime Poniachik. The puzzle consists of a grid with numbers along two sides of it. Each number indicates how many parts of a ship are in that particular row/column. The length and number of boats in the grid are also given. This specific grid was made from https://lukerissacher.com/battleships.

The Role of Computer Science in Engineering

By Olivia

The incorporation of computer science into engineering has completely changed the way engineers are now designing, analysing, and manufacturing. Engineering and computer science have now become inseparable with the computing technologies which are improving the design simulation, automation, and optimization across the multiple types of engineering, such as, mechanical, electrical, civil, or biomedical engineering. It plays a crucial role in improving efficiency, accuracy, and problem-solving capabilities.

Computer-Aided Design (CAD) and Computer-Aided Engineering (CAE):

Computer-aided design (CAD) and computer-aided engineering (CAE) are essential nowadays for modelling, simulating, and optimising engineering designs. These software tools can enable engineers to visualise prototypes before production, reducing the risk of costly errors.

CAD's individual function is to create digital blueprints and 3D models of products, including details like dimensions and shapes, using tools like sketching, extruding, and revolving. Whereas the function of CAE is to take a CAD model and perform simulations to evaluate its performance under different conditions, like stress analysis, fluid flow, heat transfer, and vibration, to identify potential design flaws before manufacturing.

Each division of engineering has different uses for CAD and CAE. Mechanical engineering uses it to design machine components, engines, turbines, and industrial tools. In civil engineering, architects and engineers use CAD for designing bridges, motorways, and buildings. Electrical engineers use it to design electrical circuits, microchips, and PCB layouts.

So, the main impacts of using CAD and CAE are increased precision in complex engineering designs, reducing prototyping costs by allowing virtual testing and the acceleration of product development cycles.

Popular software for CAD and CAE:

CAD: AutoCAD, SolidWorks, CATIA, Fusion 360. CAE: ANSYS, Abaqus, COMSOL Multiphysics

Artificial Intelligence (AI) and Machine Learning (ML) in Engineering:

In engineering, AI and machine learning are mainly used to analyse large datasets from sensors and simulations, enabling predictive maintenance, design optimisation, quality control, and process automation. This helps engineers to make better decisions by identifying patterns and predicting potential issues before they occur, ultimately improving efficiency and reducing costs through the engineering lifecycle.

The key application of AI and ML are predictive maintenance, design optimisation, quality control, process automation, simulation and analysis, but what do these actually mean. Predictive maintenance could be analysing data from machines to predict potential failures or optimising maintenance schedules, minimising downtime and maximising equipment lifespan. Design optimisation is using algorithms to explore vast design spaces and identify the optimal parameters for a product, leading to improved performance and efficiency. Quality control is analysing data from production lines to identify defects and inconsistencies in real-time, ensuring product quality. Process automation is automating repetitive tasks in manufacturing processes through machine learning models that can learn from data and adapt to changing conditions. Simulation and analysis includes using AI to sun complex simulation and analysing large datasets faster to aid in making better decisions.

The benefits of using AI and ML in engineering are the increased efficiency which comes from automating repetitive tasks and optimising processes, allowing engineers to focus on more complex tasks. The cost reduction is also a benefit which comes from identifying potential issues early and preventing costly failures through predictive maintenance. There will also be improved design quality as AI and ML aids in exploring a wider range of design possibilities and identifying optimal solutions.

An example of AI and ML in a specific engineering discipline is the optimisation of power grid operations, detecting anomalies in power systems and designing energy-efficient circuits in electrical engineering. Or another example is predicting infrastructure failures, optimising construction schedules or analysing traffic patterns in civil engineering.

Robotics and embedded systems:

Robotics and embedded computing have allowed engineers to create intelligent machines for automation, precision control, and real-time decision-making.

The main applications of robotic is in industrial automation, medical robotics and autonomous vehicles.

In industrial automation robots are used to assemble cars, inspect products, and to handle hazardous materials. In medical robotics, embedded systems are designed to power surgical robots, enabling precise manipulation of surgical instruments during minimally invasive procedures. In autonomous vehicles, embedded systems manage the complex decision-making process for self-driving cars, including navigation, staying in the same lane and detecting obstacles.

In conclusion, the integration of computing into all aspects of engineering has brought upon many advancements to the field which otherwise probably wouldn't have been achieved in design, automation, artificial intelligence, and computational simulations. From the simpler CAD and CAE software's to the complex AI simulations, computing continues to better the future of engineering and all other fields.

Esolangs
By Nadia

Esolangs or esoteric languages are programming languages, often made as a joke, with the purpose of pushing the boundaries of programming language design, to experiment with wacky ideas, as software art or a combination of the three. They are usually not designed for practical usage, hence the use of the word 'esoteric' meaning 'Having to do with concepts that are highly theoretical and without obvious practical application.' [1]. Over the years, individuals and groups of programmers have created a multitude of these languages. Find below 5 of the most well-known and eccentric esolangs and how to output "Hello world" in each of them.

INTERCAL

INTERCAL, an abbreviation for 'Compiler Language With No Pronounceable Acronym' was created in 1972 by Donald R Woods and James M Lyon. They aspired to make a programming languages with no similarities to any other programming languages and thus, INTERCAL was born. It was widely believed to be the first ever esolang.

Code written using INTERCAL usually consists of a list of statements followed by the words "READ OUT", "IGNORE", "FORGET", and modifiers such as "PLEASE" or even "PLEASEN'T". Around a third to a fifth of written statements must be polite, meaning they need to be followed by PLEASE. If the compiler determines that your code isn't polite enough, it is rejected as it is insufficiently polite. On the flipside, if your code is too polite, the compiler rejects and calls it overly polite. Additionally, if "PLEASE GIVE UP" is not written at the end of the code the compiler is designed to drive up your CPU usage to 100% which can cause your computer to stutter, become unresponsive, or crash.

Since INTERCAL's syntax is not like any other programming language, it may seem like a good idea to use its Reference manual in order to help learn its various commands and statements. However, the manual contains confusing, paradoxical and nonsensical instructions much to the detriment of any aspiring programmers. An example of this is when the manual reads:

' Caution! Under no circumstances confuse the mesh with the interleave operator, except under confusing circumstances!'[5]

The manual has a "tonsil" as "Since all other reference manuals have appendices, it was decided that the INTERCAL manual should contain some other type of removable organ"[5]. It also gives names to various ASCII symbols. For example, a single quote (') is called a spark, double quotes (") are called rabbit ears and a comma (,) is called a tail.

Given all of this, 'Hello Word' in INTERCAL is written like this:

```
DO ,1 <- #13
PLEASE DO ,1 SUB #1 <- #238
DO ,1 SUB #2 <- #108
DO ,1 SUB #3 <- #112
DO ,1 SUB #4 <- #0
DO ,1 SUB #5 <- #64
DO ,1 SUB #6 <- #194
DO ,1 SUB #7 <- #48
PLEASE DO ,1 SUB #8 <- #22
DO ,1 SUB #9 <- #248
DO ,1 SUB #10 <- #168
DO ,1 SUB #11 <- #24
DO ,1 SUB #12 <- #16
DO ,1 SUB #13 <- #162
PLEASE READ OUT ,1
PLEASE GIVE UP
```

Befunge

Befunge is a 2-dimensional programming language made in 1993 by Chris Pressey with the purpose of being as difficult to compile as possible. It was named after a typo of the word "before" by Curtis Coleman at 4am on a BBS chat system, and it has since been reverse-endowed with a fictional morphology. Be-, a corruption of the prefix bi-, meaning "two", and funge which is the fictional root of the word fungible, also meaning "interchangeable". It has been given the definition 'to interchange (program codes with data) in two (dimensions).'[6]

The programmer must write code in a 2-dimensional grid, more commonly referred to as the 'playfield', and use arrow pointers such as '^', 'v', '>' or '<' to indicate which direction the executing program, should continue to execute code. The executing program's 'instruction pointer' initially starts at the upper left corner and by default, travels to the right and executes all code in its path until encountering an arrow pointer at which point it changes direction. As such, an infinite loop could be written like this:

```
>v
^<
```

Befunge has since gone on to garner a family of esoteric programming languages consisting of direct descendants and distant relatives such as Funge-98 which extends the core concepts of Befunge to other dimensional Funges such as Unefunge which is one-dimensional, Tri-funge which is 3-dimensional and Nefunge, which is n-dimensional.

Hello world in Befunge would be written like this:

```
>             v
v"Hello World!"<
>:v
^,_@
```

Chicken

Chicken was created by Torbjörn Söderstedt who was inspired by Doug Zongker's parody of scientific speeches to make a programming language where the word "chicken" is the only valid symbol [8].

In this language, code usually consists of multiple lines of the word "chicken" as the only tokens (single element sof a programming language such as constants, separators and identifiers) recognised by this language are spaces, new lines and the word chicken. The number of chickens on each line corresponds to an operation code. For example, 3 chickens on one line corresponds to subtraction, known in chicken as 'fox' and 4 chickens on one line means addition, known in chicken as 'rooster'.

Hello world in chicken looks like this:

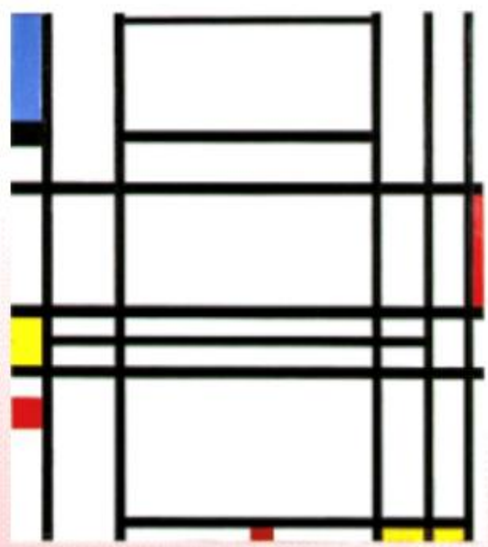
```
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken
chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken
chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken
chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken


chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken
```

```
chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken
chicken chicken
chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken

chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken

chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken

chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken chicken
chicken chicken chicken chicken chicken chicken
```

Piet

The esolang Piet was developed by David Morgan Mar and it is named after the artist Piet Mondrian, who was best known for his abstract pieces which often consisted of coloured squares and rectangles.

Piet is named after him, because code is written in a grid of pixels, and each one can have one of 20 colours. 18 of these colours relate to each other in a cyclical pattern of lightness and hue.



Composition No. 10 (1939–1942), oil on canvas, private collection by Piet Mondrian[11]

Light red (#FFC0C0)	Light yellow (#FFFFC0)	Light green (#C0FFC0)	Light cyan (#C0FFFF)	Light blue (#C0C0FF)	Light magenta (#FFC0FF)
Red (#FF0000)	Yellow (#FFFF00)	Green (#00FF00)	Cyan (#00FFFF)	Blue (#0000FF)	Magenta (#FF00FF)
Dark red (#C00000)	Dark yellow (#C0C000)	Dark green (#00C000)	Dark cyan (#00C0C0)	Dark blue (#0000C0)	Dark magenta (#C000C0)

Lightness increases going upwards and hue increases going to the left. If one pixel is green and the next is red, there would be 5 changes in hue because in Piet, you cannot have negative changes in hue or lightness.

In Piet colours are grouped together and are referred to as colour blocks. A colour block is a group of pixels that are all the same colour that are adjacent to each other. Diagonal pixels are not considered part of the same colour block. Different changes in hues and lightness between colour blocks correspond to different commands. One change in darkness and 1 step in hue corresponds to subtraction and 2 steps in hue and no changes in lightness is division.

Hue change	Lightness change		
	No change	1 darker	2 darker
No change	N/A	Push	Pop
1 step	Add	Subtract	Multiply
2 steps	Divide	Modulo	Not
3 steps	Greater	Pointer	Switch
4 steps	Duplicate	Roll	Input num
5 steps	Input char	Output num	Output char

Code is read by a direction pointer or a 'DP'. It starts in the colour block closest to the top left corner and is initially facing right. It finds a colour block that is adjacent to and furthest away from the colour block the DP is currently on and measures the change in lightness and hue and executes the appropriate command.

The last two colours in Piet are white and blank. White effectively acts as blank space in Piet. When a white colour block is encountered by the DP, Piet does not execute any commands. On the other hand, black is almost the opposite of white. The DP can't pass through it and thus tries to find another colour block.

If the DP can't find another colour block, it rotates 90 degrees clockwise. If no other colour block can be found it will conclude there is no way out and the program will terminate.

Hello world in Piet can be written in many different ways such as the following:

Malbolge

Malbolge was written by Ben Olmstead in 1998. It is named after the 8th circle of hell in Dante's inferno, 'Malebolge' which is reserved for perpetrators of fraud [12]. It was designed to be as difficult to program in as possible.

It uses trinary, also known as ternary of base-3. In contrast to binary, trinary uses the digits 0,1 and 2 which is extremely impractical in most cases and difficult for programmers to adapt to. It has 'crazy operation' which is described as such by Ben Olmstead in its documentation: "don't look for pattern, it's not there." To use crazy operation, the programmer must write 'crz' followed by 2 trinary digits, which looks like the following:

```
crz 0001112220, 0120120120
```

(The above code would return a value of 1120020211 [14])

This is how the output of crazy operation is determined:

crz		Input 1		
		0	1	2
Input 2	0	1	0	0
	1	1	0	2
	2	2	2	1

[14]

Furthermore, Malbolge has self-altering code, where instructions can mutate when executed, making it even more difficult to program in.

It took 2 years for the first Malbolge program to be written. It was found by a LISP program which had performed a beam search algorithm written by Andrew Cooke. The program outputs “Hello world” and looks like this:

```
(=<`#9]~6ZY327Uv4-QsqpMn&+Ij"'E%e{Ab~w=_:]Kw%o44Uqp0/Q?xNvL:`H%c#DD2^WV>gY;dts76qKJImZkj
```

Conclusion

While esolangs may not be practical or in widespread use, seeing what the esoteric programming community has created over the years can provide a new outlook on the high-level programming languages that we use every day. Esolangs such as malbolge can help us be more appreciative of the consistency and readability provided by these languages. On the other hand, esolangs such as Piet show that programming can even be used to make art; programming languages don't always have to consist of words or coding blocks.

These are only 5 of the thousands of esolangs that have been recorded on esolang.org, which has an expansive list of them with documentation on each. Take a look at some of the esoteric languages listed. Perhaps you may even be inspired to create your own.

Sources:

[0] https://esolangs.org/wiki/Language_list

[1] https://en.wiktionary.org/wiki/esoteric

[2]https://en.wikipedia.org/wiki/INTERCAL#Details

[3]https://www.access-programmers.co.uk/forums/threads/worst-programming-language-ever.322996/

[4]http://progopedia.com/example/hello-world/257/

[5]https://web.archive.org/web/20110716084816/http://oops.se/~urban/pit/intercal.ps

[6] https://esolangs.org/wiki/Befunge

[7] https://esolangs.org/wiki/Chicken

[8] https://www.omnesgroup.com/weirdest-programming/

[9] https://en.wikipedia.org/wiki/Esoteric_programming_language#Piet

[10] https://esolangs.org/wiki/Piet

[11]Lodder, Kokkori & Mileeva 2013

[12] https://esolangs.org/wiki/Malbolge

[13] https://en.wikipedia.org/wiki/Malbolge

[14] https://esoteric.codes/blog/interview-with-ben-olmstead

How does AI affect our Environment?

By Sreekshitha

AI is a tool that we all use in our day-to-day life, intentionally or not. With the integration of AI software and relevant applications in every corner of the internet, it is hard for such recent innovation to escape the public's notice and appreciation. The term 'Artificial Intelligence' was first coined in the mid 1950s, and it has since developed exponentially, performing tasks and executing requests at a level that a human simply wouldn't have been able to think of just 20 years prior.

However, the recent glorified and positive approach to Artificial Intelligence shouldn't be the only perspective that society considers; the long run consequences and downsides shouldn't be a dubious afterthought. One major problem that comes with AI is the intensive and draining impact it has on our environment.

To put our use of AI into perspective, out of the 334.34 million companies worldwide, over 266 million of them are already using or exploring AI in their business operations. The use of AI chatbots for customer service, or the recent introduction of generative AI on META platforms are just a few examples of how reliant we are becoming on it.

The most prominent problem is the water wastage. According to research from the University of California, the water consumption required to handle just 5-50 prompts on ChatGPT is around 500 milliliters per interaction. You can think of that as just over 2 glasses of water drained into a figurative blackhole every time you enter a couple prompts into ChatGPT. Data centres use water during construction and in the cooling of electric components. According to some estimates, AI-related infrastructure will soon consume 6 times more water than Denmark (a country of 6 million). This might not seem that excessive, until you think about how a quarter of humanity already lacks access to clean water and sanitation – a problem that is just going to get worse with our increased reliance on AI.

The electronic waste produced by AI technology has already posed a threat to the environment. E-waste contains hazardous chemicals, like lead, mercury, and cadmium – that are all notorious for contaminating soil and water supplies which in turn endanger both human health and the environment that animals rely on. Harming farmers' crops and affecting produce are both additional risks that we face if disposal of e-waste goes unchecked.

On a positive note, AI is already being used to map the destructive dredging of sand and chart emissions of methane. Optimising energy systems, evaluating solutions to climate change, building on previous theories and applications – these are all ways that it has already protected the world we live in.

While AI has its issues, it has made significant advancements in technology that all people and communities benefit from – even environmentally. The only thing we can do is to look towards greener and more environmentally friendly options, where tech companies make AI software more efficient (in both training and consumer use) and incorporate consideration for the environment.

The Involvement and Development of Computer Science in Medicine

By Tania

Medicine. A field requiring immense precision, dedication and education. Computer Science. A field that is so impressively complex that it can deliver immense precision, dedication and education and more with just a click of a button. It started off small, with computers being used in hospitals and GPs to record a person's medical data, or making notes, but with technological advancements, have eventually been developed enough to introduce robotics to medicine, and the results are simply plain evidence for how extraordinary and revolutionary the power of AI has become. Computer Science has brought in a new era of medicine.

Algorithms combined with advanced robotics can aid everything from diagnostic imaging and analysis to remote surgical assistance, and even autonomously performed procedures. These extraordinary advances in medicine due to the help of computer science bring hope for more consistent and effective treatment in the future. Looking at the rate of AI advancement nowadays, it is safe to say that there is a high probability that the future of surgery is likely to include robots with some ability to work on their own.

Surgical robots are classified by their level of autonomy, and to which degree they use algorithms to support their medical thinking and decision making -

LEVEL 0 ROBOTS – No autonomy whatsoever and rely on a human operator to work.

LEVEL 1 ROBOTS – Make us of AI to aid with procedures

LEVEL 2 ROBOTS – Robots have autonomy over certain repetitive subtasks within a procedure

LEVEL 3 ROBOTS – Robots can generate a strategy or list of strategies for a task but still relies on a human to select or approve the strategy.

There is still Level 4 and 5 of autonomy however level 3 is currently the highest level that current technology can create. But who know how the future will pan out, very soon we may be able to reach the fifth level of autonomy where the robot can control and execute everything itself.

Think about it. No room for error. Maximum efficiency. No more years of students' lives spend memorising every part of the human body. The perfect amount of precision, dedication and education needed to be a doctor. All because of the power of computer science and AI. Pretty cool huh?

Puzzle #2 - Word Ladders

C R O S S
_ _ _ _ _
_ _ _ _ _
_ _ _ _ _
_ _ _ _ _
R O A D S

R I S E
_ _ _ _
_ _ _ _
_ _ _ _
F A L L

Word ladders is a word game created by Lewis Carroll. The puzzle starts with a word and the aim is to get to the end word by changing one letter from the previous word to get another existing word to finally reach the end word. For example, to get from head to tail:

HEAD → HEAL → TEAL → TELL → TALL → TAIL

AI's Green Revolution

By Diya

Can DeepSeek and Other AI Models Save the Environment?

Artificial Intelligence, as we all know it is rapidly reshaping industries before our eyes, but one of its most crucial applications is in tackling environmental challenges and one of its most worrying concerns is its environmental impacts. From optimizing energy consumption to predicting climate change patterns, AI is emerging as a key player in sustainability efforts. However, the rise of powerful AI models, such as DeepSeek, also raises concerns about their own environmental footprint.

AI is transforming how we consume energy by making systems smarter and more efficient. Machine learning algorithms can analyse energy usage patterns and suggest optimizations, reducing waste in industries, homes, and even entire cities. Google, for example, has used AI to cut its data centre cooling costs by 40% (DeepMind, 2018). The integration of AI into power grids helps predict supply and demand fluctuations, allowing for a smoother incorporation of renewable energy sources like solar and wind.

The energy efficiency of AI is particularly relevant as energy demand increases globally. AI-driven smart grids enhance efficiency by balancing supply and demand dynamically. Predictive models utilize time series analysis, employing techniques like autoregressive integrated moving average (ARIMA) to estimate future consumption trends. These models help determine the optimal mix of energy sources to reduce reliance on fossil fuels. This application of AI significantly improves efficiency and lowers emissions, making AI an essential tool in sustainable energy strategies.

Climate modelling, a traditionally complex field requiring vast amounts of data processing, benefits significantly from AI. By identifying patterns in weather data, AI-driven models enhance the accuracy of climate predictions. The ability to process large-scale datasets using advanced neural networks improves forecasting models, helping scientists better understand and mitigate extreme weather events. AI also assists in disaster response, providing real-time analysis of wildfires, hurricanes, and earthquakes, which leads to faster and more effective emergency preparedness strategies (Rolnick et al., 2019). AI-powered geospatial analysis identifies vulnerable regions by processing satellite imagery and meteorological data, predicting areas prone to extreme weather conditions. Additionally, reinforcement learning models refine evacuation strategies by simulating different disaster scenarios, ultimately saving lives.

In conservation efforts, AI-powered monitoring systems using satellite imagery and drones have proven invaluable. These systems track deforestation, poaching, and biodiversity loss in real time, allowing conservationists to take swift action. Automated image recognition, supported by convolutional neural networks (CNNs), helps identify endangered species in vast datasets, ensuring better resource allocation in protection programs (Waldchen & Mader, 2018). Similarly, AI improves waste management by optimizing collection routes and identifying recyclable materials more accurately. Neural network-based classification systems enhance sorting methods, ensuring that more waste is properly recycled (Makri et al., 2021). By integrating AI with robotics, recycling plants achieve greater accuracy in waste sorting, increasing efficiency and reducing contamination rates in recycling streams.

ChatGPT and the Environmental Cost of Large Language Models

While AI applications offer immense benefits, large-scale language models like ChatGPT come with significant energy costs. These models require extensive computational resources, leading to high electricity consumption and carbon emissions. Studies suggest that training a model like ChatGPT can consume as much energy as an average American household does in several years (Henderson et al., 2020). The underlying reason lies in the billions of parameters these models must process and update during training.

Each query to ChatGPT requires multiple matrix multiplications within deep neural networks, consuming a significant amount of energy. Large-scale cloud infrastructures, often running on non-renewable energy, further exacerbate the issue. AI researchers are now investigating methods to reduce this impact through model distillation, which involves compressing large models while maintaining their accuracy. Other approaches include using hardware accelerators optimized for AI tasks, such as TPUs (Tensor Processing Units), which perform AI computations more efficiently than general-purpose processors.

The Rise of DeepSeek: A Game-Changer in AI Technology

In recent weeks, DeepSeek, a Chinese AI startup, has captured headlines and stirred discussions across the tech industry and beyond. The company made waves with the launch of its groundbreaking AI model, R1, in January 2025. This open-source model has been reported to rival the capabilities of leading American counterparts, such as OpenAI's offerings, while boasting an astonishingly lower cost—estimated at 90-95% less.

The impact of DeepSeek's innovation was immediate and profound. Following the release of R1, stock prices for major AI companies plummeted. Nvidia, a key player in the AI hardware market, saw its market value drop by approximately $600 billion, with shares falling 17% in just one day. Other tech giants, including Microsoft and Oracle, also experienced significant declines in their stock values as investors reacted to the shifting landscape.

Adding to the buzz, DeepSeek's AI assistant quickly ascended to become the most downloaded free application on Apple's App Store in the United States shortly after its launch. In South Korea, it garnered over a million downloads before facing removal from app stores due to allegations of data privacy violations. The South Korean government accused DeepSeek of sharing user data with ByteDance, the parent company of TikTok, raising serious concerns about data security and privacy.

Industry leaders have taken notice of DeepSeek's rapid ascent. Marc Andreessen, a prominent venture capitalist in Silicon Valley, hailed the startup's advancements as "one of the most remarkable and striking advancements" in AI technology. Many are likening this moment to "AI's Sputnik moment," suggesting that it could redefine the competitive dynamics between Chinese and American tech firms.

Furthermore, DeepSeek's rise is seen as a significant boost for the Chinese government's ambitions to achieve technological independence from Western influence. This development has sparked intense discussions about the future of AI development and the implications for global technological competition.

As DeepSeek continues to disrupt the AI landscape, its story serves as a reminder of how quickly innovation can reshape industries and challenge established norms. The world watches closely as this young startup navigates the complexities of data privacy, international relations, and technological rivalry.

Unlike traditional AI models, DeepSeek focuses on balancing power with sustainability, leveraging optimized architectures that enhance performance while managing computational costs. One of its key advantages is energy efficiency, as it requires less computational power than conventional models, resulting in lower energy consumption and reduced environmental impact. Additionally, DeepSeek offers improved performance, scalability across various industries, and a reduced carbon footprint by minimizing reliance on high-energy data centers.

However, despite these benefits, DeepSeek is not without its challenges. While more efficient than many existing models, it still demands significant processing power, contributing to energy use. Moreover, training sophisticated AI models requires vast datasets, leading to high computational costs. The model's overall sustainability also depends on the hardware running it, meaning outdated infrastructure could diminish its energy-saving potential.

AI's environmental footprint is a growing concern, with large-scale training models consuming as much energy as several hundred households over a year. Data centres hosting AI models account for nearly one percent of global electricity use, highlighting the urgent need for efficiency-driven innovations. DeepSeek plays a crucial role in addressing this issue by optimizing training processes to reduce power consumption, making it a more sustainable option. Beyond its own efficiency, it can also be used in environmental applications, from predicting energy consumption patterns to optimizing renewable energy distribution and supporting climate change research. As AI continues to evolve, models like DeepSeek exemplify the potential for intelligent computing that is both powerful and environmentally conscious.

The Future of AI and Sustainability

In conclusion, while AI offers immense potential to optimize energy usage, improve climate predictions, and support conservation, its environmental impact cannot be overlooked. Innovations like DeepSeek show that more energy-efficient AI models are possible, but the computational demands of these technologies still contribute to significant energy consumption. To reduce AI's carbon footprint, further advancements in energy-efficient algorithms, model distillation, and hardware optimization are critical. Individuals have a role to play by advocating for sustainable AI practices, supporting companies like Google, Microsoft, NVIDIA, Amazon, and Tesla, which are prioritizing energy-efficient technologies. These companies are leading the way with AI-powered energy optimizations, renewable energy investments, and innovative solutions to reduce emissions. By supporting organizations that prioritize sustainability and encouraging the shift toward renewable energy in tech infrastructure, we can ensure that AI's future contributes positively to both technological progress and the health of the planet. Taking action now—whether through supporting green technologies, reducing personal tech consumption, or fostering sustainable practices—will help ensure a responsible and sustainable future for both AI and the environment.

References

- DeepMind (2018). "Reducing Google Data Center Cooling Bill with Deep Reinforcement Learning." Retrieved from https://deepmind.com/blog/
- Henderson, P., et al. (2020). "Towards the Green AI Movement: Reducing AI's Carbon Footprint." Proceedings of AAAI.
- Makri, A., et al. (2021). "AI in Waste Management: A Step Toward Sustainable Cities." Journal of Environmental Management.
- Rolnick, D., et al. (2019). "Tackling Climate Change with Machine Learning." Proceedings of NeurIPS.
- Strubell, E., et al. (2019). "Energy and Policy Considerations for Deep Learning in NLP." arXiv preprint.
- Waldchen, J., & Mader, P. (2018). "Machine Learning for Conservation: Applications in Ecology and Wildlife Monitoring." Biological Conservation.

Homomorphic Encryption in Finance

By Janette

Banks and financial institutions have sought many ways to increase protection over their confidential data and the increasing use of homomorphic encryption has shown to do wonders in this sector.

Homomorphic encryption (HE) is when encrypted data (data which is transformed into, essentially, a code that can only be accessed or understood by specific people – used as a security measure - data that is unreadable to the human eye) can be analysed without exposing the unencrypted data to the systems, environments or people who process the data. In short, this means that information can be processed without even having to be decrypted, which means the data will never be exposed.

How does it work?

HE works when you take raw data, encrypt it, and then allow computations (performing an operation on it) on the encrypted data. Then that result will be sent to be decrypted, which will get you the real value.

There are 3 types of HE:

1. ***Partially* HE** – allows only one operation [only addition/only multiplication] to be performed on the data, but it can be done infinite times.

2. ***Somewhat* HE** – allows both addition and multiplication but for a limited number of times.

3. ***Fully* HE** – both addition and multiplication used infinite number of times. Most expensive computationally, but also the most powerful and effective.

This means implementing homomorphic encryption can be significantly expensive, because it relies on extremely difficult maths calculations which could require lots of the computer's memory and computation. If an operation, e.g. in banking, if we need to multiply two encrypted values together, the encrypted result could be a very big value.

In 2019, financial companies suffered $5.86 million losses on average for every data breach. This means that the companies had to pay huge compensation due to the leak. Therefore, when HE became more known, more companies invested in it, for instance, ING, Rabobank, Scotiabank are now all experimenting with HE.

Ways homomorphic encryption can be utilised to benefit the finance industry:

1. **Fraud detection** – algorithms can detect fraud activities when assessing over encrypted data, which means that the data's privacy is kept, yet it is still a good security measure.

2. **Loan approvals** – banks can make sure that data is protected when making loan decisions [e.g., looking at credit score- which shows the borrower's creditworthiness].

3. **Prevents bid rigging [e.g., in stock market auctions]** - for instance, competitors cannot see each other's bid, therefore it decreases the chances of there being tampering].

4. **Collaborative benchmarking** – multiple financial companies can combine their encrypted data as shared data.

The financial sector experienced 3,400 cyber incidents in 2023, with financial motives driving 71% of data breaches. This shows how the financial sector became more urgent to adopt homomorphic encryptions, to secure the privacy and security of their data.

Challenges faced when adopting homomorphic encryption:

1. **High memory/ bandwidth needed** - when banks store huge values after computations are processed, it means these values could take up huge amounts of space.

2. Slow performance – because 'HE is computationally heavy,' this means that it takes a lot longer to perform calculations on the encrypted data.

3. Scalability – there is a lot of data being handled in banks, therefore, to perform HE on all data could need specialised hardware, and it will not be easily manageable.

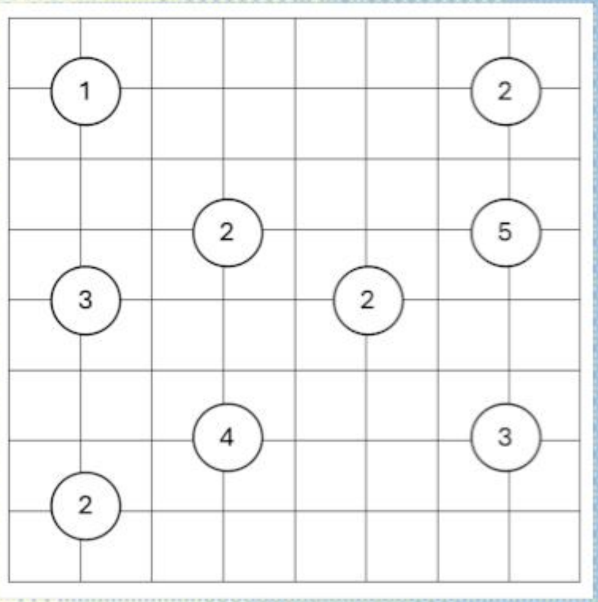
4. Expensive – banks need skilled engineers, specialists, specialised hardware, which could take years of research and development.

Citations:

- https://www.ideapoke.com/growthleader/homomorphic-encryption-boosts-fintech-security-innovation
- https://www.fortunebusinessinsights.com/homomorphic-encryption-market-111218?utm_source=chatgpt.com

Puzzle #3 - Bridges/Hashi

Bridges, or Hashiwokakero (also known more simply as Hashi), literally meaning "build bridges" in Japanese, is a puzzle created by Nikoli, a Japanese publisher specialising in games and puzzles. The game consists of a grid with circular islands. The numbers on these islands indicate how many bridges are connected to that island. Bridges are straight lines that travel in one direction only. They can only be horizontal or vertical, not diagonal and cannot cross over each other. There can only be two bridges at most connecting two islands. The bridges must also connect the islands in a single connected group; there cannot be two or more separate groups of connected islands.



CAPTCHA

By Priyanka

What is CAPTCHA?

CAPTCHA is an acronym that stand a for 'Completely Automated Public Turing test to tell Computers and Humans Apart'. Essentially, these are a type of challenge-response tests that are used in computing to tell whether the user of a certain website is human or a bot. This helps deter bot attacks and spam by reducing the number of harmful bots that can access websites and data.

Despite their primary purpose of managing bots, CAPTCHAs themselves are fully automated and programmed to pop up in certain places on a website, and then they automatically pass or fail users. This enables CAPTCHAs (and its successor reCAPTCHA) to create automatic protection for websites.

How did the first CAPTCHA work?

The first CAPTCHAs used distorted letters, and asked the user to identify them. The general idea was that bots world not be able to identify them, and would just input random letters, causing failure. However, humans would be able to pass the tests as they are used to seeing things in different ways. These are commonly found in log-in forms, account sign-up forms, online polls, and e- commerce checkout pages. With the progress of technology, they are slowly being replaced because bots are becoming smarter and more adept at identifying different forms of letters.

reCAPTCHA

reCAPTCHA was created to combat more sophisticated bots, and they are focused purely on preventing bots from automatically visiting website pages, filling out forms, and spamming forums or social media sites with comments. reCAPTCHA is more advanced in using images and analysing user behaviour, like the path of their mouse. They are also more user-friendly, especially with the creation of checkboxes. At the time of its creation, this solution was able to detect and block most automated threats. However, some modern bots can now bypass reCAPTCHA as easily as CAPTCHA.

Types

There are three common version of reCAPTCHA:

- legacy reCAPTCHA (v1) - These are similar to original reCAPTCHA, where the user has to identify distorted media, such as images or text, correctly and accurately.
- checkboxes/invisible reCAPTCHA (v2) - These check boxes are coded in a different way or set not to be spotted so easily by bots. They also track the path of the user's mouse to the box to see if it is too straight (only bots can follow these paths due to slight human error). When they are clicked by the user, the checkboxes will analyse the user's web activity and other risk factors associated with the login, checking whether the user is safe to be authenticated.
- NoCAPTCHA reCAPTCHA (v3) - These have powerful analytical tools that monitor users' behaviours and other risk factors entirely in the background, ready to request additional authentication if suspicious activity presents itself. These do not require any input by the user.

Positives and negatives of using CAPTCHA/reCAPTCHA

Security: CAPTCHA prevent bots from accessing certain websites or creating fake accounts, protecting that website's users.	**User frustration:** Some CAPTCHAs can be quite challenging to understand or hard to read.
Accessibility: Modern CAPTCHAs can be designed to be accessible for users with disabilities.	**Time-consuming:** Completing CAPTCHAs can add an extra step to the user experience, slowing the process.
User Verification: They check that the user is human, reducing risks of spam and fraudulent activities from bots.	**False positives:** CAPTCHAs are not completely reliable and may identify real users as bots, causing inconvenience.

Overall, while CAPTCHAs serve an essential security purpose, they can also pose challenges in terms of user experience.

AI and Big Data

By Freddie

As the world becomes more and more technologically advanced, we are beginning to form larger and larger data sets, filled with information on all forms of topics, ranging from social media companies holding personal information about its users, to records of collisions in particle colliders. These extremely large data sets are referred to as big data, each data set largely defined by a few key components; volume, which describes the size of the data set itself, velocity, which describes the speed that new data is generated and processed, and variety, describing the diversity of the data, like if it is text or an image. With the explosion of the internet, we have seen the volume and velocity of data skyrocket, and it has become impossible to process through these data sets using humans. The only way to get any information out of these datasets without technological assistance is to simply take out a small chunk to analyse and hope it's representative of the full dataset, but this can lead to great inaccuracy. Instead, artificial intelligence (AI) has been used to get a true view of the entire data set. These AI models run off neural networks and machine learning algorithms, giving them data to begin with so the computer can learn from past experiences and improve without being explicitly programmed. (Source)

Big data and AI are crucial to each other, as the more data that we grant the AI access to, the more powerful and intelligent the model will become. It will improve its ability to analyse the data present and be able to create more accurate predictions. As AI improves, more and more companies use AI for various uses. For example, many companies may use AI on datasets containing personal data, creating a 360-degree view of the customer, meaning that they will have a far greater understanding of their audience than ever before. This leads to far greater personalisation of services, as AI models analyse our behaviour and make predictions about our preferences and what we want out of a service. On top of this, AI may also be used in price optimisation and forecasting, allowing companies to plan ahead with their pricing, and also showing them what the ideal price point is for them to maximise profit. On one hand, AI being used in this way can benefit both the company and consumer, allowing for more personal products that everyone can enjoy to the maximum. However, it can also potentially pose privacy risks, as companies get a larger and larger incentive to extract as much of our data as possible, potentially resulting in us not having a single piece of our identity hidden from large tech corporations. (Source)

AI can also be very useful for scientific research when looking through large datasets. For example, the Large Hadron Collider (LHC) produces incredibly large amounts of data, with billions of particles colliding each second. This is would be impossible for humans to search through, and traditional algorithms would only work if researchers knew exactly what they were looking for, which they may not. AI is an incredibly powerful tool for this research, as it can quickly search through the data, and it will be able to tell where there is an anomaly. (Source)

In the past few years especially, generative AI has seen rapid advancement, models like Google Gemini or ChatGPT becoming increasingly integrated into our lives. In order for us to continue the development of this AI, we must create increasingly large data sets to be processed, giving these models more information to base responses off of, generally resulting in improved accuracy. However, after years of training, the amount of useful data risks running out, as huge AI data centres process almost any text developers can find to the point that the Internet is beginning to run out of things to offer these models. In order to sustain the growth of AI, companies may begin to use our own personal conversations (like DMs) as training data, raising privacy concerns amongst users, many of whom wishing to not be used as training data for these huge AI models. Another approach that may be used is using AI-generated content as training data, resulting in a steady flow of new data to be used for training. However, this poses the risk of 'model collapse', as each time we use these AI generated responses as training we will lose a bit of the starting information, similar to the effect of photocopying something that has already been photocopied. (Source)

In conclusion, AI and Big Data are strongly linked to one another, as the larger these data sets get, the more complex these AI models become, which in turn makes big data more useful due to more accurate predictions being made based on it. As data sets get larger and larger, the power of data analysis will grow rapidly, allowing for us to make huge advancements in scientific fields and grant us the ability to greatly improve the personalisation of products. However, we must be wary of the risks to privacy that could be created if we begin to become too focused with finding as much data as possible, and we should protect private conversations from being used as training data.

The Mermaid's Tale in Virtual Reality

By Eleanor

Its 2023 and in hospital a 3-year-old girl has only about 2 or 3 weeks left to live. Her fourth and sadly last birthday is a few days away. She loves mermaids and for this birthday she wished to be a mermaid. Dressing her up in a mermaid costume was possible but that wouldn't really make her into a mermaid. Making her into a mermaid seemed impossible.

Her brother's teacher followed VR Therapies on social media. VR therapies is a social enterprise which supports people with disabilities and children with special needs. They do this through VR games and immersive experiences. The teacher thought that they might be able to make the girls dream come true, and contacted Nurse, CEO and founder of VR Therapies Rebecca Gill and told them of her wish. Rebecca posted it on her social media, which caught the attention of Professor Sylvia Xueni Pan. As a professor of Virtual Reality at Goldsmiths, University of London, she is widely followed by over 6,000 people from all around the world and she posted to ask if they have ever tried to create a mermaid game.

It turns out that many people have, which is great news, and for the next 48 hours Sylvia and her team work to narrow it down to a few key games by testing and selecting the best VR experiences sent to them. Additionally, a number of developers from all around the world created unique applications just for her, including an underwater journey with various creatures. They add in extra features, customising the avatar to look like her, matching her appearance and skin tone her to make her feel more like a real mermaid. When she holds up a magical mirror in the game she sees herself as an underwater princess. A special VR storybook fairy tale was made, and someone even designed an experience with hidden birthday messages from her family. Her brother can play as well, and they both can swim with the dolphins and jellyfish.

Not only did they get these VR experiences to her and VR Therapies in time for her magical, mermaid-themed birthday party in their sensory room, but she was also given a crown made out of real sea shells, a wand, and a mermaid costume. In the interactive VR games, she swam with dolphins and explored underwater worlds. When she was too unwell to leave her bed, VR Therapies brought a VR headset to her home so she could continue enjoying the experience. I think this is an amazing thing that VR therapies and virtual reality creators have done.

I am sure that most of you have played a Virtual Reality game too. Virtual Reality headsets can transport you to different world. Games range from gruesome battling to completing mazes. VR can make your impossible dreams come to life. I have been to many events where I was immersed in the game, such as being transported from a greenhouse in Kew Gardens to a rainforest and interacted with characters. VR is also used to cure phobias, like trypanophobia (the fear of needles). In this simulation you go into a hospital waiting room, and are taken all the way through the process to the needle coming right next to your arm. Arachnophobia can also be treated this way. Additionally, children with cochlear implants can be trained to hear by a target shooting game where you have to listen and shoot in the direction of the sound.

If you would like to start building a VR world of your own then you might like to try using an app called CoSpaces. I have used it, and I thought it was so fun. To see your world in 3d you will need to use a phone and a Google Cardboard VR Phone holder. You can build new worlds, make mazes, and add interactions with block based coding, or even make a rollercoaster. You can program games and then explore them in VR. CoSpaces also allows you to go into other peoples shared creations and play them. In the games you can interact with objects, see characters and travel across the area. I made a maze where there were objects you could touch, talk to and click on. CoSpaces is free, however the free version is quite limited. A pro version is offered, but that does cost money. So, if you think you want to play or make VR Games, I suggest that you try using the free version of the app to start with.

If you would like to see this for yourself with or without a 3d headset, go to https://edu.cospaces.io/MXT-ZNK or scan the QR code.

Virtual Reality has the power to virtually make your dreams come true. While there are still some challenges, like cost and accessibility, the technology is improving quickly and opening up new possibilities. As VR continues to evolve, it will change the way we learn, work, and experience the world. The potential for VR is huge, and we're just beginning to see what it can really do. To learn more about VR Therapies and the incredible work they do, visit their Facebook page at www.facebook.com/vrtherapies.

Thank you to Rebecca Gill for help and advice with this article.

Computing Crosswords: Human vs AI

By Jia

cs4fn Code Breaking

So how good are you at code breaking? Here is a code crossword. No clues just the code to break. We've given you a few letters to start. The key is at the top. All letters of the alphabet appear in the key and grid...but which is which letter? Work out the code and it will reveal one of the greatest movie messages of all time....and to make it a bit more fun, you have to answer the following questions about the grid:

1) Which lump of clay ran away because it wanted to have fun golem
2) What is the caffeine-loaded programming language? java
3) What animal has a crush on you? python
4) What explosive song did Debbie Harry of Blondie sing? atomic

SO_TWARE
f j v
SOFTWARE

START WITH 8 8 15
PATTERN RECOGNITION
8 8 15

11 7 14 3 11 15
A N I _ A L
A N I M A L

aal
eel
ool
iil
uul
yyl

25
R_E
ROE
~~RIE~~
RYE
RUE

JAVA OR VAJA

14 22 is a 2 letter word x2
14 7 is a 2 letter word
7 10 is a 2 letter word x2

If 14 is vowel, 22 and 7 is consonant

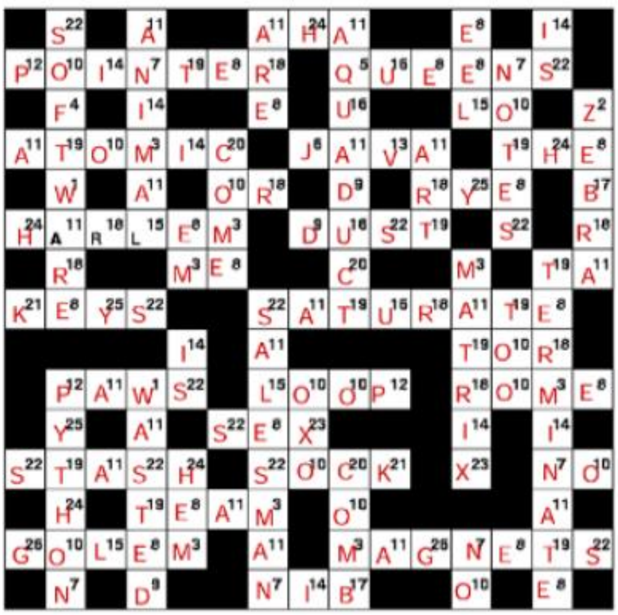
dont' forget y

14 22 = I_
14 7 = IN
7 10 = NO

possibly 7 is n or t
7 is consonant so 14 is a vowel

vowels
14 or 7

maybe
20, 11, 7
25, 10, 16



16 and 7 are consonants
2 is consonant
24 is a consonant
22 is a consonant
13 is a consonant

25 is ~~O~~, Y or U
19 10 10 ~~10~~ is a vowel that can double up

SOC_

15 10 10 12
L _ _ ?
~~LII_~~
LOO_
~~LUU_~~
~~LYY_~~

_O - O_E
NO - ONE
7 is most likely n

14 22

IN
UN

_OU
you

ma_nets
b d f g h j k p q u v w y z
magnets

com_
b d f h j k p q u v w y z
comb

atomi_
atomic

_ALE_MAN
b d f g h j k p q s u v w y z
SALESMAN

S_ACE
d f j p v w
SPACE

19 8 18 3 14 7 11 19 8
_ E R M I N A _ E
TERMINATE

_ebra
d f h j k p q u v w y z
zebra

AQUA_UCT
AQUADUCT

PA_S
f j v w
PAWS

SOC_
d f h j k p v w
SOCK

STAS_
d f h j p v w
STASH

SAT_RATE
SATURATE

16 always comes after 5
U always comes after Q

Computational thinking is present in our day-to-day lives as part of our problem-solving process. When presented with a challenge, we consider multiple ways to go about it, which mostly leads to a systematic process with which we solve a puzzle. I started this code crossword from cs4fn not quite knowing what to do. So to start with, I filled in the letters that were already given (A, R and L). This is decomposition, where the big empty grid is split into what we know and what we don't know, and the process is used in every problem-solving technique. Next, I looked for patterns that may give clues to what to do next. I found a three-letter word 8 8 15 which translates to _ _L. All words have at least one vowel or y, and the "yyl" was not a word so there must be a repeated vowel. After trying every vowel combination systematically (a, e, i, o, u) I found e was the letter that worked. This uses pattern recognition and a methodical trial and error to find one of the words, which computers may use for problems requiring heuristic solutions like this puzzle. Once again, I filled in the letter e for every box and re-evaluated the puzzle.

I did attempt to determine 25 from R_E finding that it must be a vowel or y and that it could be O, Y or U, which was not very helpful. Computers use backtracking when they reach a dead end, just as I followed a different route, instead focusing on 10, which occurred in pairs more than once and must be a vowel or y. By trying multiple letters, it was revealed to be O, and again every letter was filled.

I continued to look at the smallest letters with the least number of gaps to deduce what the missing letters were. A computer would similarly break down a large problem into smaller, more manageable problems where there is the most information to work from, ignoring the bigger problems for the time being (abstraction) until there was enough data to solve them. When reaching the larger words, a trial-and-error approach was used with all the letters left, finding the correct one (e.g. t in terminate). Every time a letter was found, it would reduce the number of letters I (or a computer) needed to search, meaning it would be easier and faster to solve the next one.

While a normal computer would search every single letter, humans have a level of intuition that allows us to spot the real words faster. When dealing with SAT_RATE, it was quite simple to guess the letter would be U without trying every combination. The more letters were placed in the puzzle, the more intuition helped fill in uncommon words, e.g. harlem, matrix, and atomic. Repeated letters helped me in pattern recognition to complete salesman. While humans would use common sense for many of the words, an algorithm would follow a series of steps, so although its speed makes it likely it would execute faster than a human could solve it, the number of comparisons (or average time complexity) may be larger than how a human would solve it. Perhaps AI would be able to replicate intuition and solve the puzzle more efficiently than we could.

I ran this problem through ChatGPT and Gemini to see if they could solve it. All Gemini versions and ChatGPT 3.5 were not capable of solving the puzzle as they cannot compute "advanced data analysis" yet. ChatGPT 4.0 took several hours and wrong attempts only to concede that it was unable to solve the puzzle, so it seems current publicly available AI is not capable of solving heuristic problems such as these. What is interesting is when solving the puzzle, the AI (ChatGPT 4.0) either guessed random English words or used most common English words to try and solve the puzzle, resulting in wrong answers. The AI did not seem to fully understand the puzzle even after explanation. However, with the recent leaps in AI development, it is likely that AI will be capable of these challenges in the near future.

The Role of AI in Neurology and Medicine: Transforming Diagnosis, Treatment, and Research

By Zahid

Artificial intelligence (AI) is transforming neurology dramatically, transforming the diagnosis, treatment, and management of neurological disease. By interpreting large volumes of medical data, AI has the potential to help specialists diagnose disease earlier, tailor treatment to the individual patient, and even forecast patient prognosis more accurately. As AI becomes increasingly incorporated into healthcare, its influence on neurology grows with it, ushering in exciting possibilities along with intimidating challenges.

One of the greatest benefits of AI to neurology is that it has the potential to make diagnoses more accurate. Machine learning algorithms can comb through huge amounts of data—e.g., brain scans, genetic information, patient records—to spot patterns of neurological illness. In neuro-oncology, for example, AI helps detect brain tumours by combing MRI images with precision that sometimes equals or even surpasses the human eye. As per a report from AIMultiple, AI-driven imaging modalities have helped a lot in the early diagnosis and treatment planning of brain cancer.

Apart from imaging, AI is being applied in the early detection of dementia as well. Researchers in Scotland are investigating the potential of AI to read retinal images and detect early signs of neurodegenerative disorders like Alzheimer's. Because the retina has the same characteristics as neural networks in the brain, retinal scans offer an inflammation-free method of detecting changes even before symptoms occur. Researchers hope it can change the trajectory of early treatment in dementia disorders.

AI is also being used in the treatment of neurological conditions. AI-enabled wearable systems can monitor the real-time brain activity and even predict seizures before they happen; in the instance of epilepsy. This enables the patient to take precautionary actions and possibly lessen the impact of an attack.

Among the most significant developments is the way AI helps in the treatment of stroke. Technology like that created by Viz.AI allowed hospitals to speed up diagnosis and treatment for stroke by quickly analysing patient scans. More than an hour is cut off the stroke patients' waiting time for treatment through this technology, greatly improving survival and recovery rates, states Time.

AI is also revolutionizing neurological research, enabling researchers to understand brain disease more clearly and create more effective treatments. AI algorithms can foresee disease progression and identify new targets for treatment by analyzing millions of brain scans. The NEURii project, for instance, is utilizing AI to analyse more than 1.6 million brain scans in order to forecast a person's risk of developing dementia. Predictive analytics like these have the potential to result in earlier treatment as well as personalized treatment plans for patients.

Though AI is promising, there are legitimate concerns to be considered. Patient confidentiality is of the highest priority, particularly in the case of sensitive neurological information. Then there is the issue of bias—if AI software is trained on non-diverse data, they may perpetuate existing imbalances in diagnosis and treatment. It will be significant to be able to witness AI tools being regulated to a satisfactory extent and being used responsibly in clinical settings in the years to come.

AI has the potential to transform neurology in certain dramatic fashions, from enhancing the accuracy of diagnosis to furthering research in custom-made medicine.

The technology, although having encouraging prospects, also has ethical and regulatory issues that must be handled with sensitivity. As AI continues to evolve, its application in neurology will grow, introducing new technologies to aid doctors and ultimately improving the lives of neurologically ill patients.

Quantum Computing

By Lizzy

If you do computing, I'm sure you'll be familiar with the idea computers store information using bits that can take on the value of either a one or a zero, right? Like how a switch exists in only 2 states: off or on. Well, what if I told you that it doesn't have to be that way. Welcome to the concept of qubits – quantum bits – that can exist in multiple states simultaneously, enabling unparalleled computational power. These qubits can take on richer states that extend beyond just 1 or 0 – they can be in 'superposition', or a complex combination, of both 1 *and* 0.

So, I'm sure you're wondering, what is superposition? What does all this even mean? Let's think about Schrodinger's cat, a famous thought experiment that can illustrate the concept of superposition, which is fundamental to quantum computing. The experiment imagines a cat in a sealed box, with a radioactive atom that has some probability of decaying between the start and end of the experiment. One atom decaying won't harm the cat, but if it decays, it triggers a Geiger counter, which triggers a poison, which kills the cat. Before you open the box, you don't know what the state of the atom is – it's in a superposition of intact and decayed, meaning the Geiger counter is both triggered and not, so the cat is both dead and alive.

According to the thought experiment, opening the box is the only thing that settles the cat into one state or the other; the cat is in a superposition of being both dead and alive until observed, just like how qubits can exist in multiple states simultaneously, its state remaining in superposition until measured.

I know what you're thinking – this sounds like complete nonsense right? A cat that is both dead and alive until observed?! However, this idea of superposition is essential to quantum computing, with quantum computers being able to access new computational abilities that are inaccessible to any classical computer. Already, in October 2019, Google's groundbreaking achievement of 'quantum supremacy' demonstrates the enormous potential for quantum computing. Google claims their quantum computer solved a specific problem that would take a classical computer thousands of years to complete, hence achieving quantum supremacy. This advancement opened a window into a future where applications for quantum computing could revolutionise fields like AI and machine learning, financial modelling, cyber security, drug discovery, even weather forecasting, offering solutions once thought impossible.

However, qubits are extremely sensitive to noise and errors caused by environmental interactions – even stray particles of light can introduce errors. Of course, to build practical quantum computers, developing reliable error correction is vital. Nevertheless, even though today's quantum processors are powerful enough to accomplish some contrived tasks more efficiently than even the fastest classical supercomputers, there is still a long way to go. Most current quantum computers have around 50-100 qubits, far from the thousands or millions needed for practical applications. This is because scaling up quantum computers to hundreds or thousands of qubits while maintaining high levels of coherence and low error rates remains a major challenge.

Even so, a recent breakthrough in quantum computing inspired by Schrodinger's cat could lead to more reliable quantum computers. By using 'cat qubits', quantum computers might require fewer qubits for error correction, potentially reducing the number of qubits needed by tenfold compared to other superconducting circuit designs. These cat qubits, created by trapping light in a tiny hole on a chip, can oscillate in 2 distinct ways simultaneously, creating a quantum superposition similar to Schrodinger's cat. This cat qubit shown a remarkable resistance to bit-flip errors, maintaining its state for an unprecedented 10 seconds without errors.

So, while there lies the prevalent problem of error correction for today's quantum processors, the potential applications of quantum computing are vast and game changing. Even though experts estimate it may take several years before quantum computing delivers widespread practical benefits, many major tech companies and research institutions are actively investing in quantum computing research and development to unlock its full potential. Recent advancements like cat qubits and Google's quantum supremacy demonstrate the progress that is being made towards quantum computing and its practical, large-scale implementation across the world.

Video Game Design

By Dahami

Video game design is the process of creating the rules, story characters and world of a game. Designers decide the specific rules upfront and create gameplay environments and characters as they go along with production. Some common video game design subdisciplines are world design, level design, system design, content design, and user interface design.

Just like film directors video game designers shape the general look of the game but has overall artistic and technical control - they bring together all game play components, storylines and other visual elements to make users feel this one unified interesting experience.

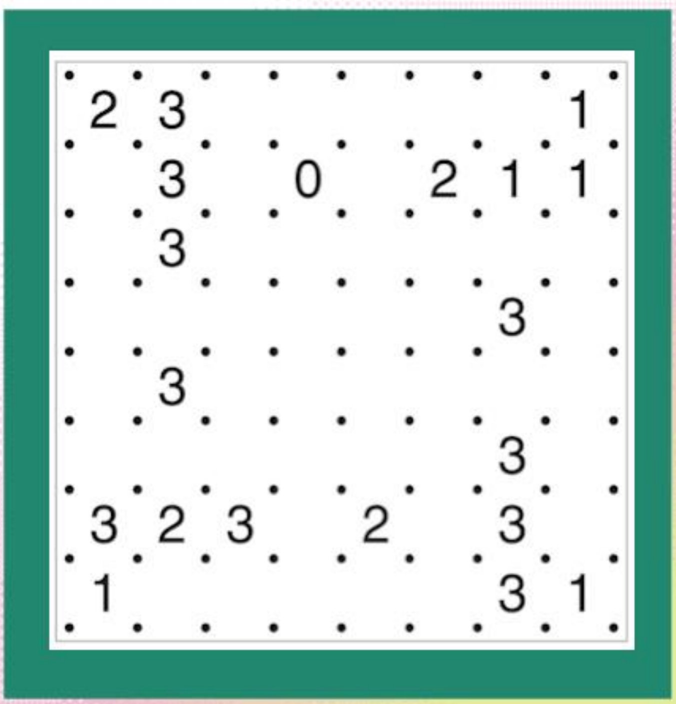
Shigeru Miyamoto had a hand in laying the foundation for contemporary game design through super Mario bros and the legend of Zelda, known for his cinematic storytelling and innovative game play. Hideo Kojima is the person behind Metal Gear Solid and Death Stranding. Building the games of the Elder Scrolls and Fallout series around the concepts of open-world exploration and player choice is Todd Howard.

Video Game design overlaps with art as game design requires a blend of creative thinking and technical understanding. Designers must be able to communicate their vision clearly to artists and developers. Art enriches the games' content, enhancing its content and making the game enjoyable and enthralling. Very good design therefore helps in providing the users' cognitive engagement with the game, in that colour, symbols as well as perspectives makes sense of everything in the real word - abiding by the laws of nature.

Coding is central to developing games from the design of game engines to the creation of game mechanics. Computer scientists use programming languages such as C# and C + + which are used in engines like unity and unreal engine for creating games like Fortnite and Pokémon Go respectively to shape mechanics, AI and physics. Python is also popular for prototypes while JavaScript enables browser-based games such as slither.io.

Computer science plays a key role in essentially bringing the game to life through technical implementation so that both aspects work together to create a fully functionally engaging game .

Video game design is set to develop in the future with advancements of technology. Virtual reality (VR) is a stimulated experience which employs 3D near-eye displays and pose tracking, giving the user immersive and interactive experiences. This development will offer users deeper and more engaging worlds, allowing users to experience more lifelike, interactive worlds and making games feel like real-life adventures Another advancement is cloud gaming, allowing users to play games on a remote server rather than on a local device. This enables users to play high-quality games without needing powerful hardware lowering the barrier to entry, overall giving users more accessible and enjoyable gaming experiences.



Puzzle #4 - Slitherlink

Slitherlink is another puzzle created by games and puzzles publisher Nikoli. It is played in a grid of dots. The aim is to create a single shape using the dots. The numbers inside squares of the dots indicate how many lines there are surrounding them.

This specific grid was made by https://www.gmpuzzles.com/blog/tag/slitherlink-2+classic/

Threats of Cyber-Attacks
By Amelia

What are cybersecurity threats?

Cybersecurity threats are actions conducted by malicious people with the intention of stealing information, damaging computers, or interfering with computer systems. Malware, social engineering, denial of service (DoS), injection attacks, and man in the middle (MitM) attacks are common types of cyberthreats.

What are some of the most common sources of cyber threats?

- **Criminal groups**: organized hacker groups conduct cybercriminal activities like phishing, spam, and malware to extort, steal private data, and run online scams for profit.
- **Nation states**: hostile nations launch cyber-attacks on local entities to disrupt communications and cause damage.
- **Hackers**: individuals who target organizations with various attack techniques, motivated by gain, revenge, financial profit, or politics.
- **Malicious insiders**: employees with legitimate access may abuse privileges to steal or cause damage for personal gain; insiders can be insiders of the organization or outsiders with impersonating accounts.
- **Terrorist organisations**: launch cyber-attacks to damage critical infrastructure, threaten security, disrupt economies, and harm citizens.

What are the different types of threats?

One type of cybersecurity threat is a malware attack. Malware (abbreviation of "malicious software") is the most common kind of cyberattack and includes viruses, worms, trojans, spyware, and ransomware. Malware typically enters a system through an unapproved software download, an email, or a link on an unreliable website. It installs itself on the target system, gathers private information, modifies and prevents access to network components, and has the power to erase data or completely shut down the system.

Another type of threat is a social engineering attack. Social engineering is a method of tricking users into offering malware access. Because the attacker pretends to be a legitimate actor, the victim unintentionally installs malware on their device or shares sensitive information.

Software developers and vendors are facing a new kind of threat: supply chain attacks. Its goal is to use source code, build procedures, or software update mechanisms to infect trustworthy applications and spread malware. In order to compromise the build and update process, change source code, and cover up malicious content, attackers search for insecure network protocols, server infrastructure, and coding techniques. Because the compromised applications are signed and certified by reliable vendors, supply chain attacks are particularly serious. The software vendor is unaware that its updates or applications are infected with malware in a software supply chain attack.

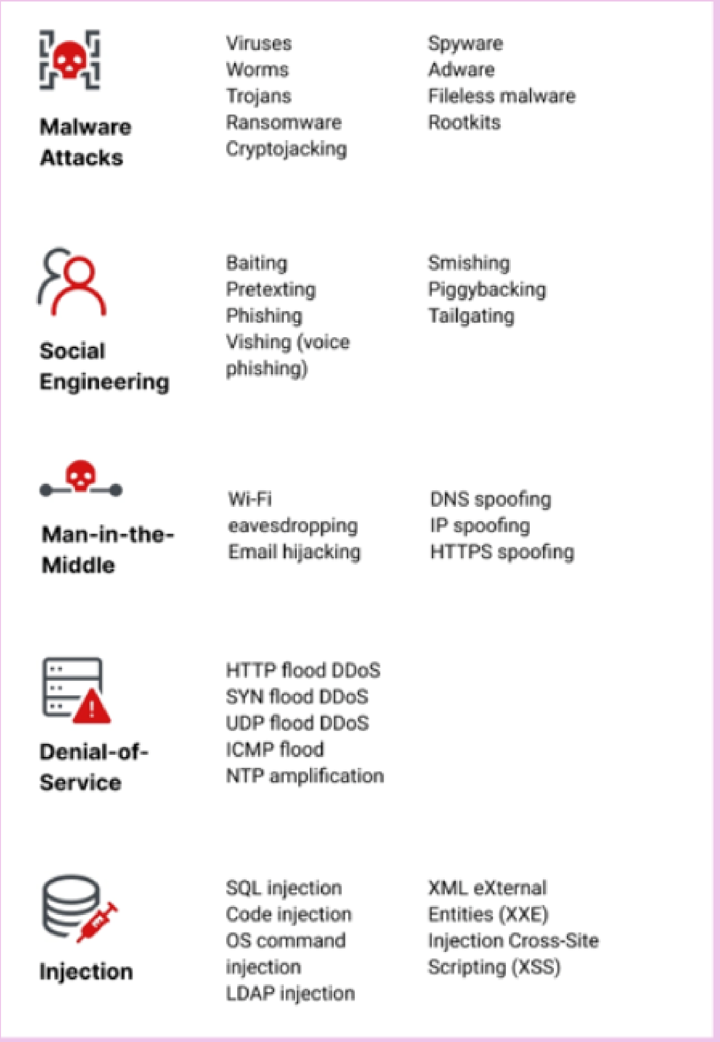
Intercepting communication between two devices, such as a user and an application, is known as a Man-in-the-Middle (MitM) attack. The attacker has the capacity to impersonate each party involved in the conversation, eavesdrop on the communication, and steal confidential information.

By flooding the target system with traffic, a Denial-of-Service (DoS) attack prevents the system from operating normally. A distributed denial-of-service (DDoS) attack is one that involves multiple devices.

In order to directly introduce malicious input into a web application's code, injection attacks take advantage of several vulnerabilities. Attacks that are successful could compromise the system as a whole, reveal private data, or launch a denial-of-service attack.

How can you protect yourself against these threats?
Organisations use cybersecurity solutions as tools to help protect themselves from physical disasters, unintentional damage, and other threats. The main types of security solutions are as follows:

- **Network security**: monitors and manages potentially malicious traffic to block threats.
- **Endpoint security**: deployed on servers and workstations which prevents threats including malware and unauthorized access.



- **Threat intelligence**: integrates various attack data to enhance security event understanding, detection, and response design.
- **Application security**: tests vulnerabilities, protecting software from network and web attacks.
- **Cloud security**: secures public, private, and hybrid clouds by detecting and fixing security vulnerabilities.
- **Internet of Things (IoT) security:** enhances protection for devices handling sensitive data by offering visibility and improved security.

The RSA Algorithm
By Nithika

The RSA algorithm is a cryptosystem used to encrypt messages and data to securely transmit this data over a network. Despite its creation and publication in 1977 created by Ron Rivest, Adi Shamir and Leonard Adleman, it is still used widely today, though quite a few vulnerabilities have been found, reducing its strength from when it was first used. The National Institute of Standards and Technology believes that 2048-bit RSA keys should be able to provide sufficient protection against decryption until at least 2030. With the end of RSA's usage slowly approaching, the logic behind this complex algorithm is worth looking at.

RSA is an asymmetric cryptography method, using a public key known to everyone for encryption and a private key used for decrypting, which must be kept secret by the receiver. For example, if Computer A is sending a message to Computer B using asymmetric encryption, Computer A will encrypt the message using Computer B's public key, creating the ciphertext. Once Computer B receives the encrypted message, it will decode the message using its private key to retrieve the original plaintext, allowing for secure communication. The ciphertext cannot be decrypted using the original public key used to encrypt it.

In order to securely transfer a message, the RSA algorithm uses 4 key steps: key generation, key distribution, encryption and decryption.

Step 1 - Key Generation

A key is a string of characters, normally numbers or letters, that can be used to encrypt/decrypt messages when processed using a cryptographic algorithm. The length of a key is known as its key length. RSA keys typically range from 1024 – 4096 bits, with 2064 bits commonly being used as the key length. The RSA algorithm first generates the public and private keys.

i. Choose two large prime numbers, p and q. These two prime numbers should remain secret. A primality test is normally used to find prime numbers for encryption.

ii. Calculate the product of the two prime numbers that have just been chosen to get n. $n = pq$. n will be used in both the private and public key.

iii. Calculate Euler's Totient Function for n ($\Phi(n)$). This function will return the number of numbers in the set of numbers {1, 2, 3, ..., n-1} that are relatively prime/coprime to the input number.

Two numbers are coprime to each other if the two numbers have no common factors other than one. For example, using 8 and 21, 8 has factors 1, 2, 4, 8 and 21 has factors 1, 3, 7, 21. Since 8 and 21 only have 1 as a common factor, they are relatively prime to each other.

For a prime number, the function will return one less than the prime number as all numbers will be coprime to a prime number. The function is also multiplicative, meaning that $\Phi(ab) = \Phi(a) \times \Phi(b)$ if the greatest common divider of a and b is 1 (meaning that a and b are coprime).

$$\Phi(n) = \Phi(pq) = \Phi(p) \times \Phi(q) = (p-1) \times (q-1)$$

$\Phi(n)$ will be kept secret.

iv. Choose a large integer e, such that $1 < e < \Phi(n)$ and e and $\Phi(n)$ are coprime. e will be used as part of the public key.

v. Calculate d using the $ed \equiv 1(\text{mod } \Phi(n))$.

mod calculates the remainder when one number is divided by another. For example, 12 mod 5 = 2.

$a \equiv b \ (\text{mod } m)$ means that indicates that a is congruent to b mod m. This means that both a and b have the same remainder when divided by m.

The modular multiplicative inverse is an integer X such that $AX \equiv 1 \pmod{M}$. The value of X should be in range of {1, 2, ..., M-1}.

The value of d can be found by testing each value from 1 to $\Phi(n) - 1$, or by using a more complex but faster process known as the Extended Euclidean Algorithm.

The Euclidean Algorithm calculates the greatest common divisor (gcd(a, b)) of two numbers by dividing the larger number by the smaller, and then repeatedly dividing the smaller number by the remainder until the remainder is 0. So, to find the greatest common divisor of 270 and 192:

$$(1)\ 270 = (1 \times 192) + 78$$

$$(2)\ 192 = (78 \times 2) + 36$$

$$(3)\ 78 = (36 \times 2) + 6$$

$$(4)\ 36 = (6 \times 6) + 0$$

This means that the greatest common divisor of 270 and 192 is 6.

The Extended Euclidean Algorithm calculates 2 integers, x and y, such that $ax + by = \gcd(a, b)$ by reversing through the steps from the original algorithm.

Starting with step (3), $78 = (36 \times 2) + 6$, we can rearrange to get:

$$(5)\ 6 = 78 + 36(-2)$$

We can then rearrange step (2) to get:

$$(6)\ 36 = 192 + 78(-2)$$

We can substitute step (6) into the 36 in step (5) to get:

$$(7)\ 6 = 78 + (198 + 78(-2))(-2) = 78 + 198(-2) + 78(4) = 78(5) + 198(-2)$$

We can rearrange step (1) to get:

$$(8)\ 78 = 270 + 192(-1)$$

Finally, we can substitute step (8) into the 78 in step (7) to get:

$$(9)\ 6 = (270 + 192(-1))\,(5) + 198(-2) = 270(5) + 192(-5) + 198(-2) = 270(5) + 192(-7)$$

From this we can see that $x = 5$ and $y = -7$.

For the RSA algorithm, we get that $ed + (\Phi(n) \times y) = 1$ as $\gcd(e, \Phi(n)) = 1$ since e and $\Phi(n)$ are coprime. Taking mod $\Phi(n)$ of both sides means we can remove $(\Phi(n) \times y)$, as $(\Phi(n) \times y) \bmod \Phi(n)$ will be 0. This gives us $ed \equiv 1 (\text{mod } \Phi(n))$. As a result, using the Extended Euclidean Algorithm, we can find a value for d.

d will be kept secret as part of the private key.

The public key will be created using (n, e) and the private key will be created using (n, d)

Step 2 - Key Distribution

If Computer A wants to send information to Computer B, Computer B's public key (n, e) will be transmitted to Computer A. Computer B's private key (n, d) will not be transmitted.

Step 3 - Encryption

A message M will be encrypted using the receiver's public key to create a ciphertext C. The message will first be converted to a numerical form. This can be done by using ASCII to get numerical values for each letter, which will be referred to as m.

Using the public key (n, e), the letters of the ciphertext, which will be referred to as c can be calculated using:

$$c = m^e \ (\text{mod } n)$$

This will calculate a value for each letter of the ciphertext, which will then be sent to the recipient computer.

Step 4 - Decryption

The recipient computer can use its private key (n, d) to retrieve the plaintext using:

$$m = c^d \ (\text{mod } n)$$

RSA is used in a wide range of applications, such as in VPNs, communications, online banking and e-commerce. One of RSA's biggest advantages is that it allows for the use of digital signatures. A message being sent can be signed using the sender's private key and can be verified using the recipient's public key, allowing for transmission of messages and data to be authenticated. However, it does have its disadvantages. RSA has to use large key sizes in order to be secure. 512-bit RSA is no longer secure, and keys of this length can be found using brute force attacks in just hours. Longer key sizes means that more storage is required, and more time may be needed for decryption. This also contributes to its slow processing speeds, making it less suitable for some applications where data may need to be decrypted quickly. Private keys can also be found through side channel attacks, which collect information from side channels and look at timing variability to get the private key. RSA's biggest disadvantage is that it will likely be vulnerable to quantum computers. Shor's algorithm is a quantum algorithm used to find the prime factors of an integer and can possibly factorise large integers quickly and efficiently on an ideal quantum computer, something which can take a very long time on a classical computer.

Overall, RSA's strength has slowly declined over its life, but with a variety of ways to strengthen it such as by increasing the key length, the algorithm has managed to continue to ensure its security. However, as advances of technology continue and the improvements in quantum computing, RSA and similar methods of cryptography may one day have to be replaced with stronger and much more complex algorithms.

Quantum Supremacy: The Rise of Quantum Computing

By Arjun

What is Quantum Computing?

Richard Feynman, one of the most important physicists, first proposed quantum computing in the 1980s, consequently forging the relationship, that we currently see today, between physics and computer science.

Feynman desperately wanted to uncover the secrets of the quantum realm and to achieve this, he needed to directly observe quantum events in real-time. This feat however was impossible because of the fragility surrounding quantum systems, containing completely different sets of laws that we are unfamiliar with. Instead, he began to design a simulation capable of mimicking quantum events. Whilst performing such simulations it became apparent to him that his current computer systems were inefficient for such complex calculations.

Feynman in his unrelenting pursuit of quantum knowledge continued to contemplate a variety of methods to establish the simulation. During his studies he reached a pivotal moment of insight, this breakthrough changed the trajectory of quantum mechanics forever. This concept laid the foundation of quantum computing, it was to create a computer system made up of quantum elements itself, using the laws of quantum physics.

In essence, quantum computing was originally proposed towards generating quantum simulations by performing complex simultaneous calculations.

Quantum Computers: How it Works and Why it's Unique?

Classical computers and all the devices/embedded systems that surround us have one thing in common to process information, they use bits. Bits are fundamentally small units used in computing that represent either a 1 or 0, forming the foundation of computing to store and process information. However, the main limitation is that they can only be at a single state (1 or 0) at a time, restricting them to only solve complex computational calculations using trial and error. The world's fastest supercomputer would be able to simulate 20 electrons but anything greater will require up to a lifetime of calculation before an accurate answer is returned, even with all the computers in the world operating together or, for a more constructive scale, if there was a supercomputer as big the world it would still be unable to solve it.

On the other hand, quantum computers have the proficiency to solve it, very efficiently too. Quantum computers use qubits which is the basic unit for quantum information. Physically qubits can be any quantum system containing two states (1 or 0), capable of being in any one of the two states at the same time, bypassing the limits of a normal bit. Additionally, due to the properties of qubits, theoretically, quantum computers can solve problems thought to be intractable on normal computers. Intractable problems are problems that take extended periods to be solved, up to millions or billions of years.

Think of a qubit as a sphere, technically known as a Bloch Sphere, remember that when a qubit is measured for its value it collapses into either one of the two states (a 1 or 0). In the middle of the sphere, there is an axis (a point where an object rotates) with an arrow attached to this axis, this arrow can point in any direction. When the arrow points straight downwards the qubit collapses into a 0 when measured and when pointing straight upwards it collapses into a 1. However, the arrow can point in any direction, and when it does it is called a superposition state, meaning that when measured there is a probability for it to collapse into either state. The probability of a certain state increases when the arrow points closer to its direction (up or down).

Quantum physicists change this probability by taking advantage of the wave-like behaviours a qubit possesses so they can force qubits to predict the correct answers. Qubits have wave-like behaviours as they can be represented as a wave function (mathematical version of a physical wave), so experience some fundamental wave properties: superposition and interference. This is the reason why a qubit is in a superposition state; it has two amplitudes (two probability amplitudes) one for the qubit going into state 0 and another for the qubit going into state 0 which overlap so superposition occurs as the multiple states are added together to create the final wave function.

Interference is then used to force the qubits to output the answer using two types of interference: constructive and destructive. Constructive interference causes a specific state's amplitude to be increased, therefore increasing the chance that the state will return the correct result. Destructive interference causes a specific state's amplitude to decrease, therefore reducing the chance of incorrect answers being outputted. This grants it the ability to solve intractable problems such as the Shors algorithm.

What are the Problems Affecting Quantum Computers?

Qubits are very sensitive towards surrounding particles due to their property of entanglement. Entanglement is when qubits entangle with other qubits causing them to be a part of one quantum state, hence changing one of the qubit's probability changes the others as well. Entanglement can also cause the qubits to entangle with the surrounding environment such as radiation from phones, noise, heat or any other type of rogue particle. This occurrence is called decoherence which induces the incorrect probability in qubits and is the reason for the incremental steps towards quantum computing. Currently, companies are trying to construct quantum computers with a zero percent error probability by using different particles to act as the qubits which are more stable and to perfect their quantum algorithms so they will always output the correct answer.

What is the Potential of Quantum Computing?

In 2019 quantum computers gained quantum supremacy as the Google Sycamore quantum computer with 53 qubits performed a calculation significantly faster than that of the world's fastest supercomputer at that time, the Summit with 2.4 million CPU and GPU cores with 10PetaBytes of RAM, demonstrating that they can solve certain problems much faster than classical computers. The

Sycamore completed the calculation in 200 seconds while the Summit was estimated to take 10,000 years to complete the calculation.

More recently Microsoft revealed their new first quantum processing unit called the Majorana 1 chip after 17 years of research, this was said to be the beginning of the quantum age due to the massive leap forwards in quantum mechanics. The Majorana 1 is powered by a topological qubit using a newfound material called a topoconductor which they self-engineered. These topoconductors help create an entirely new state of matter only theorised by physicists until last year where they were able to physically observe it and are now capable of controlling and interacting with it; these exotic particles that can be used as qubits are called Majorana zero modes. These qubits are claimed by Microsoft to be stable, fast and digitally controlled. Powerful by design and incorporates error resistance at the hardware level making it more stable by reducing the effect of decoherence. Microsoft's team redesigned how they measured each qubit vastly simplifying how quantum computing works, so has the proficiency to hold scale up to 1 million qubits on a single chip, currently holding 8 qubits. The chip's initial measurement is at a 1% error probability, but Microsoft stated they are on their way to significantly reduce it.

It is believed by Microsoft and many other companies that reaching a system containing a million qubits can help us solve problems faced in many fields such as chemistry, material science and other industries. For instance: self-healing materials, catalysts to break down microplastics and enzymes for more effective healthcare. Furthermore, people believe that merging AI and quantum computers will cause us to reach the peak of technological advancement, it would allow us to simply design and simulate a range of items and receive the correct product the first time, with no trial and error, AI can transform answers from quantum computers into language we can understand without any translation. Thus, we will be able to tackle problems at fundamental levels, finding new materials, new chemicals, and new discoveries to tackle the problems we face today.

Mankind is defined by the discoveries they make along the way, therefore what do you think would happen when we can radically gain the solutions to solve and fix problems to manipulate life around us?

Sources

- https://www.youtube.com/watch?v=-UlxHPIEVqA&ab_channel=DomainofScience
- https://en.wikipedia.org/wiki/Quantum_algorithm
- https://www.ibm.com/think/topics/quantum-computing
- https://builtin.com/hardware/quantum-computing
- https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/

Artificial Intelligence and Matrices: The Mathematical Backbone of Machine Learning

By Janet

Artificial Intelligence (AI) is changing the way we work and live, from improving healthcare to enhancing financial decisions. A key mathematical tool that helps AI function is the matrix. Matrices provide a structured way to store and process information, making them essential in AI applications such as learning patterns, recognising images, and understanding languages. Without matrices, many of the advanced AI technologies we rely on today would not be possible.

The Role of Matrices in AI

AI systems rely on matrices to handle large amounts of data. In machine learning, matrices store information and help computers recognise patterns in numbers, text, or images. Neural networks, a type of AI model, use matrices to process and improve their understanding over time. For example, in computer vision, AI converts images into matrices of numbers so it can recognise objects like faces or cars. An image in grayscale can be represented as a matrix where each number corresponds to a pixel's intensity:

$$\begin{bmatrix} 0 & 255 & 128 \\ 64 & 128 & 192 \\ 255 & 0 & 64 \end{bmatrix}$$

Here, 0 represents black, 255 represents white, and values in between represent varying shades of grey.

In language processing, words are turned into numerical values stored in matrices, allowing AI to understand and generate text.

Another useful application of matrices in AI is reducing data complexity. Sometimes, AI systems must analyse large datasets that are too big to process efficiently. Techniques like Principal Component Analysis (PCA) simplify the data by keeping the most crucial details while removing unnecessary information. This makes AI work faster and more accurately in making predictions or recommendations. Similarly, recommendation systems, like those used by Netflix and Amazon, use matrices to analyse user preferences and suggest relevant content.

Matrices also play a role in robotics and automation. Robots need to process information about their environment, such as their position and movements. Matrices help with these calculations by representing distinct positions and angles, allowing robots to navigate spaces efficiently. In self-driving cars, matrices process sensor data to detect obstacles, identify road signs, and make driving decisions in real-time. For example, the transformation of a robot's position in space can be represented using a rotation matrix:

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

where theta is the angle of rotation. This matrix helps in calculating how a robot or a self-driving car should adjust its movement when turning or changing direction.

Connecting Matrices to Further Mathematics

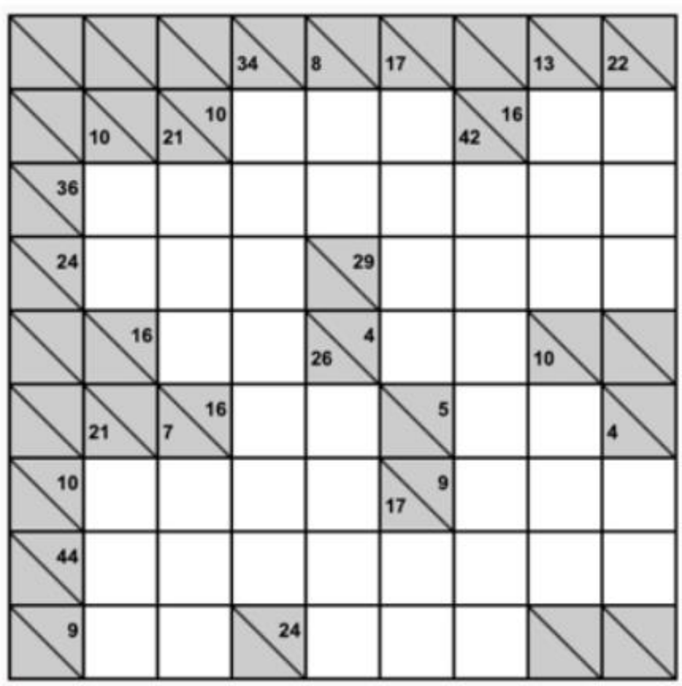
Matrices are not only useful in AI but also play an important role in mathematics. They help describe how objects move and change, which is useful in physics and engineering. In AI, matrices help adjust models so they can learn better, making them more accurate over time. For example, gradient descent, an optimisation method used in AI training, relies on matrix operations to fine-tune algorithms and improve their predictions. Understanding how matrices work improves our ability to build smarter and more efficient AI systems.

Beyond AI, matrices are widely used in other fields such as economics, cryptography, and even in 3D graphics for video games and animations. Their ability to organise and manipulate data makes them indispensable in scientific research and technological advancements.

The connection between matrices and AI shows how mathematics supports technological progress. As AI continues to improve, the role of matrices will become even more important in making machines smarter and more capable. Learning about matrices helps us understand how AI works and how it can be used to solve real-world problems. The future of AI will depend on further refining these mathematical tools, ensuring continued advancements in smart technology. Whether in AI, robotics, or other scientific fields, matrices will remain a fundamental tool in shaping innovation and progress.

Puzzle #5 - Kakuro

Kakuro is another puzzle created by games and puzzles publisher Nikoli. The aim is to fill the empty white cells with digits 1-9 so that the numbers add up to make the numbers in the grey boxes to the left/above them. Duplicate digits cannot be used in any one group of digits. For example, at the top, there are 3 empty boxes which add up to 10 as shown by the grey box on the left. 2, 6, 2 would not be an appropriate solution for these empty boxes as 2 is used twice.



This puzzle was made from https://www.kakuroconquest.com/

AI and Neuromorphic Computing

By Ethan

Artificial Intelligence has rapidly evolved, reshaping industries ranging from healthcare to finance. However, traditional AI models face significant challenges, including high power consumption and inefficiencies in real time learning. Neuromorphic computing (inspired by the human brain) presents a promising alternative, offering energy efficient and adaptive processing. This article explores the intersection of AI and neuromorphic computing, examining how this emerging field is revolutionising computing paradigms and linking AI with neuroscience and physics.

The Foundation of Neuromorphic Computing

Neuromorphic computing aims to replicate the structure of biological neural networks through hardware and software. Unlike Von Neumann Architecture, which separate memory and processing units, neuromorphic systems integrate computation and memory, mimicking the parallel processing of the brain.

AI and Neuromorphic Computing: A Symbiotic Relationship

Traditional AI models excel in pattern recognition and large-scale data processing but struggle with real time adaptation and efficiency. Neuromorphic computing addresses these limitations by:

Reducing Power Consumption: Neuromorphic chips consume significantly less energy, making AI deployment easier in IoT devices.

Enhancing Real time Learning: Unlike conventional deep learning, which requires extensive retraining, neuromorphic systems can adapt dynamically based on new inputs, similar to biological learning.

Improving Computational Efficiency: By processing data in parallel and locally storing information, neuromorphic systems eliminate bottlenecks associated with traditional architectures.

Interdisciplinary Connections: AI, Neuroscience and Physics

Neuromorphic computing sits at the crossroads of multiple disciplines, particularly neuroscience and physics:

Neuroscience: By emulating the brain's spike-based communication, neuromorphic systems provide insights into cognitive processes and disorders such as Alzheimer's and Parkinson's.

Physics: The development of quantum neuromorphic computing leverages principles of quantum mechanics, which can lead to more efficient computing models.

Real World Applications and Future Prospects

Neuromorphic AI can be applied across various industries:

Healthcare: AI driven neuromorphic devices can enhance brain to computer interfaces (aiding patients with neurological disorders).

Autonomous Systems: Energy efficient AI enables real time decision making in robotics, self-driving cars and drones.

Cybersecurity: Adaptive threat detection powered by neuromorphic AI strengthens defence mechanisms against evolving cyber threats.

Research in neuromorphic computing is expected to accelerate with advancements in:

Quantum Neuromorphic Systems: Combining quantum computing with neuromorphic principles could change AI's computational capability.

Brain to Computer Integration: Further advancements may lead to direct communication between AI systems and human brains, opening doors to enhanced cognitive performance.

Low Power Edge AI (IoT Devices): Neuromorphic processors will play a crucial role in enabling smart and energy efficient AI in IoT devices.

Neuromorphic computing represents a transformative approach to AI, bridging the gap between biological intelligence and digital processing. By integrating principles from neuroscience and physics, this field is driving innovation in AI, making it more efficient, adaptable and scalable. As research progresses, neuromorphic AI holds the potential to reshape industries, enhance human to computer interactions and bring AI closer to true human like intelligence.

Algorithmic Trading

By Leo

I'm sure many of you have heard about the term trading. Whether it be in the foreign exchange markets, stock markets or cryptocurrencies I'm certain we all have a basic understanding. Tradespeople buy stocks and shares in products when they are low and use their knowledge of the market to predict when the value of it will increase, so that they can sell it to make a profit. In simple terms, algorithmic trading uses computer programs to create models that suggest when it is suitable for a user to buy and sell shares and stocks. The use of multi-tasking with multi-core CPU's is essential for many traders as it allows them to create models for future trades, based large amounts of old data that the computer processes.

Algorithmic trading allows for tradespeople to work at a quicker rate. This is since a lot of the thinking they would have to do is processed by a clever CPU in seconds. These CPUs are designed to have many cores. This allows them to process large amounts of data at a faster rate as the multiple processors means that each can tackle an individual task quickly. Hence, the computer can suggest when it is right for the user to buy or sell a share, in a matter of seconds. Furthermore, it means that place multiple trades at once without having to pay 100% attention to each as the computer monitors the trade's trajectory and sells when the user makes a suitable profit. Increased rate of trading is a massive benefit for traders, so this aspect of algorithmic trading elevates the trading experience and ultimately can maximise profits.

In addition, algorithmic trading requires large amounts of data to be analysed at fast rates. This concept overlaps with computer science as this is an example of data mining. The 3-v's aspect of big data mining is applied here as there is a great volume of various data that needs to be processed quickly. This data is previous charts of stocks over many years, in every commodity, stock, foreign and cryptocurrency. Moreover, the context of each turn in the chart must be researched in order the increase the validity of the algorithm. This is due to the fact that many currencies (particularly currencies and stocks) are affected by real life events. However, these factors need to me made understandable for the computer to comprehend. This process also takes time which is why it is essential that the device used to process this data contains a CPU with many cores, or if possible, a GPU.

Finally, the automation of trades in algorithmic trading is a concept covered in Computer Science also. Using the data mining to suggest when the user should buy and sell their shares, the computer simulates the outcome of this thousands of times, considering many different outcomes and possibilities to suggest the best for the user. Stop-losses are put in place which prevent a user from losing too much money if the trade goes wrong, while take profits are implemented to take the profit for the user once it reaches a certain amount. The computer must set these and automatically takes the profit or stops the loss for the user. This means that the user does not have to watch the trade as it happens as if the loss becomes too great the computer will detect this and 'cash out'. This is based on the algorithm that can be created partly by the computer and the user and uses if or selection statements. In pseudocode a simple stop loss would be like:

```
Function stop.loss()
WHILE stock!= 10
  Stop loss==False
Endwhile
Stop loss==True
Function stop.loss()
```

A benefit of this is the increased risk management as the computer detaches emotions from the trade and uses practicality rather than greed, fear or excitement. This allows the user to minimise losses and benefits them as a trader overall.

Algorithmic trading is just one example of a link between computer science and finance but there are many more examples of connections between computer science and other fields and professions due to the versatility of the subject. Computers are very clever and even things like trading which may be viewed as a human job can be made computational and digital.

Cryptography and Cybersecurity in the Quantum Age

By Toby

With the steady progress of quantum computing, many new opportunities are opening up in the field of computer science. By storing information in quantum bits, or 'qubits', quantum computers are able to solve problems that would otherwise be intractable for classical computers. Qubits utilise certain principles of quantum mechanics (which is the physics of how very small, light objects work) in order to improve the computer's performance. For example, superposition gives a way for the state of a particle to exist as the combination of multiple states. Playing the same song from two nearby speakers will result in you hearing the one song, but louder than if it was only played from one of the speakers; the volume of the song is a sum of the volume of the song being played from each speaker. Qubits can use this to hold multiple possible configurations at once, allowing them to process several equations simultaneously. Other principles such as quantum entanglement, which can allow for information in several qubits to be determined from measuring one, can also be used to speed up calculations.

These super-fast calculations can be used for improvements in many fields, like massive data handling, or the development of new medicines. However, with these advancements, there are also advancements in less favourable fields.

Currently, most sensitive data is encrypted using a method called public key cryptography. This is where two 'keys' are used in sending a message: one to encrypt it, and one to decrypt it. These keys are generated by multiplying extremely large prime numbers together and would take so long to calculate using classical computers that they are basically impossible to work out and have the encrypted information still be relevant. However, with the advent of quantum computers and their massive calculation power, it's entirely possible that this method of encryption will soon become child's play to crack.

To combat this, new methods of cryptography are being developed using the exact same tools threatening the current methods. Enter quantum cryptography: methods of encrypting data securely using the inherent principles of quantum physics. As well as superposition and entanglement, the properties of certain particles are used to do this. For example, photons (or particles of light), have a property called spin of which they can only possess certain values. These spin values can be used as a stand in for 1s and 0s in a classical binary computer.

This property of photons is used in the most common form of quantum cryptography – quantum key distribution, or QKD. This is a way to build a key without the risk of it being discovered or calculated. To do this, a stream of photons is sent between two parties through a fibre optic cable, with their spin values representing 1s and 0s. When these photons reach the receiver, they are sent through a beam splitter. This is a device that randomly splits the photons into one of two paths into a photon collector. The position of the photons that were sent and the position of the photons that were received after being sent through a beam splitter are then compared, and the ones that have changed position are discarded. The photons that are left, and their respective binary values, make up the new key.

Another property of quantum particles can be used to ensure these keys are not discovered: collapse. This is where the superposition of the various states of a particle decay into one state when a measurement is made. In short, quantum systems are fundamentally changed when they are measured or observed. This means that if someone gains access to the cable used to send the photons, the two parties involved will be able to tell, and create a new key.

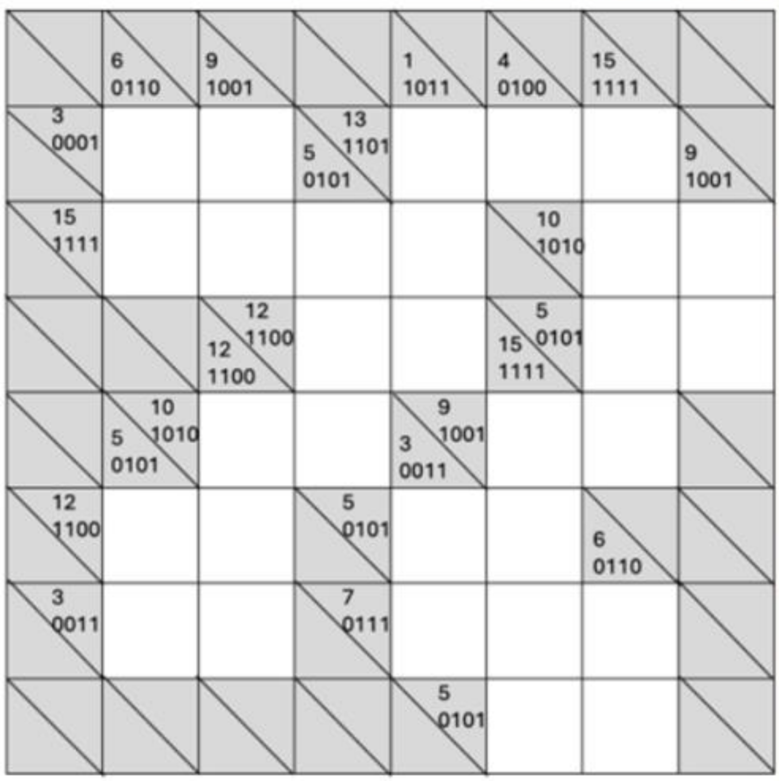
With today's vast advancements in technology, not everything will be used to improve our lives. Planning ahead can help avert the worst of these effects, and tying fields together can give us even further progress. (For anyone interested, consider reading about post-quantum/structured lattice cryptography :D)

Sources:

- [What Is Quantum Computing? | IBM]
- https://www.ibm.com/docs/en/integration-bus/10.0?topic=overview-public-key-cryptography
- [What is Quantum Computing? - NQCC]
- [Next steps in preparing for post-quantum cryptography - NCSC.GOV.UK]
- [What Is Quantum Cryptography? | IBM]
- [What is Quantum Key Distribution (QKD) and How Does it Work?]
- [What Is Post-Quantum Cryptography? | NIST]

Puzzle 6# - Bakuro

Bakuro is a variation of Kakuro, which uses binary instead of decimal. The white cells in the grid should be filled using the digits 1(0001), 2(0010), 4(0100) or 8(1000) along with their binary equivalents. As in Kakuro, numbers in the white cells should add up to make the numbers above them/to the left of them and no number can be used twice in any sum.



The Mathematics Behind Machine Learning and its Growing Importance

By Abhirup

Machine learning (ML) has revolutionized industries, from healthcare and finance to self-driving cars and natural language processing. At its core, ML relies on a strong mathematical foundation to develop algorithms that can learn from data and make predictions. As the field advances, the role of mathematics in ML will only become more critical, shaping the next generation of intelligent systems.

The Mathematical Foundations of Machine Learning

Mathematics is the backbone of machine learning, providing the tools needed to create and optimize models. Some of the key mathematical disciplines involved include:

1. Linear Algebra

Linear algebra is fundamental to ML, as it deals with vectors, matrices, and tensors—the building blocks of many algorithms. Key concepts include:

- **Matrix operations**: Essential for handling large datasets and performing transformations.
- **Eigenvalues and eigenvectors**: Used in principal component analysis (PCA) for dimensionality reduction.
- **Singular Value Decomposition (SVD)**: Used in recommendation systems and data compression.

2. Probability and Statistics

Probability theory helps in modelling uncertainty in ML predictions, while statistics is used to analyse and infer patterns from data. Key concepts include:

- **Bayes' Theorem**: The foundation for Bayesian inference and probabilistic models.
- **Probability distributions**: Such as Gaussian, Poisson, and Bernoulli distributions used in different ML algorithms.
- **Hypothesis testing and confidence intervals**: Crucial for evaluating model performance.

3. Calculus and Optimization

Most ML models rely on calculus to optimize functions and adjust model parameters. Some key applications include:

- **Gradient Descent**: A fundamental optimization algorithm used in training deep learning models.
- **Derivatives and partial derivatives**: Used to compute gradients in neural networks.
- **Lagrange Multipliers**: Utilized in constrained optimization problems.

4. Graph Theory

Graph theory is essential for neural networks, social network analysis, and recommendation systems. Some key applications include:

- **Graph neural networks (GNNs)**: Used for analysing relationships in complex networks.
- **Shortest path algorithms**: Applied in routing and logistics optimization.
- **Markov Chains**: Used in reinforcement learning and stochastic processes.

5. Information Theory

Information theory measures the amount of information and helps in designing efficient learning systems. Key concepts include:

- **Entropy**: Measures the uncertainty in a dataset and is used in decision trees.
- **Kullback-Leibler Divergence**: Measures the difference between probability distributions.
- **Mutual Information**: Helps in feature selection and dimensionality reduction.

Aspects of Data Science and Statistics in Machine Learning

Machine learning is deeply intertwined with data science and statistics, as these fields provide the methodology to extract insights from data and validate models. Some critical aspects include:

1. Data Preprocessing and Feature Engineering

Raw data is often messy and needs to be cleaned, transformed, and structured before it can be used in ML models. Statistical techniques such as imputation, normalization, and outlier detection play a key role in improving data quality.

2. Exploratory Data Analysis (EDA)

EDA is a crucial step in data science that involves using statistical measures and visualizations to understand the underlying patterns in data. Techniques like correlation analysis, box plots, and histograms help identify relationships and anomalies before modelling.

The Growing Importance of Mathematics in Machine Learning

As machine learning continues to evolve, the role of mathematics will become even more prominent in the following ways:

1. Advancements in Explainable AI (XAI)

Understanding how ML models make decisions is crucial, especially in critical fields like healthcare and finance. Advanced mathematical models are needed to develop interpretable ML systems that can provide transparent reasoning behind predictions.

2. Development of More Efficient Algorithms

Mathematics helps optimize algorithms to reduce computational costs and increase efficiency. For example, innovations in convex optimization and sparse matrix computations have led to faster ML models with lower memory usage.

3. Quantum Machine Learning

With the rise of quantum computing, mathematical models that bridge quantum mechanics and ML, such as quantum probability and tensor networks, will be vital in developing next-generation algorithms.

4. AI Ethics and Fairness

Mathematics is key in designing fair and unbiased AI models. Techniques like fairness constraints, causal inference, and game theory are increasingly being used to ensure equitable AI decision-making.

Mathematics is the foundation of machine learning, providing the theoretical framework for developing smarter and more efficient models. As AI and ML continue to advance, mathematical innovations will play a critical role in shaping the future of intelligent systems. A deeper understanding of mathematical principles—alongside core data science and statistical methods—will be essential for researchers, engineers, and policymakers looking to harness the full potential of AI while ensuring fairness, efficiency, and transparency.

The Rise of AI Software on iPhones: Transforming User Experience and Economy

By Sanjay

AI has changed the technology sector in many ways. Artificial intelligence (AI) is a set of technologies that enable computers to perform a variety of advanced functions, including the ability to see, understand and translate spoken and written language, analyse data, make recommendations, and more. AI is used across various industries and applications, significantly transforming technology, business, and daily life. These industries include smartphone and consumer electronics, healthcare, finance and banking, business and marketing, transportation, manufacturing and robotics, education and much more. In this article it will mostly be written about "The rise of AI software on iPhone: transforming user experience and economy."

Artificial intelligence (AI) is used in 77 percent of the world and one of the main aspects it's benefited in is smartphones, particularly In Apple phones. Artificial Intelligence (AI) has become a vital part of an Apple iPhone. From enhancing photography to improving personal aid, AI software has revolutionized how users interact with their devices. As Apple continues to integrate AI-driven functionalities, iPhones have become smarter, more intuitive, and increasingly capable of understanding user preferences.

There are many AI-powered features in an iPhone, such as Siri – the AI assistant. Siri is Apple's Ai powered virtual assistant, which has been developed alongside apples IOS updates. Why is Siri a crucial part to Apple users?

Well Siri uses machine learning and natural language processing to understand user queries, provide relevant responses, and perform tasks such as setting reminders, sending messages, and even controlling smart home devices. A simple call out to Siri such as "Hey Siri" gets the user multiple functions to the phone and other smart home devices. The Siri (AI) assistant is a benefit to ppl due to the task speed. AI assistants like Siri enhance efficiency, enabling users to complete tasks faster. This means that it can increase overall workforce productivity while also shifting job roles in tech, customer service, and digital assistant industries. Siri uses an algorithm for this, and that algorithm can be shown below:

```python
def speak(text):
    """Convert text to speech"""
    engine.say(text)
    engine.runAndWait()

def listen():
    """Capture user speech and convert it to text"""
    recognizer = sr.Recognizer()
    with sr.Microphone() as source:
        print("Listening...")
        recognizer.adjust_for_ambient_noise(source)
        try:
            audio = recognizer.listen(source)
            text = recognizer.recognize_google(audio)
            print(f"You said: {text}")
            return text.lower()
        except sr.UnknownValueError:
            return "I didn't catch that"
        except sr.RequestError:
            return "Service unavailable"

def process_command(command):
    """Process user commands and execute tasks"""
    if "time" in command:
        current_time = datetime.datetime.now().strftime("%I:%M %p")
        response = f"The current time is {current_time}"
    elif "open google" in command:
        webbrowser.open("https://www.google.com")
        response = "Opening Google"
    elif "play music" in command:
        os.system("start spotify")  # Example: Open Spotify
        response = "Playing music"
    elif "who are you" in command:
        response = "I am Siri, your virtual assistant."
    else:
        response = "I am not sure, let me search that for you."

    print(response)
    speak(response)

def main():
    """Main function to run Siri-like AI"""
    speak("Hello, how can I help you?")
    while True:
        command = listen()
        if "exit" in command or "stop" in command:
            speak("Goodbye!")
            break
        process_command(command)

if __name__ == "__main__":
    main()
```

This proves the basic inputs that Siri can do and use. For photography, people like to take pictures with the high-quality camera the iPhone has to offer. The camera alongside the Apple phone has AI technology integrated with it. The iPhone's camera system is one of the biggest beneficiaries of AI integration. AI-powered computational photography enhances image quality, perfects lighting, and enables features like Portrait Mode, Night Mode, etc.

In today's digital landscape, data is one of the most valuable assets, and AI plays a crucial role in how companies like Apple monetize it. AI plays a key role in how Apple generates revenue by enhancing user engagement through personalized recommendations. Machine learning algorithms analyse user behaviours to suggest music, apps, news articles, and other digital content, increasing the likelihood of purchases and subscriptions. This drives revenue from Apple Music, the App Store, Apple News+, and in-app advertisements. By refining recommendations based on user preferences, AI helps Apple maximize the time users spend on its platforms, contributing to the expansion of the digital economy.

Additionally, Apple sets itself apart by prioritizing privacy-centric AI, processing much of this data on-device rather than relying on cloud-based tracking. This approach not only ensures data security but also strengthens customer trust, making Apple's AI-driven services more appealing in an era where digital privacy concerns continue to grow.

The future of AI on iPhones looks promising as Apple continues to enhance its AI capabilities, introducing more advanced and intelligent features. Siri is expected to become even smarter, with expanded compatibility across non-Apple apps allowing for more seamless interactions. Photography included within the apple industry will see a massive improvement, making video recording and editing easier and more precise. AI-powered automation in the Shortcuts app will help users create more advanced and efficient tasks, saving time and effort. Health monitoring will also improve, using AI to predict potential health issues and provide personalized wellness tips. These updates will make iPhones even smarter and more user-friendly, improving daily life in many ways.

Encryption and Quantum Technologies

By Lev

Until recently, traditional data encryption methods have been considered sufficient to provide secure communication. These methods typically rely on the fact that multiplying two large prime numbers is much easier than doing the inverse, i.e. finding the two original prime numbers from their product.

How do traditional encryption methods work?

RSA is one of the most widely used data encryption methods. RSA takes two large prime numbers and uses their product to generate public and private keys. The public key can be used by anyone to encrypt data that is to be sent to the computer, but the data is practically impossible to decrypt without the private key, which is only known by the recipient. It is infeasible for even today's most powerful super computers to crack such a code, due to the sheer number of possibilities that need to be checked.

A threat to data security

Recent advances in quantum computing – albeit mostly theoretical – have made scientists question how long traditional encryption will remain sufficient. Famously, Shor's algorithm, devised by the mathematician Peter Shor in 1994, provides a theoretical method for decrypting RSA and other such techniques in a matter of minutes, by harnessing the properties of quantum computers. This has put pressure on cryptologists to prepare for when such computers become a reality.

Quantum-proof encryption

To combat the threat of quantum computers being used for decryption, encryption methods are being developed that also use these new technologies. Where traditional encryption uses mathematics, quantum encryption relies on the physical properties of particles.

Quantum Key Distribution (QKD) is one of the most widely researched of these new techniques. It involves the transmission of a random sequence of single photons (light particles) over fibre-optic cables. These photons are passed through polarising filters on the sender's end that affect the photon's 'spin' in a certain manner – in this way, each photon represents a single qubit – the quantum equivalent of a traditional bit, with its direction of spin determining if it is a 0 or a 1. This sequence of photons is received at the other end, and the measurements of each photon compared to the expected ones. Due to the fundamental quantum theory of the 'uncertainty principle', if the photons have somehow been measured between the two nodes by a hacker, their delicate quantum state will have been altered, and therefore the receiver knows that the data has been compromised. This theoretically makes it impossible to bypass QKD, as it is impossible to observe a photon without altering its state.

Challenges with Quantum Key Distribution

QKD, still in its early stages of development, has many practical limitations. For one thing, it relies on the theoretical transmission of a single photon at a time through fibre-optic cables, but such a transmission device is very difficult to manufacture, meaning that a tiny beam of photons is often used instead. This provides a way for data to be intercepted without altering its quantum state, by splitting the beam and measuring part of it.

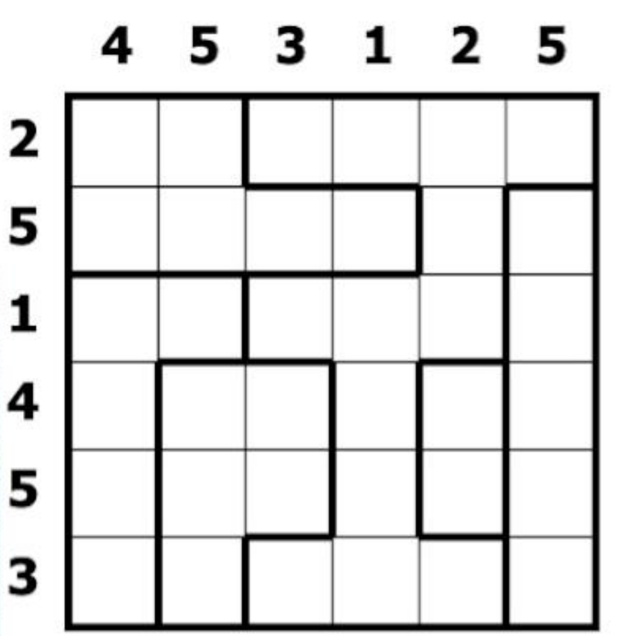
Photons also degrade over distances of 250-300 miles, reducing the range of QKD systems. This required specific infrastructure to be put in place, such as secure nodes that can hold photon repeaters, which must not alter the quantum state of the photons.

Into the future

With the quantum age predicted to be as little as 20 years away, it is vital that the world is prepared for the possible challenges of this new powerful technology. Some high-level organisations such as government services already use quantum encryption for their data. However, it is thought that quantum technology will always have its limitations, as any system must have elements of traditional technology, which will introduce weak points that could be exploited with new, more powerful techniques.

Sites used:

- https://www.techtarget.com/searchsecurity/definition/RSA
- https://www.ibm.com/think/topics/quantum-cryptography
- https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography#:~:text=Post%2Dquantum%20cryptography%2C%20also%20known,quantum%20computers%20become%20a%20reality
- https://en.wikipedia.org/wiki/Quantum_cryptography



Puzzle 7# - Aquarium

Aquarium is made up of a grid split into separate blocks known as aquariums. The aim is to fill the aquariums with water up to a certain level or leave them empty, so that each row/column has the same number of boxes filled with water as shown above. The water level must be the same throughout the block.

This puzzle was made from https://www.puzzle-aquarium.com/

Quantum Computing

By Eric

Quantum computing, a rapidly developing field at the intersection of computer science, physics, and mathematics, promises to change the way we process information. Unlike contemporary computers that rely on bits to represent data as 1s or 0s, quantum computers utilise qubits, which can exist as either both or simultaneously due to the principle of superposition. This unique property, combined with entanglement and quantum interference, allows quantum computers to explore a vast number of possibilities concurrently, potentially solving problems that are intractable for contemporary computers. While the field is still in its early stages, ongoing research and development by companies like IBM, Google, and AWS are paving the way for practical quantum computing applications. From breaking traditional encryption methods to optimising complex systems and accelerating drug discovery, quantum computing holds the key to unlocking unprecedented computational power and transforming various industries in the years to come.

Quantum computing is deeply intertwined with physics and mathematics. Its foundation lies in the principles of quantum mechanics, which describes the behaviour of matter and energy at the smallest scales. This connection is further solidified by linear algebra, complex numbers, and information theory to model and manipulate quantum states. Applied mathematics plays a crucial role in developing algorithms and understanding the computational complexity of quantum systems. This collaboration between physics and mathematics fuels ongoing research and development in quantum computing, leading to new insights and advancements in both fields.

Imagine two coins spinning in the air, connected in a way that if one lands heads, the other must land tails. This is a simplified analogy for entanglement, where two or more qubits are linked in a way that their fates are intertwined, even if they're physically separated. Measuring the state of one entangled qubit instantly reveals the state of the others, regardless of the distance between them. This "action at a distance" is a core concept in quantum mechanics and allows quantum computers to perform calculations in a fundamentally different way than contemporary computers.

Quantum algorithms are designed to leverage the unique properties of superposition and entanglement. They are like specialised programs that exploit these quantum phenomena to speed up calculations for specific problems. For example, Shor's algorithm can factor large numbers much faster than any known classical algorithm, which could have major implications for cryptography. This ability to solve certain problems much faster than contemporary computers is one of the key reasons why quantum computing is so exciting.

Quantum computing is assured to revolutionise computing, with a projected market reaching £64 billion by 2035. While still in its research and development phase, it promises to achieve unprecedented capabilities in processing speed and problem-solving efficiency. Industries are already exploring its applications in areas like supply chain optimisation and financial modelling. The market is expected to reach £40 billion by 2030, indicating that practical applications are closer than many anticipate. The future of quantum computing is bright, with exciting possibilities for transforming various sectors and addressing complex challenges.

The K-Nearest Neighbour Algorithm

By Shourya

What is the K-Nearest Neighbour algorithm?

*"**A man is known by the company he keeps**" - Aesop. KNN works in a similar way.*

The k-nearest neighbours' algorithm (KNN) is utilized in machine learning mainly for classification (but sometimes also regression), popular for its simplicity and effectiveness. It is used widely from text mining and facial recognition to recommendation systems like Amazon, Netflix and Hulu.

What is the basic principle of the KNN algorithm:

As a lazy learner algorithm, it does not process training data immediately, rather it stores it to perform operations on the dataset until it needs to make a prediction. When performing the classification, the algorithm finds the closest k neighbours to a datapoint and takes the majority vote to make its prediction.

For example, if we have a dataset that contains the weight and width and top speed of cars. Now we are giving a new car's top speed, weight and width. Using the new car's values, we can calculate their distances to other datapoints to find the closest k neighbours to the new car (and for simplicity's sake let k be 7). We find that out of the 7 closest neighbours, 2 are sportscars, 1 is a hatchback and 4 are SUVs. Therefore, taking the majority vote, the prediction made is that the new datapoint we were provided is an SUV

How are distances calculated:

There are different mathematical methods to find the closest k neighbours and the method used is dependent on the data provided, efficiency and what the use case is. The methods more complex than a few lines, but to summarise, the common methods of calculating distances when using KNN are:

Euclidian Distance -

The most common distance metric utilized, it is the straight-line distance between two points in Euclidean space.

Manhattan Distance -

The distance between two points if you could only travel in horizontal and vertical lines. Also known as city block distance.

Minkowski's Distance -
A metric that generalizes Euclidian, Manhattan – so is very versatile.

How are k-values calculated:
The number of neighbours to consider during predictions should be decided based from the input data. There are several ways to do this, but some common ways of calculating the optimal k value are Cross Validation and the Elbow method. It is also recommended that an odd value is selected for k to avoid ties in the majority vote.

Cross Validation – The data is divided into multiple folds, and the algorithm is tested on these folds to fine tune the k value, based on its effectiveness.

Elbow Method – Try different values of k to find the trend in k values against a measure of how spread-out data points are, to approximate the value of k that is most effective.

Advantages of KNN algorithm:
- Easy to implement and understand
- The algorithm due to its nature accounts for any new samples added to the training data
- Only has two hyperparameters
- Works for both regression and classification
- Excels in pattern recognition and intrusion detection
- Achieves 97.37% accuracy on the Iris dataset (a common dataset used for machine learning)

Disadvantages of KNN algorithm:
- Suffers from the curse of dimensionality – as the number of features increases KNN becomes less accurate in its classification
- Scalability issues – it has time and space complexity of O(n*d) - where n is the number of datapoints, and d is the number of features and is a lazy algorithm, so it becomes slow and demanding memory-wise when dealing with large quantities of n or d.
- Struggles with imbalanced cases

Applications of KNN algorithm:
The KNN algorithm has a wide range of uses, here are some examples:

- In the finance world, it can be utilized for stock market prediction, identifying patterns in historical data to aid investors in their decisions. It is also used for fraud detection, checking perhaps if a credit card transaction was legitimate.
- In terms of stock market prediction, authors from the International Journal of Business, Humanities and Technology wrote in 2013: "According to the results, KNN algorithm was stable and robust with small error ratio, so the results were rational and reasonable... So, we consider that employing this prediction model, KNN is real and viable for stock predictions." - this was before it was widely used by hedge funds.
- In E-commerce and streaming, it is used to recommend products or episodes by comparing the users' past preferences to the features of other items.
- In security, KNN can be utilized in facial recognition to restrict and allow access

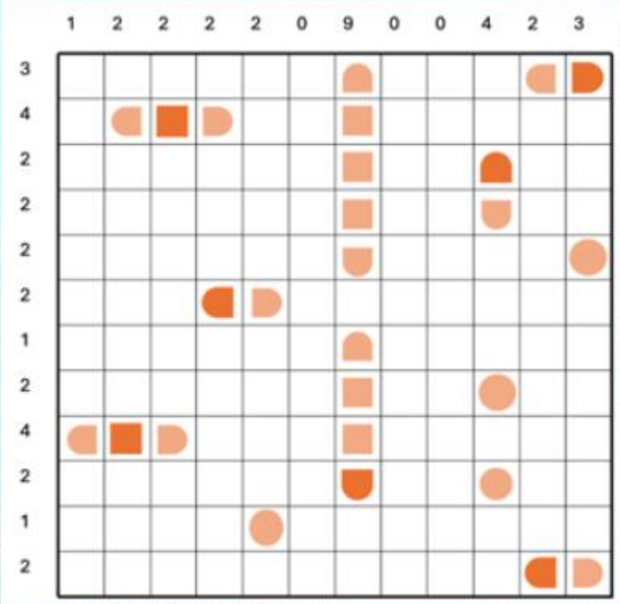
To summarise, KNN is an effective but relatively simplistic machine learning algorithm that can be utilised for both regression and classification. It works by finding the closest k neighbours to a given datapoint and taking the majority vote. The k-values that are used, and the distance metric used affect its performance based on the data the algorithm is working with. And, although it is good at what it does, the algorithm has many scalability issues.

Sources:

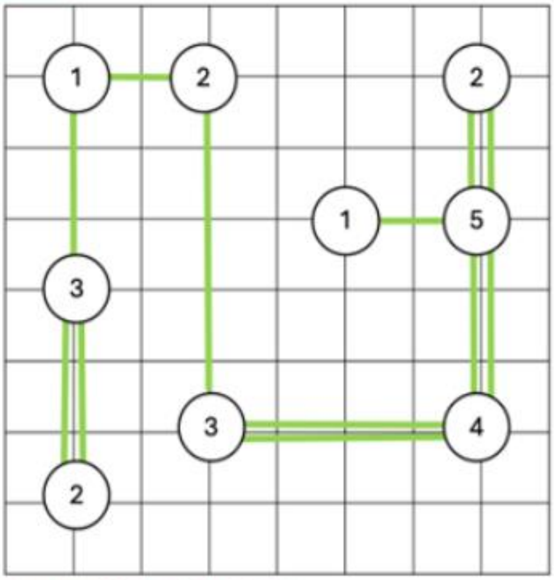
- https://www.ibm.com/think/topics/knn
- https://keylabs.ai/blog/k-nearest-neighbors-knn-real-world-applications/
- https://www.geeksforgeeks.org/k-nearest-neighbours/
- https://www.ijbhtnet.com/journals/Vol_3_No_3_March_2013/4.pdf

Puzzle Answers

#1 – Battleship Solitaire



#2 – Bridges/Hashi

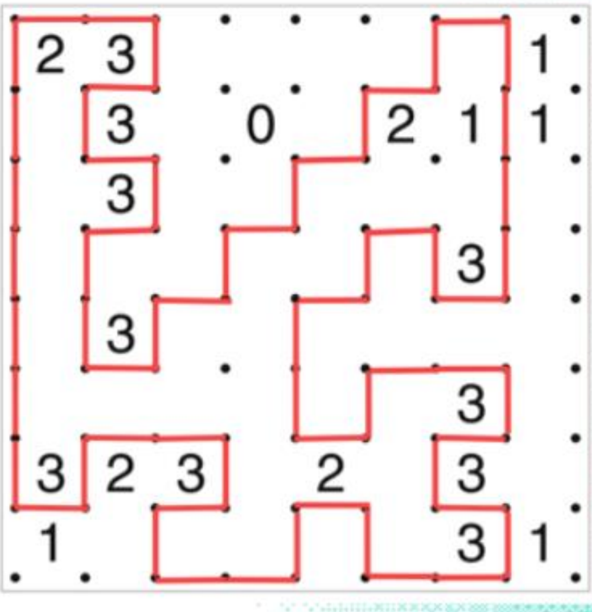


#3 – Word Ladders

C R O S S
C R A S S
G R A S S
G R A D S
G O A D S
R O A D S

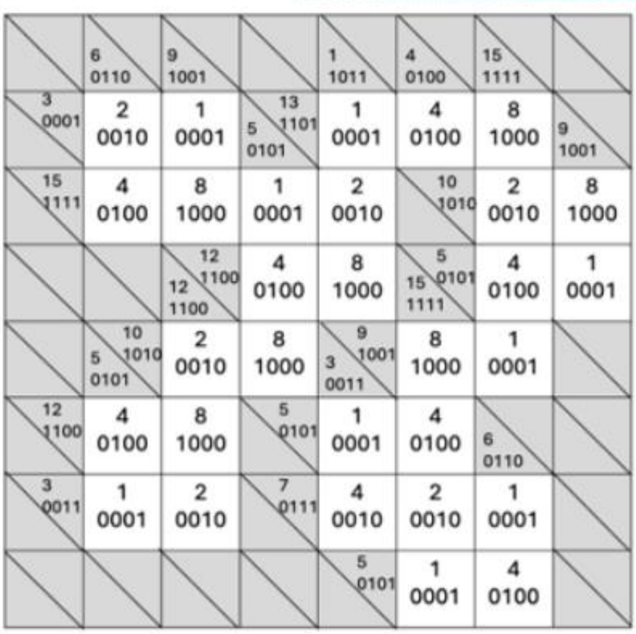
R I S E
R I L E
F I L E
F I L L
F A L L

#4 – Slitherlink



#5 – Kakuro

#6 – Bakuro



#7 – Aquarium