UIT2205: Quantum Computation
AY 2017/18 Sem 2

Ang Yan Sheng
A0144836Y

Essay 1
On the Future of Classical Computation

From its theoretical conception in the 1930s, computational technology has grown into an indispensable part of modern life. However, other than its number-crunching abilities, it is natural to ask if there are more fundamental ways in which computation will affect humanity. In this essay, I will argue that information technology has been, and will continue to be, a source of knowledge essentially different from the human mind.

In daily usage, information refers to any kind of meaningful data. This can come in various forms such as text, audio, or visual (images and video). Since all of these data types, and many others, can be encoded and stored on a computer in binary, we will define the term 'information' for the purposes of this essay as any data that can be expressed as strings of 0/1 bits.

As such, information technology can be seen as the mechanisation of manipulating or processing strings of bits. This processing can be performed by logic gates, the basic building blocks which take only a few input bits at a time; logic circuits, which are comprised of several gates for more complex computations; finite state machines, which allow some bits to enter a feedback loop; and most generally, Turing machines, which have unlimited memory space, and are practically implemented as computers today. By the widely-accepted Church-Turing thesis, all known forms of computation with bits can be expressed in terms of a Turing machine. Thus we will take information technology to mean computers, and their associated technologies.

The concept of knowledge, however, is less clearly defined. For our purposes, we will arrive at a working definition by abstracting the common points of the following two examples:

- I know the Pythagorean theorem;
- I know that I like durian.

The common defining traits of these two pieces of knowledge are as follows. If I know some proposition P, then:

- P must be true, or empirically verifiable; I cannot know that the Pythagorean theorem is false.
- I must believe that P is true/verifiable; for instance, if P = "Louie would like durian once he tries it," but Louie has never tried durian and does not believe P, then Louie cannot know P even if it is true. This also highlights the subjective nature of knowledge: there must be a self-aware subject who holds such beliefs. Since there is no evidence that there are any such subjects other than humans, we will require in particular that such knowledge can be understood by humans.
- I must have reason to believe that P is true/verifiable. More specifically, we will restrict our discussion to the case where a human can arrive at P using either deductive reasoning ("I can prove the Pythagorean theorem"), or inductive reasoning ("I have enjoyed eating durian on previous occasions").

Hence we will restrict our attention to the subclass of knowledge which consists of true/verifiable beliefs that can be humanly justified by deduction or induction.

In the remainder of this essay, we will show the following two claims: computers can derive true/verifiable statements, with deductive or inductive justification for humans, so that they are a source of knowledge; and they do so in an essentially different way from humans, so that this source of knowledge is genuinely new.

We first note that not all computer-generated truths, even in the fully deductive and logical field of mathematics, counts as knowledge under our definition. Historically, computers have been used to mechanically check the truth of mathematical propositions, particularly if there are many cases which are infeasible for a human to check by hand. This method has recently been applied in Heule, Kullmann and Marek (2016), who produced a 200-terabyte formal verification of the Boolean Pythagorean triples problem, by far the largest computer-assisted proof to date. For comparison, Born and Short (2012) estimated the daily information consumption of the average American at 34 gigabytes, so even if all the media consumed by a human were replaced by this proof, it would take around

$$200\,\text{TB} \times \frac{1000\,\text{GB}}{1\,\text{TB}} \times \frac{1\text{ day}}{34\,\text{GB}} \times \frac{1\text{ year}}{365\text{ days}} = 16.1\text{ years}$$

to display in its entirety, not to mention checking its validity. Thus, even if the proof is logically sound, it is not a humanly verifiable justification for the mathematical statement that it proves, and hence its status as human knowledge is dubious.

However, recent advances in both mathematics and computing have given rise to automatic generation of human-checkable proofs for new mathematical statements. For instance, Wilf and Zeilberger (1992) studied identities of hypergeometric and q-series, such as

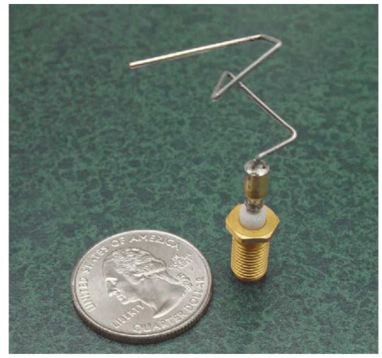
$$\sum_{i+j+k=n} \binom{i+j}{i}\binom{j+k}{j}\binom{k+i}{k} \stackrel{?}{=} \sum_{l=0}^{n} \binom{2l}{l},$$

and introduce the concept of 'proof certificates,' short proofs of these identities which are designed to be more human-checkable. For instance, the certificate for the above sum is an algebraic expression involving the sum of seven rational functions, each a quotient of degree 5 polynomials in three variables; the proof of the general identity above is reduced to showing that this specific expression is equal to 0. By working in conjunction with computer algebra systems, such a certificate can be found by a brute-force search; Wilf and Zeilberger presented such an algorithm in their paper, and write (emphasis in original):

> When we presented [an identity found by the algorithm] to George Andrews [an expert in q-identities], he was able, of course, to prove it independently, but the proof was very long and used several esoteric results. At any rate, our unified method *discovered*, and simultaneously proved, a new identity.

Wilf and Zeilberger's program is able to discover new mathematical truths, and their associated proof certificates; furthermore, such a certificate can be verified by anyone using only elementary algebraic manipulation in a routine, if tedious, manner. Thus, after checking the proof certificate by hand, one can deduce the truth of the original statement, and is justified in believing it. Hence, by our operational definition of knowledge, this program does produce new knowledge.

Modern computation has also made similar contributions in industrial applications. Many engineering problems can be expressed as an optimisation problem over a large number of parameters, and then solved with various heuristics. Hornby, Globus, Linden and Lohn (2006) described the successful case study of antenna design for NASA's ST5 mission. Due to the complexity of the electromagnetic interaction between the antenna and the surrounding structures of the spacecraft, it is difficult to design an antenna by hand to fit the mission requirements, such as mass, dimensions, power consumption, and gain patterns.



To find a design that meets the complex constraints, Hornby et al. used a heuristic known as the genetic algorithm. Initially, a number of candidate designs are placed in a 'gene pool.' At each generation, the algorithm simulates each design in operation, and discards the worst-performing designs to obtain the next generation. In theory, this procedure selects and combines the best features from each design, analogous to Darwinian evolution. In practice, this resulted in an unconventional shape for the antenna (see figure), but the evolved antenna offers lower power requirements, more uniform coverage, and much higher efficiency (93% vs. 38%), as compared to a conventional design.

Here, computers have arrived at a new antenna design, previously unknown to humans. We are justified in believing beforehand that the evolved design will perform well, either by deduction from the theory of genetic algorithms, or by induction from the success of the genetic algorithm in solving other problems. Furthermore, the performance of the evolved design has been confirmed both theoretically (in simulation results) and experimentally (from the success of the ST5 mission). Hence this new design represents another form of knowledge that we can derive from computers. Similarly, computer-aided solutions of other large-scale optimisation problems in engineering and design can also be considered as knowledge.

Now that we have seen two examples of knowledge derived from computers, we note further that such knowledge is inaccessible by the unaided human mind, for two reasons. First, there is a vast difference in processing speed between humans and computers. Moscoso del Prado Martín (2009) analysed human reaction times in English visual lexical decision and word naming tasks, and suggested that the information processing speed of the cognitive system is 4 bits/s for such stimuli on average, but can be dynamically adjusted to a maximum of about 60 bits/s. On the other hand, we can estimate the average processing speed of consumer CPUs by looking at published statistics from distributed computing projects. For instance, as of 12 Feb 2018, the SETI@Home project reports 2607.20 TFLOPS (trillion floating-point operations per second) total across the 146423 participating computers, for an average of 17.8 GFLOPS per computer. Assuming a minimum of 32 bits per floating point number, and at least one number per operation, this gives a maximum processing speed of 5.7×10^{11} bits/s.

Even though these two numbers are not directly comparable, the difference of ten orders of magnitude suggests that some analytic, number-crunching computer algorithms are impossible for humans, even in principle. The exhaustive search and optimisation heuristics in the previous examples belong precisely to this category: they take advantage of the processing speed of computers to explore a massive amount of possibilities, and find solutions that elude even human experts. Therefore, even though humans can easily perform each individual logical or arithmetic task in a computer, there are problem solving strategies that can be implemented on computers but are inaccessible to humans.

Furthermore, the underlying architecture of the human mind and a CPU are fundamentally different. In most modern CPUs, the control unit fetches, decodes and executes program instructions, using the arithmetic logic unit for information processing. Hence the operation of the computer is completely logical, barring hardware or software failure. However, cognitive psychology has found that humans consistently make logical errors in specific scenarios, as summarised by Morewedge and Kahneman (2010):

- In attribute substitution, evaluation of a target attribute is automatically substituted by evaluation of an associated, but different, attribute which is more accessible. For example, the answer to "How many dates did you have last month?" in a survey was found to be highly correlated to the response to the more difficult question "How happy have you been lately?" if asked in this order, but uncorrelated if asked in reverse order.
- In anchoring, an initial piece of information is used as an anchor which subsequent judgements are based around, regardless of whether this information is relevant. In one study, participants gave significantly lower estimates of Gandhi's age at death when first asked if he died before age 9, compared to before age 140, even though both anchors are clearly impossible.
- In the overconfidence effect, subjective confidence in a hypothesis is exaggerated due to coherence or redundancy in the evidence. For example, given a sample of coloured balls and asked to decide if the population contains more red balls than white balls, the consistent sample {3 red, 0 white} is associated with higher subjective confidence than the sample {13 red, 9 white}, which is incorrect by Bayesian inference.

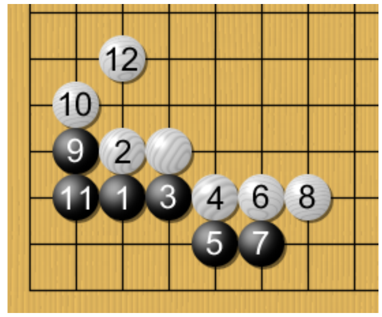
To account for the above logical errors, Morewedge and Kahneman described a dual-process model of the human mind, where an unconscious, automatic System 1 draws from associative memory to form impressions and initial judgments, which a slow, rational System 2 might accept, reject or modify, acting as a controller. This model explains why humans are consistently susceptible to cognitive biases, but also how humans can effortlessly generate skilled judgments, even in scenarios with incomplete information: in contrast to computers, the basis for human decision-making is not logical, but intuitive.

Thus the natural next step in computer knowledge generation is an analogue of human intuition, to be used alongside logical computation. The rise of deep reinforcement learning, and the remarkable success of AlphaGo (Silver et al. 2017), is one of the many recent efforts in this direction. Due to the huge state space, conventional search methods cannot cope with the exponential growth of possible moves in game of Go. However, by using human expert game databases, deep neural networks, self-play reinforcement learning, and application-specific hardware known as tensor processing units, the Google DeepMind team created an AI for Go, which successively defeated the European champion Fan Hui, 18-time world champion Lee Sedol, multiple world champions in online blitz games (as AlphaGo Master), and world top-ranked player Ke Jie (as AlphaGo Master). Silver et al. announced a new version, AlphaGo Zero, which did not learn from any human games but surpassed all previous versions of AlphaGo.

Version	Elo rating
AlphaGo Fan	3144
AlphaGo Lee	3739
AlphaGo Master	4858
AlphaGo Zero	5185

Go players are customarily ranked by the Elo rating, a mathematical system where a player is expected to win 75% of all games with another player with 200 points lower rating. The table shows the Elo ratings of all versions of AlphaGo; for comparison, the top-ranked human go player (as of 12 Feb 2018), Park Junghwan, has an Elo rating of 3668. Silver et al. reported that AlphaGo Zero performed 100-0 against AlphaGo Lee, and 89-11 against

AlphaGo Master.



Even though AlphaGo is unable to provide high-level human justification of its gameplay, experts have been able to obtain new insights into Go from its matches against humans and self-play games. One major example, as reported by Lin (2017), is the scenario shown in the figure, known as a 3-3 invasion. This sequence of moves has been well-studied, and was believed to be the optimal play for both sides. The ending position is thought to be advantageous for white, so move 1 by black would be considered a mistake. However, AlphaGo was observed to play move 1 in the Master games, deviating from the sequence shown from move 9 onwards. This strategy has been interpreted by experts as suggesting that moves 10 and 12 strengthen White's position unnecessarily, so Black's move 9 was suboptimal. Hence this is a previously unknown blind spot in human Go theory, and professional Go players have since successfully incorporated this 3-3 invasion into their tournament games.

The example above is only one of many scenarios in which AlphaGo was able to produce surprising moves, which were later confirmed to lead to viable new lines of play. Thus the Go community was able to derive empirically verifiable and justifiable statements from AlphaGo's games. This means that AlphaGo is a new source of knowledge; more importantly, thanks to the new ideas which lie behind its operation, AlphaGo is able to perform a task which is beyond both humans and the search/optimisation algorithms in the previous examples.

Given the rapid pace of technological evolution, and continued progress in theoretical computer science, it is reasonable to anticipate that computers will continue to give rise to yet other modes of knowledge in the future, in the same way that they have given us search and optimisation algorithms and AlphaGo. However, neither humans nor computers can achieve this alone; like an elegant mathematical proof, or a beautiful game of Go, we can only solve new problems, or find new ways to see the world, by making use of every tool we have—the immense computational power of information technology, and the unique power of human intuition.

References

Born, R., & Short, J. (2012). *Measuring Consumer Information*. Int. J. Commun. 2012(6): 980–1000.

Heule, M.J.H., Kullmann, O., & Marek, V.W. (2016). "Solving and Verifying the Boolean Pythagorean Triples Problem via Cube-and-Conquer." In: N. Creignon, D. Le Berre (eds), Theory and Applications of Satisfiability Testing – SAT 2016, 228–245. SAT 2016. Lecture Notes in Computer Science, vol 9710. Springer, Cham. DOI:10.1007/978-3-319-40970-2_15.

Hornby, G.S., Globus, A., Linden, D.S., & Lohn, J.D. (2006). *Automated Antenna Design with Evolutionary Algorithms*. Space 2006, AIAA Space Forum. DOI:10.2514/6.2006-7242.

Lin, V. (2017, May 20). A new perspective on the star point and the implications thereof. Retrieved from `https://www.eurogofed.org/index.html?id=127`

Morewedge, C.K., & Kahneman, D. (2010). *Associative processes in intuitive judgment*. Trends Cogn. Sci. **14**(10): 435–440. DOI:10.1016/j.tics.2010.07.004.

Moscoso del Prado Martín, F. (2009). *The thermodynamics of human reaction times*. arXiv:0908.3170 [q-bio.NC].

SETI@Home. (2018, Feb 12). *CPU performance*. Retrieved from `https://setiathome.berkeley.edu/cpu_list.php`

Silver, D., Schrittwieser, J., Simonyan, K., Antonoglou, I., Huang, A., Guez, A., . . . , Hassabis, D. (2017). *Mastering the game of Go without human knowledge*. Nature **550**: 354–359. DOI:10.1038/nature24270.

Wilf, H.S., & Zeilberger, D. (1992). *An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities*. Invent. Math. **108**: 575–633. DOI:10.1007/BF02100618.