Paradox

Issue 1, 2006

THE MAGAZINE OF THE MELBOURNE UNIVERSITY MATHEMATICS AND STATISTICS SOCIETY

MUMS

PRESIDENT:	Andrew Kwok a.kwok2@ugrad.unimelb.edu.au
VICE-PRESIDENT:	Maurice Chiodo m.chiodo@ugrad.unimelb.edu.au
TREASURER:	James Zhao j.zhao1@ugrad.unimelb.edu.au
SECRETARY:	Joanna Cheng j.cheng1@ugrad.unimelb.edu.au
EDUCATION OFFICER:	Daniel Yeow largestprime@gmail.com
PUBLICITY OFFICER:	Michael de Graaf m.degraaf@ugrad.unimelb.edu.au
EDITOR OF *Paradox*:	Nick Sheridan n.sheridan@ugrad.unimelb.edu.au
1ST YEAR:	Han Liang Gan h.gan5@ugrad.unimelb.edu.au
2ND YEAR:	Zhihong Chen z.chen5@ugrad.unimelb.edu.au
3RD YEAR:	Tharatorn Supasiti sapiensis@gmail.com
HONOURS:	Jonathan Budd j.budd@ugrad.unimelb.edu.au
POSTGRADUATE:	Geordie Zhang geordie@ms.unimelb.edu.au
WEB PAGE:	http://www.ms.unimelb.edu.au/~mums
MUMS EMAIL:	mums@ms.unimelb.edu.au
PHONE:	(03) 8344 3385

Paradox

EDITORS:	Nick Sheridan and James Wan
LAYOUT:	Stephen Farrar
WEB PAGE:	http://www.ms.unimelb.edu.au/~paradox
E-MAIL:	paradox@ms.unimelb.edu.au
PRINTED:	March, 2006

Words from the Editor

Welcome all to the first edition of Paradox for 2006! We are the magazine of the Melbourne University Mathematics and Statistics Society (known as MUMS for historical reasons). This edition is full, as always, of interesting articles about all things mathematical, and even some things computer scientific. You can find out how some people spent those priceless summer months working on the clustering problem, and how the Google metric allows us to quantify exactly how stupid George W. Bush is. If you're interested in attacking the code used by nations and banks around the world to keep their communication secure, then you need look no further than our article on cryptography, and if you are interested in irrational numbers and the lives they have claimed, then we've got you covered. Chaos, you will learn, is not only a state of mind but a well-defined mathematical concept, and there are a few amusing anecdotes from the excellent book *Mathematical Apocrypha*, by Steven G. Krantz, thrown in for good measure.

Paradox articles are written mainly by students (this edition includes articles by three first-time contributors). So if you would like to have a go at writing an article (it doesn't have to be technical or anything) then go for it! You can ask questions and send articles via email: `paradox@ms.unimelb.edu.au`.

— Nick Sheridan

The Front Cover

The bizarre object on our front cover is a Roman dodecahedron. That is quite strange – the Greeks were the ones who were obsessed with numbers and Platonic solids and so on, the Romans weren't really renowned for their interest in such frivolities. Yet these hollow bronze dodecahedra (about 10cm across), dating from around 200AD, have been found all over Europe, from Great Britain to Hungary. Their purpose is undetermined, and conjectures range from candlesticks to surveying instruments to toys. There was one case of a bronze Roman icosahedron. It was misclassified as a 'dodecahedron' in a museum's basement storage for decades before someone noticed that it was not, in fact, a dodecahedron, but an entirely new phenomenon.

Words from the President

Welcome to what should be another action-packed year from the Maths and Stats Society. MUMS is a society that represents all mathematics and statistics students, offering competitions, seminars and our magazine Paradox. Our events are open to all Melbourne University students as well as the general public. In particular all students studying a mathematics or statistics subject are automatically members of MUMS.

Weekly seminars are held most weeks, covering areas of mathematics that are often not found in high school or university. I strongly encourage you to attend these as they offer students a chance to discover interesting aspects of mathematics in an informal and friendly environment. Certainly the highlight of the year should prove to be the Puzzle Hunt, which keeps competitors intrigued and challenged for over a week. The competition has grown in popularity over the past few years, with over 600 people competing last year from across the world. I would like to stress that, despite the common perception, the Puzzle Hunt is not mathematically oriented and contains puzzles that require general logic and problem solving skills.

Another popular competition is the University Maths Olympics, which is held in second semester. As the name suggests, this competition combines problem solving and physical prowess, where teams compete in an exciting and fast-moving atmosphere. We also run a trivia night each semester.

Our website (`www.ms.unimelb.edu.au/~mums`) is designed to provide informative and relevant content for students, as well as up-to-date information on our latest events and seminars. In particular, there is a guide to free software which students may find useful in their studies and personal pursuits. You can keep in touch with all that's happening in MUMS by joining our mailing list, which can also be found on the website.

We're always looking for people who'd like to contribute to MUMS, so if you would like to become more involved, please consider coming along to our AGM to run for a position. Our AGM will most likely be held in late April or early May.

We would love to hear any comments or suggestions you may have, whether it be via email or in person. In fact, if you're walking through the building, feel free to pop in for a chat and see what's going on in the MUMS room.

The MUMS committee looks forward to meeting many of you this year.

— Andrew Kwok

Why don't you go for a swim instead of reading maths articles?

Imagine yourself sailing in the halcyon Aegean Sea, while cogitating over the diagram depicting a square. Something dawns on you and, excited, you notify your colleagues. Suddenly, cultivated examination of your scroll turns into a brawl, and you are sentenced unanimously to death by being thrown overboard.

The subject of the dispute, however, is not over important matters like wealth, politics or who ate the papyrus used for making scrolls. There was a time when studying maths could be dangerous, especially for Hippasus, who more or less suffered the above fate. For the Pythagoreans, his discovery split asunder the rational world: he had shown that the diagonal of a square compared to its side length is not a ratio of integers.

To see a proof of this now trivial fact, see the previous editions of Paradox. For those who knew the story from kindergarten, have a look at this alternative:

If $\sqrt{2}$ is rational, pick the smallest natural number n such that $n\sqrt{2}$ is an integer. It follows that $n(\sqrt{2}-1)$ is an integer and so is $n(\sqrt{2}-1)\sqrt{2}$ (expand the bracket). But $n(\sqrt{2}-1) < n$ as $2 > \sqrt{2} > 1$, which contradicts the minimality of n. Hence no such n exists and $\sqrt{2}$ is irrational.

This proof uses no divisibility arguments and can be constructed from the definition of rationality alone; it can be easily extended to prove that any non-square integer has an irrational square root; and by induction, any non-nth power has an irrational nth root.

Here is another proof that does not involve number theory: if $\sqrt{2} = m/n$ in lowest terms then it also equals to $(2n-m)/(m-n)$ (check by cross multiplying), so it is reduced to yet lower terms, which means it cannot be rational.

How did we come up with these fractions in the first place? Well, A4 papers are made in the ratio of $\sqrt{2} : 1$, so when you fold it in half the same ratio applies. Now if you let $\sqrt{2} : 1 = m : n$, and draw the largest square using 3 sides of the paper, you can see that the leftover rectangle has ratio $(\sqrt{2}+1) : 1 = n : (m-n)$, which gives $\sqrt{2} = \frac{2n-m}{m-n}$, as required.

Just as you may think it cannot get any simpler than this, we'll prove the irrationality of the golden ratio:

Definition: when a segment is divided in two such that the ratio of the whole to the longer part equals the ratio of the longer part to the shorter part, then that ratio is the golden ratio ϕ.

Now assume ϕ is n/m in lowest terms. Take n to be the length of the whole and m the length of the longer part. Then we have $n/m = m/(n-m)$. Oops, now we found a fraction in lower terms. Contradiction.

The Pythagoreans worshipped the golden ratio. Pythagoras supposedly discovered it and noted its various occurences in the pentagon (for instance, $\cos(36°) = \phi/2$ is used in the straightedge and compass construction of the shape); for this reason the pentagon also became a subject of fervent study. Fascinatingly, the fractional form of ϕ was apparently never sought after. In fact, ϕ is the most irrational number in the sense that its continued fraction is the slowest (of all numbers) to converge.

The existence of irrational numbers greatly vexed Pythagoras, who could not logically prove it wrong: probably that was why the numbers got their name. So he denied their existence. As a note, this is by no means the strangest thing he had done. Legends have it that, once, threatened by a poisonous snake, he bit the snake to death. He was also said to be the son of Apollo, have appeared in two places at once, and walked on water.

Not well known was that mathematicians were not totally comfortable with the notion of irrational numbers until the 19th century, when Dedekind and Cantor finally settled the problem. More than 2 millenia had passed and many theorems were proven about those numbers before they were formally defined. Even the word "surd" comes from Latin "surdus", or deaf. Interestingly, imaginary numbers were first shown to exist (in solution to cubics) and had the consistent theory worked out in less than 100 years.

One of the most famous numbers in maths, e, was shown to be irrational by Euler; only in 1873 Charles Hermite showed e is transcendental (i.e. not the root of a polynomial). Its irrationality is now often left as a first year exercise:

Taylor's series yields

$$e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots$$

If $e = n/m$, then $em!$ is an integer. In the expansion, $em!$ = integer plus the leftover,

$$\frac{1}{m+1}+\frac{1}{(m+1)(m+2)}+\ldots<\frac{1}{m+1}+\frac{1}{(m+1)^2}+\ldots=\frac{1}{m}$$

(infinite sum of a geometric series), which clearly cannot be an integer ($m=1$ is trivially impossible). Hence $em!$ has a fractional part, contradiction.

Logarithms are also easily shown to be irrational. For instance, if $\log_2 3 = m/n$, then $2^m = 3^n$, which clearly is false.

It is by no means easy to determine the irrationality of a number in general; that for π was only solved in 1761 by Johann Heinrich Lambert, with the inspiring comments, *"The diameter of a circle does not stand to the circumference as an integer to an integer"*. He was so thrilled by this and his other feats like the hyperbolic functions that, when Frederick II asked him in which science he was most proficient, Lambert modestly replied "all". Amazingly, the modern version of the proof, though it heavily involves calculus, uses only one fundamental property of π: $\sin(\pi)=0$.

In fact, almost all real numbers are irrational (in the sense that rationals are countable and reals are not), and almost all the irrational numbers are transcendental. For instance, $\cos x$ and $\tan x$ in radians are irrational for all nonzero and rational x. In general, to prove a number is irrational is extremely hard, and transcendental even harder. Gelfond's theorem is an exception: if a is algebraic (i.e. not transcendental) and not 0 or 1, and b is irrational and algebraic, then a^b is transcendental. A famous consequence is that $e^\pi = (-1)^{-i}$ is irrational. $\pi + e^\pi$ was proven irrational as recently as 1996.

It is not known whether $\pi + e$ and $\pi - e$ are irrational. Neither do we know about 2^e, $\pi^{\sqrt{2}}$, or the Euler-Mascheroni constant for those who care.

A slight modification to Gelfond's theorem is not true: if a and b are irrational, then a^b can be rational! For example, take $a=b=\sqrt{2}$. If a^a is rational then we are done. If it is irrational, then $(a^a)^a = a^2 = 2$, and we are also done.

Now here is one for you to try. π^e. if you happen to have a correct proof for its rationality or otherwise, drop it into the MUMS room in utmost secrecy, and we'll let you collect a large black suitcase somewhere in the Stochastic Modeling section of Richard Berry building (because no one ever goes there). Do not mention the proof to anyone else or you'll face death by drowning. Good luck.

— James Wan

Clustering

Clustering is a fundamental problem in computer science[1]. The idea is simple: place related items in the same *cluster*, and dissimilar items in different clusters. Figure 1 gives an illustrative example. There are literally hundreds of formulations of this problem—you can cluster most anything: basic items, like vectors in $\mathbb{R}^n$, or an arbitrarily complex object such as a lecturer.

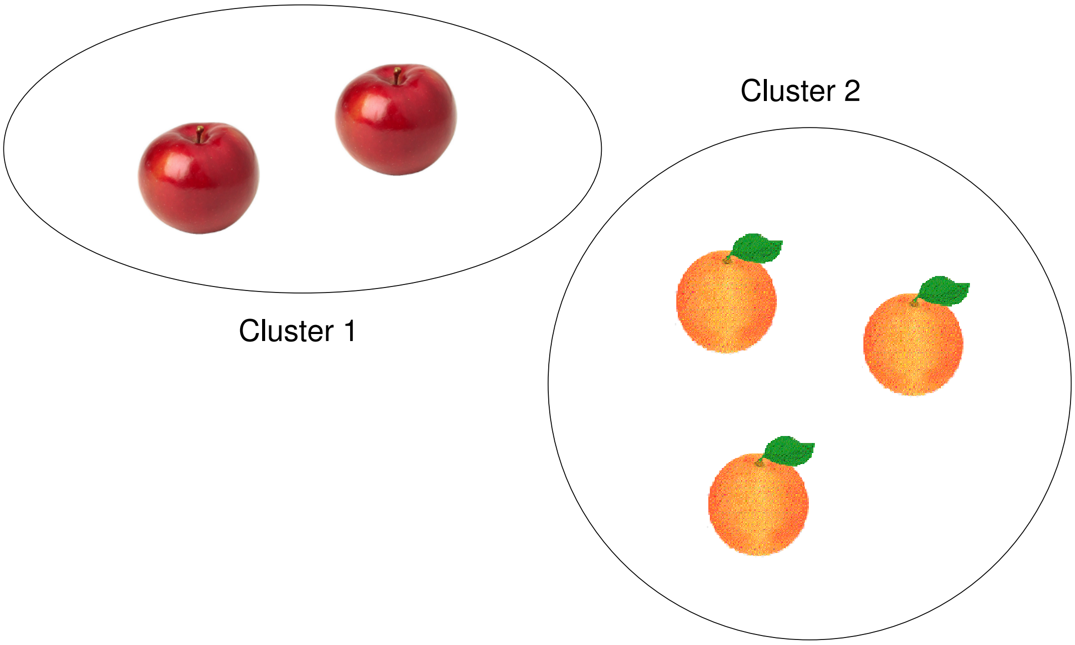


Figure 1: An example of clustering elements in $\mathbb{F}$: the set of fruit

Over the summer, I worked with Dr Anthony Wirth from the Department of Computer Science. Tony is a lecturer and a researcher in the department[2]. Although he works in Computer Science, he's had a life-long love for mathematics—he was the president of MUMS in 1999.

Tony and I have had a productive summer reading research papers, gathering experimental results, and even writing our own paper for a conference! My work was supported in part by a summer studentship from the Department of CS. I strongly encourage second-year students to attempt to get summer work at the university—I've had so much fun that I'm actually continuing work into the semester.

[1] So what's it doing in Paradox? It's a fundamental and *interesting* problem, that's what.
[2] He lectured 433-152 and 433-254 in 2005, and is doing so again this year.

Clustering is, in general, a *difficult* problem, on several levels. Most formulations of the problem (including the *k-centre* clustering defined below) are NP-hard—what this means is that unless something very improbable is true, a clustering that optimises a given criterion function cannot be found in polynomial time. Other results have further reinforced the difficulty of clustering; most notably, a 2002 paper presented an *impossibility theorem* for clustering [J. Kleinberg, Advances in Neural Information Processing Systems (NIPS) 15, 2002]. Three more-or-less reasonable properties that one might like a clustering system to have were given, and it was shown that no formulation can satisfy all three at the one time. The Rolling Stones got it right: you can't always get what you want.

And yet, not all is lost. Although we generally cannot cluster optimally in polynomial time, we can create procedures which in practice get very close to the optimal solution. These algorithms are called approximation algorithms, or heuristics[3]. I'll define a simple approximation algorithm shortly.

A simple formulation of clustering could run as follows: given n points in $\mathbb{R}^n$, pick *k centres* such that you minimise the maximum distance from a centre to any of the given points. The cost of a given solution is precisely this distance. If concrete examples are your bag (baby), then consider placing pizza outlets to satisfy the claim, "Delivered in 30 minutes, or your pizza free." Ideally, you would build outlets (centres) such that you keep the time taken to get to the most distant customer (point) as small a possible. Pizzas are delivered from the nearest outlet, and in a similar way, points will be assigned to their nearest centre to form *clusters*—one per centre. This form of clustering is called k-centre.

In Algorithm 1, the *furthest-first* algorithm (FFA) is presented. The intuition behind this algorithm is to spread out the centres as much as possible. To this end, we start with an arbitrary choice of initial centre, and then repeatedly pick the point most distant from the current set of centres. We define the distance between an item and a set as the distance between the item and the nearest member of the set. We can make some performance guarantees for this algorithm, as shown in Theorem 1.

Theorem 1. *Suppose* $\mathsf{C}_{\mathsf{FFA}}$ *is the cost of the FFA-produced solution. Then*

$$\mathsf{C}_{\mathsf{FFA}} \leq 2 \cdot \mathsf{C}_{\mathsf{OPT}}$$

[3] There is in fact a subtle distinction between the two: approximation algorithms are heuristics with theoretical performance guarantees

Algorithm 1 FFA: Furthest-first approximation algorithm for k-centre clustering.

```
Require: Set of points $V$ in $\mathbb{R}^n$, integer parameter $k$
  Pick a point $\mathbf{p}$ from $V$ and initialise $C = \{\mathbf{p}\}$
  while $|C| < k$ do
    Find $\mathbf{y}$, the point in $V$ furthest from its nearest centre in $C$
    Set $C = C \cup \{\mathbf{y}\}$
  end while
  return the set of centres $C$
```

where $\mathsf{C}_{\mathsf{OPT}}$ *is the cost of the optimal solution.*

Proof. First, note that if Algorithm 1 were to run for $k + 1$ iterations, the distance of the point $\mathbf{y}$ picked on the final iteration would be precisely $\mathsf{C}_{\mathsf{FFA}}$. Also note that the distance of the $\mathbf{y}$ picked at each iteration is less than or equal to that of the $\mathbf{y}$ chosen at the previous step, because otherwise we would have picked the current $\mathbf{y}$ earlier. As a result, the points in C, as well as the $\mathbf{y}$ we would have picked at the next iteration are all separated by *at least* $\mathsf{C}_{\mathsf{FFA}}$.

When we assign points to the centres in the optimal k-centre solution (which we don't actually know), the pigeon-hole principle guarantees that (at least) two of these $k + 1$ points will be assigned to the same centre. A lower bound on the diameter of this cluster is $\mathsf{C}_{\mathsf{FFA}}$, and so the minimum cost of the optimal solution is $\mathsf{C}_{\mathsf{FFA}}/2$. □

Although there's certainly theoretical work being done in clustering, the majority of the literature is concerned with practical methods, and experimental results hold more clout than the nicest theoretical properties[4]. For example, Tony and I are working on document clustering: given a set of documents (say, newspaper articles, or MUMS magazines), cluster them into somewhat useful topics. Document clustering is more complex than the simple $\mathbb{R}^n$ problem posed above. You can represent documents as a real vector (think of a bag of words), but you lose some information about the document in doing so; just what is lost is very hard to define and predict, making it extremely difficult to provide any kind of theoretical performance guarantees.

Active research areas in clustering include:

[4] Except with Tony—he likes mathematics too much

- Soft clustering: almost all forms of clustering allow an object to be assigned to one cluster, and one cluster only. (Practical) multiple membership is still an issue under consideration in the literature.
- Efficiency/quality tradeoff: most algorithms can provide a good clustering given enough time, but datasets can be of sizes of the order of billions of items with thousands of dimensions. On these datasets, many standard algorithms become completely infeasible.
- Anything you can think of! Clustering is such a broad area, with such diverse applications, that papers are constantly being published which apply standard techniques to new kinds of data. Many of the theoretical results in the field are relatively recent because of the largely empirical nature of the initial clustering research.

If there's one thing to go away knowing about clustering, it's this: all clustering is in the eye of the beholder. If you were asked to cluster a set of natural numbers, you could group them into even or odd—you could also group them into prime and composite classes, or even intuitively "big" numbers and "small" numbers. There is never a single canonical clustering over a set of data: it always depends on what you actually *want* and why you began clustering in the first place.

— Michael Bertolacci

Nobert Wiener (1894–1964, inventor of cybernetics) was quite a celebrity around MIT. Students were in awe of him. Therefore, when one of his students spied Wiener in the post office, the student wanted to introduce himself to the famous professor. After all, how many MIT students could say that they had actually shaken the hand of Norbert Wiener? However, the student wasn't sure how to approach the famous savant. The problem was aggravated by the fact that Wiener was pacing back and forth, deeply lost in thought. Were the student to interrupt Wiener, who knows what profound idea might be lost? Still, the student screwed up his courage and approached the great man. "Good morning, Professor Wiener," he said. The professor looked up, struck his forehead, and cried, "Wiener! That's the word."

The Google Metric[1]

Many a geeky maths student has asked what happens when we integrate an apple with respect to an orange. The answer, of course, is that this is a silly question; apples and oranges are completely different things. But what if we change the question slightly? What if we ask the question, how far apart are an apple and an orange? It might seem ridiculous to think about a "distance" between unrelated objects, but after a little thought, one might more or less say that the distance between an *apple* and an *orange* is greater than the distance between a *Granny Smith* and a *Red Delicious*, but smaller than the distance between *Fiona Apple* and *Apple Martin*. Vague as it may be, there seems to be some concept of distance going on here.

Luckily, two Dutch mathematicians, Rudi Cilibrasi and Paul Vitanyi, have already investigated the matter[2], and come up with a solution using the neverending catalogue of knowledge known as Google. As their theory goes, two phrases that are closer to each other, when put into a search engine, should return relatively more web pages that contain both of those phrases. The concept is really very simple, with the main technical difficulty being to account for discrepancies caused by some phrases having more search results, or *hits*, than others. For example, there are 10 million pages containing both *microsoft* and *dog* but only 2 million containing both *knife* and *fork*, yet the latter pair are obviously closer.

How do we fix this? We have some normalising to do, but it isn't at all clear how to do it. A good idea is to use logarithms of hits rather than the number of hits themselves, since the difference between 10 and 100 hits is more like the "10 times" difference between 1000 and 10000 than the "90 hits" difference between 1000 and 1090. Recalling our high school logarithm laws, multiplying by 10 is the same as adding $\log(10)$ to the logarithm, so this means we only have to add and subtract rather than dividing and multiplying. The rest of the process of finding the optimum normalisation procedure is mostly trial and error; Cilibrasi and Vitanyi came up with the following formula:

$$d = \frac{\log x - \log z}{\log M - \log y}$$

[1] Pedants beware: this isn't really a metric, as it doesn't satisfy the triangle inequality

[2] See http://arxiv.org/PS_cache/cs/pdf/0412/0412098.pdf

Here, x is the number of hits for the first phrase and y is the number of hits for the second phrase, with order chosen such that $x \geq y$; z is the number of hits for both phrases, and M is the total number of pages indexed by Google, which is currently around 10^{10}. A possible interpretation is that this distance is the number of hits for one phrase that don't contain the other, scaled to fit with the rarity of the individual phrases among Google's database.

At this point, some philosophical questions come into it. Can we take it one step further and define a word entirely by the collection of contexts in which it is used? Apparently, we can, but our Dutch friends claim we'll need a much bigger pool of information than even Google to start with.

For now, it's much more fun to just play with the formula, as shown below. Remember, kids: put the phrases in quotation marks, so that Google understands to search for them verbatim rather than their constituent words. As a guide, anything lower than around 0.6 is "close" and anything higher is "distant".

Phrase 1	**Phrase 2**	**Distance**
apple[3]	orange	0.60
granny smith	red delicious	0.23
fiona apple	apple martin	0.67
microsoft	dog	1.02
knife	fork	0.46
george w bush	stupid	0.54
george w bush	intelligent	0.86
theodore j knott	knot man	0.29
maths	olympics	0.69
john howard	kim beazley	0.28
algebra	spaghetti	0.90
rubik	cube	0.11
tweedledum	tweedledee	0.03
fashion sense	lecturer	1.25
maths	career	0.83
google	metric	0.83

— James Zhao

[3] This search excluded references to Apple Computer Inc.

Chaos Theory

Chaos; we've all heard it somewhere. In fact, it has become one of those buzz words, such as 'quasi' or 'quantum', that just gets thrown about to make someone sound pseudo-intelligent [1]. When you get to the bottom of it though, what is mathematical chaos all about?

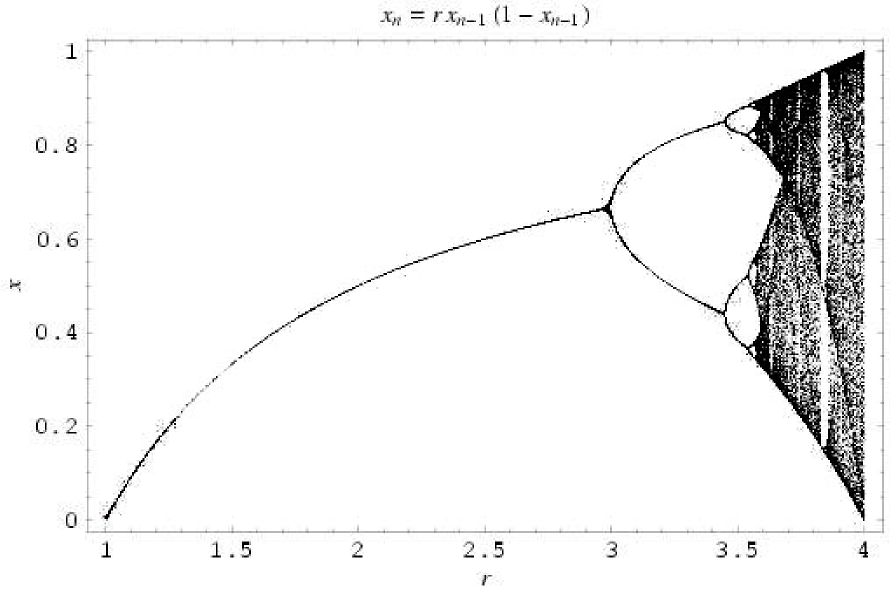
Contrary to the common notion of chaos as being something utterly random, mathematical chaos is actually deterministic. This means that, in mathematics, chaos is not actually random and could be predicted given enough information. However, superficially it does seem to be quite 'chaotic'. The easiest way to get a feeling of what it's all about is probably to take a look at a very simple chaotic system.

The logistic map is specified as follows: $x_{n+1} = rx_n(1 - x_n)$; for the sake of simplicity, we shall only deal with $0 < x_n < 1$ and $r > 1$ in this article. As you can see, this mapping takes a number and shoves it through a series of iterations to produce a sequence. For example, if we start with $r = 1$ and $x_1 = 0.5$, you would produce the following sequence: {0.5, 0.25, 0.188, 0.152, 0.129, 0.112, 0.100, 0.090, 0.081…}. It should be intuitive that this sequence might converge to 0. Indeed, if you try this with all the numbers between 0 and 1, you'll find that the sequence has a limit of 0. This should be no surprise, because, when $r = 1, x_{n+1} = x_n(1 - x_n) = x_n - x_n^2$, so you're subtracting a bit of the number every time you get a new term. Here, 0 is known as a fixed point. Now, fixed points are just points that stay constant after any number of iterations. Furthermore, if all of the adjacent points to our fixed point a converges to a, then a is known as a stable fixed point. On the other hand, we also have unstable ones, where all adjacent points will diverge (it's interesting that for any real numbers outside of our specified range for x_n, successive iterations will cause our sequence to 'blow down' to negative infinity).

So far, it has been fairly obvious and predictable what our sequences will converge to. In the tried and true traditions of the dead cat [2], let's see what happens when we change the r-value. I find that a diagram helps, so here's one someone else prepared earlier.

[1] Pseudo-intelligent is also one of those buzz-words.

[2] The one killed by curiosity, that is. Obviously it had a few lives left, otherwise, how could we follow its tradition?



This is a bifurcation diagram. In this particular case, r has been plotted against x, and the clear single lines in the picture are 'attractors', whilst the shaded portion is where chaotic behaviour is exhibited. Definition time. Attractors are just sets that our 'system' will evolve to over time. In our example of $r = 1$, the attractor is simply $\{0\}$, just as you can see that for $r = 2$, it's $\{1/2\}$ (i.e. if $r = 2$, then after many iterations, our sequence x_n will converge to 1/2). For now, let's just examine the single unbranched line from $r = 1$ to $r = 3$, a little calculation will show that these stable fixed points (a type of attractor) are just $(r-1)/r$. If we let x be the value that our sequence x_n converges to, then: since $\lim_{n\to\infty} x_n = x_{n+1}$, $x = rx(1-x)$, $0 = rx - rx^2 - x$, $0 = x(x - (r-1)/r) \Rightarrow x = 0$ or $x = (r-1)/r$.

Now something quite strange happens at $r = 3$, according to the above calculations. Although what we've worked out shows that there will always be a fixed point at $(r-1)/r$, why on earth do we have two lines branching off? Moreover, what are the formulae for these new attractors?

To be able to half-answer these questions (I'm not going to fully answer them), let's figure out what the two lines mean. Take $r = 3.2$ and $x_1 = 0.9$ and we get the following sequence; $\{0.9, 0.288, 0.656, 0.722, 0.642, 0.735, 0.623 \ldots 0.799, 0.513, 0.799, 0.513 \ldots\}$. In effect, what we've ended up with in this case is called a period-two orbit; an attractor that is a sequence of two repeated numbers (here $\{0.799, 0.513\}$).

To work out what the period-two orbit will be, all we need to do is to think about what happens to x_n and x_{n+2} as n tends to infinity. That is, $\lim_{n\to\infty} x_n = \lim_{n\to\infty} x_{n+2}$. For the ease of typing this up, let's just call this limit x. Then,

$$x_{n+2} = r(x_{n+1})(1 - x_{n+1}) = r[rx_n(1 - x_n)][1 - rx_n(1 - x_n)]$$

Or, as $n \to \infty$,

$$x = r^2x(1 - x)(1 - rx + rx^2)$$
$$0 = r^2x(1 - x)(1 - rx + rx^2) - x$$

Since all x has to satisfy is $x_n = x_{n+2}$, so the fixed points that we worked out earlier are both solutions for x. This means that we can divide everything by x and $x - (r - 1)/r$ to obtain a simpler equation.

$$0 = r^2x^2 - (r^2 + r)x + (r + 1)$$
$$\Rightarrow 0 = rx^2 - (r + 1)x + \frac{r + 1}{r}$$

Using this equation, it is now easy to derive the period-two orbit as well as the determinant of this equation. The attractor lines can be found by the formula, $[(r + 1) \pm \sqrt{(r - 3)(r + 1)}]/2r$. On the other hand, the discriminant $\Delta = (r - 3)(r + 1)$, which is greater than 0 when $r > 3$. This partially explains the phenomenon that we witnessed in the bifurcation diagram since it shows that the period-two orbit is only possible from $r = 3$ onwards. However, it does not explain why these period-two orbit attractors are preferred over the original single-lined, stable point. To do so, we do the following. Let $f(x) = rx(1 - x) \Rightarrow f'(x) = r - 2rx$. Now, let's think about this: in order for a point k to be stable, it would need to have quite a small gradient. Indeed it might make quite a bit of sense for the stable attractor to have $|f'(k)| < 1$, because having your derivative greater than 1 means the magnitude of the next term in the sequence will be further away from the current attractor. Whereas $|f'(k)| = 1$ preserves the distance between x_n and k and it follows that, if the magnitude of the derivative is less than 1, then the sequence is brought closer to k with each iteration. Indeed, with the help of Taylor's polynomials, this hypothesis can be easily confirmed. Since $f'((r - 1)/r) = r - 2(r - 1) = 2 - r \Rightarrow |f'((r - 1)/r)| < 1$ for $1 < r < 3$. Therefore, $(r - 1)/r$ is a stable fixed point for $1 < r < 3$.

Going back to the bifurcation diagram, you may see why the rest of the periodic orbits behave that way. The original period-two orbit branches more and more to create a pattern that will look fairly similar no matter how many times you magnify it. This type of pattern is often known as a fractal. At $r \approx 3.57$, something quite interesting happens, the fractals stop, and instead, we have the onset of chaos. In this strange region, the smallest difference in our initial x value will result in massive differences after only a few iterations; take a look at the following example. Let $r = 4, x = 0.871$, then we have: {0.871, 0.449, 0.990, 0.040, 0.155, 0.525, 0.997, 0.010, 0.040, 0.151…} and for $x = 0.872$: {0.872, 0.446, 0.989, 0.045, 0.173, 0.572, 0.979, 0.082, 0.303, 0.844…}. Although the initial difference was only 0.001, after only 10 iterations we have already had deviations as great as by 0.693! There are two other qualities that a chaotic system must have: it needs to be topologically mixing and dense with periodic orbits. Without being rigorously correct, you might like to know that topologically mixing is having the points 'mixed around' or 'spread out' after iteration. This is important, because you don't want the points to clump together and form a stable fixed point or periodic orbits. Denseness, on the other hand, can be thought of as follows: take any point in the region that our chaotic mapping occupies, and draw a small circle around this point. If, no matter how small you draw the circle, there will always be a point from our system found in it, then whatever we had was dense.

Lastly, just take a look at the white vertical strokes in the bifurcation diagram. They are actually just places where there are newly formed cycles, such as at $r = 1 + 2\sqrt{2}$, where we have a period-3 orbit that branches into a period-6 orbit, to a period-12 orbit and so forth. It's fascinating why this type of thing should happen at all: one minute, we're dealing with a patch of fuzzy grey denoting chaos and the next we're looking at a window of orderly periodic cycles. As pathetically clichéd as it might sound, there is order in amidst all that chaos.

This article only convers a tiny portion of the mesmerising world of chaos theory, and there are many questions and topics that are interesting to consider.

- Why are there fractals when we're dealing with chaotic systems?
- One of the Feigenbaum constants is $\delta = 4.6692016091029906 71\ldots$ and this number ascribes the limit of the ratio between successive bifurcation intervals, and hence can be used to predict when the system becomes chaotic. It doesn't just apply to the logistic map, but actually holds true for all one-dimensional mappings with a single hump. Why is this the case? In addition, the number is suspected to be transcendental, which in itself can be interesting.

— Yi Huang

Adventures in Cryptography – The RSA scheme

It is the year 2020. An evil secret society, calling itself Team X, and run by politicians and mercenary physicists, is plotting its next dastardly act, to secure world domination. At the helm of the heinous organisation is someone unspeakably ruthless and nefarious, known only as Dr X_0. The rest of his hench-men are similarly code-named X_1, $X_2, \ldots$

Already the sinister organisation has infiltrated every country of the earth. In every corner of the globe preparations are being made for a sequence of events that will consummate the cruel dominion of Team X irrevocably.

In the midst of this woe, there is a flicker of hope. Karen, a 20-something mathematician is desperate to stop the clandestine activities of Team X before it is too late, but has very little inside information.

She does however know one critical fact. Team X has decided to implement the RSA cryptographic protocol to secure its evil communications. Created in 1978, RSA is famed for its unbreakability, thus Team X has chosen it.

Karen needs to do some research:

The RSA Protocol in a Nutshell

RSA (named after its creators Ron Rivest, Adi Shamir and Leonard Adleman) is a protocol for encrypting data, based on the supposed computational difficulty of factoring numbers with large prime factors. Here's how it works:[1]

Alice wants to be able to receive encrypted messages from anyone, such that only she can decrypt them. So:

1. She finds two large primes p and q.[2]
2. She finds integers e and d such that $ed \equiv 1 \bmod \phi(pq)$ (once she picks e, she can calculate d by the Euclidean Algorithm).
3. She publishes $\langle e, pq \rangle$ as her *public key* maintaining $\langle d \rangle$ secretly as her *private key*.

[1] If you are unfamiliar with RSA, a detailed explanation can be found in Paradox Issue 1, 2004: http://ms.unimelb.edu.au/ paradox/archive/issues/p04-1.pdf

[2] There are many algorithms to find large random primes e.g. Miller-Rabin test.

Bob wants to send Alice a secret message M. Here is what he does:

1. He looks up Alice's *public key*.
2. His message M is basically just an integer[3]. He calculates $C \equiv M^e \bmod (pq)$ and sends the ciphertext C off to Alice.
3. Alice receives C. Using her *private key* she computes $C^d \equiv (M^e)^d \equiv M^{k\phi(pq)+1} \equiv M \cdot (M^{\phi(pq)})^k \equiv M \cdot 1^k \equiv M \bmod (pq)$, by Euler's Theorem[4].
4. Alice thus obtains the original message M.

NB: e is known as the *public exponent*, d the *private exponent* and pq the *public modulus*.

The Enigma:

Karen knows that deciphering communications will be nearly impossible. RSA's reputation as cryptographically impenetrable is formidable. The situation is not entirely hopeless though.

Unbeknownst to Team X, she has access to the email server that connects Dr X_0 to his minions X_i. Naturally all the emails contained on this server are encrypted with RSA, but encrypted data is better than no data at all.

She first considers a couple of simple approaches.

Bruting the Message Space:

- If Dr X_0 were to encrypt simple messages like 'Show No Mercy' (or split messages into small blocks, each of which is encrypted), it is theoretically possible that Karen could simply encrypt an enormous number of different plaintext messages M until she found a match with the intercepted ciphertext C. In reality this tends to be much worse than searching for a needle in a haystack.

[3] A message can easily be converted to one or more integers, e.g by using ASCII and interpreting the block(s) in base 256.

[4] We require M to be coprime to pq, however the probability it isn't, is so ridiculously small, it is scarcely worth checking beforehand.

Searching d:

- Karen could encrypt some message M with the public exponent e to yield C. She could systematically compute $(C)^d$ mod pq, incrementing d each time, until M was returned. Then she would know d, and be able to decrypt any intercepted messages.

  Again this attack is impractical, since d is invariably way too large to systematically search for.

Since both approaches are almost certainly futile, Karen turns her attention to other alternatives.

Factorising pq:

- She reads in a book "Attacking the public modulus is often considered the best means of cracking RSA, and therefore many algorithms have been devised to facilitate this..."

  If Karen were able to factorise the public modulus pq, it would be a simple task to calculate $\phi(pq)$, and hence knowing e, calculate d, thereby decrypting any cipher text.

  Karen reads of several algorithms for attempting a factorisation of pq, but notes that if pq is very large, even with the most powerful computers, this can be an exceptionally time-consuming task.

Karen is still researching, when she receives an urgent email from a friend...

SOMETHING BIG IS HAPPENING. BY NOON NEXT MONDAY, X_0 WILL HAVE EMAILED A SECRET MEMO TO ALL HIS HENCHMEN. I HAVE A LIST OF ALL THEIR PUBLIC KEYS. WE MUST DO SOMETHING...

==TEAM X PUBLIC KEYS==

$$X_0 : e_1 = 257,\ P_0 = 2937598.........$$
$$X_1 : e_2 = 257,\ P_1 = 9406335.........$$
$$X_2 : e_3 = 257,\ P_2 = 7363941.........$$

.

.

.

Later that day Karen is showering and pondering the email, when suddenly, out of the blue, she has a brilliant flash of inspiration. Entirely forgetting that she is stark naked, she streaks down the street in ecstasy shouting "Eureka!"

The Attack:

Karen's euphoria lies in just two things:

- The same secret memo M is being sent to all X_i.
- All X_i have the same public exponent, $e = 257$.

At noon on Monday, having access to all emails sent from Dr X_0 to X_i, she obtains 257 different encryptions of M.

$$\begin{gathered} M^{e_1} = M^{257} \equiv C_1 \text{ mod } P_1 \\ M^{e_2} = M^{257} \equiv C_2 \text{ mod } P_2 \\ M^{e_3} = M^{257} \equiv C_3 \text{ mod } P_3 \\ . \\ . \\ . \\ M^{e_{257}} = M^{257} \equiv C_{257} \text{ mod } P_{257} \end{gathered}$$

She now applies The Chinese Remainder Theorem to solve, yielding:

$$M^{257} \equiv K \text{ mod } P_1 P_2 P_3 P_4 \ldots P_{257} \text{ where } K \in \mathbb{Z}^+$$

Since the encryption process requires that $M < P_i \; \forall \; i$ Karen can be certain that $M^{257} < P_1 P_2 P_3 P_4 \ldots P_{257}$, and therefore that $M^{257} = K$.

To recover M, she simply calculates $\sqrt[257]{K}$.

Having decrypted the message, Karen wastes no time. She anonymously posts the decrypted memo all over the internet. With Dr X_0's secret memo made public, his plans are thrown hopelessly into disarray. Karen's ingenuity saves the day.

Afterword:

What Karen independently realised, is known more generally as a broadcast attack. Many RSA implementations use low exponents (even $e = 3$) for their speed. Team X used $e = 257$ since $257 = 100000001_2$, thus encryption with respect to pq requires only 8 modular squarings and 1 modular multiplication. In such implementations, it is paramount that the same messages intended for multiple recipients are individually padded randomly, to prevent this type of attack.

— Kim Ramchen

The Preface to *States of Matter*, a recent text on statistical mechanics by David L. Goodstein, reads as follows:
Ludwig Boltzmann, who spent much of his life studying statistical mechanics, died in 1906, by his own hand. Paul Ehrenfest [Boltzmann's student], carrying on the work, died similarly in 1933. Now it is our turn to study statistical mechanics.

It is said that, late in his life, Hilbert was reading a paper and got stuck at one point. He went to his colleague in the office next door and queried, "What is a Hilbert space?"

Paradox would like to thank James Wan, Kim Ramchen, Yi Huang, Michael Bertolacci and James Zhao for contributing articles to this edition.

Great is Caesar: He has conquered Seven Kingdoms.
The Third was the Kingdom of Infinite Number:
Last night it was Rule-of-Thumb, to-night it is To-a-T;
Instead of Quite-a-lot, there is Exactly-so-many;
Instead of Only-a-few, there is Just-these.
Instead of saying, 'You must wait until I have counted,'
We say, 'Here you are. You will find this answer correct;'
Instead of a nodding acquaintance with a few integers,
The Transcendentals are our personal friends.
Great is Caesar: God must be with Him.

— W.H. Auden, *For the Time Being*

Solutions to Problems From Last Edition

Problem 1 Take a cross section of the sphere, so we get a circle with a middle section removed. Let the centre of the circle be the origin. Let the radius be r and height of section above the x-axis be h, then the volume left, using the formula for rotational solids, is

$$\pi \int_{-\frac{5}{2}}^{\frac{5}{2}} y^2 - h^2 \mathrm{d}x = \pi \int_{-\frac{5}{2}}^{\frac{5}{2}} r^2 - x^2 - h^2 \mathrm{d}x = \pi \int_{-\frac{5}{2}}^{\frac{5}{2}} (\frac{5}{2})^2 - x^2 \mathrm{d}x = \frac{125\pi}{6} \mathrm{cm}^3$$

Problem 2 Take out a tablet of type B, so now he has 2 of each type. Cut them in half (or dissolve them and take half of the solution) and take each half on different days.

Problem 3 *No one* was able to solve this one, so now we offer $10 for the best solution. The problem is:

A polynomial of degree $n > 1$ with real coefficients has n distinct real roots. Show that the sum of the gradients of the normals to the graph of the polynomial at these roots is 0.

Paradox Problems

The following are some problems for which prize money is offered. The person who submits the best (clearest and most elegant) solution to each problem will be awarded the amount indicated beside the problem number. Solutions may be emailed to `paradox@ms.unimelb.edu.au` or you can drop a hard copy into the MUMS pigeonhole near the Maths and Stats Office in the Richard Berry Building. Congratulations to Yiling Cao, Vitaly Beliavski, Tsubasa Nagashima and Han Wah Chew who solved Question 2 from the last edition of Paradox. As Han Wah Chew submitted the answer earlier than the rest, you can come by the MUMS room to pick up the prize whenever you like.

1. ($2) What is the probability of obtaining no combinations (i.e. no any form of double, flush or straight) in a poker hand (5 cards)?
2. ($2) Can $x^2 + y$ and $y^2 + x$ both be perfect squares, if x, y are positive integers?
3. ($5) Prove that a divides b if and only if F_a divides F_b, where F_n is the nth Fibonacci number.

The 2006 Melbourne Uni Puzzle Hunt

Monday March 27th – Friday March 31st

Do you **LOATHE**

- Problem Solving
- Lateral Thinking
- Having fun
- Being creative
- (potentially) Unlimited bragging rights?

Then you probably won't want to participate in the 2006 Melbourne University Puzzle Hunt.

For more information:

- Google "puzzle hunt"
- Go to `http://www.ms.unimelb.edu.au/˜mums/puzzlehunt/` or `http://puzzlehunt.tk`
- Email MUMS at `mums@ms.unimelb.edu.au` or subscribe to our mailing list at:
  `http://www.ms.unimelb.edu.au/˜mums/mlist`