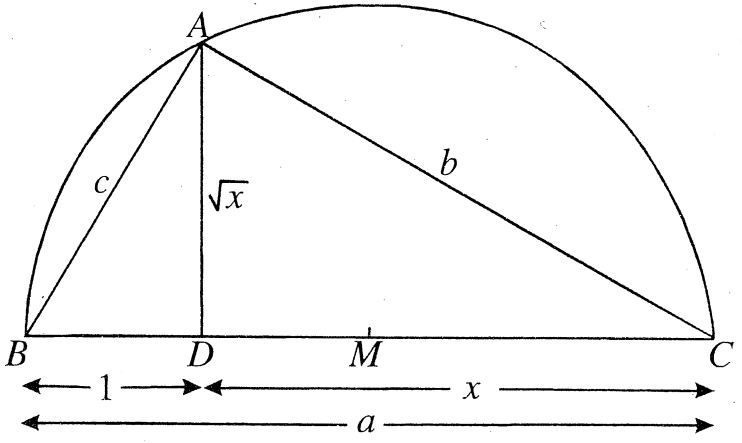
Function

A School Mathematics Journal

Volume 24 Part 1 **February 2000**



Department of Mathematics & Statistics – Monash University

Reg. by Aust. Post Publ. No. PP338685/0015

Function is a refereed mathematics journal produced by the Department of Mathematics & Statistics at Monash University. The journal was founded in 1977 by Prof G B Preston. *Function* is addressed principally to students in the upper years of secondary schools, and more generally to anyone who is interested in mathematics.

Function deals with mathematics in all its aspects: pure mathematics, statistics, mathematics in computing, applications of mathematics to the natural and social sciences, history of mathematics, mathematical games, careers in mathematics, and mathematics in society. The items that appear in each issue of *Function* include articles on a broad range of mathematical topics, news items on recent mathematical advances, book reviews, problems, letters, anecdotes and cartoons.

* * * * *

Articles, correspondence, problems (with or without solutions) and other material for publication are invited. Address them to:

The Editors, *Function*
Department of Mathematics & Statistics
PO BOX 28M
Monash University VIC 3800, AUSTRALIA
Fax: +61 3 9905 4403
e-mail: function@maths.monash.edu.au

Function is published five times a year, appearing in February, April, June, August, and October. Price for five issues (including postage): $25.00* ; single issues $7.00. Payments should be sent to: The Business Manager, Function, Department of Mathematics & Statistics, PO Box 28M, Monash University VIC 3800, AUSTRALIA; cheques and money orders should be made payable to Monash University.

For more information about *Function* see the journal home page at `http://www.maths.monash.edu.au/~cristina/function.html`.

---

* $13 for *bona fide* secondary or tertiary students.

EDITORIAL

Welcome to all readers our first issue of the millennium!

This is certainly a very special year for mathematics; it was declared by UNESCO as the World Mathematical Year. Celebrations are taking place all around the world. Only a few weeks ago we had an exciting maths festival at the University of Melbourne. We include here a report from one of our *Function* readers. If you attended the festival, why don't you send us too an account of your experiences?

What does the number e have to do with the starsigns? Well, it is part of the answer that Michael Deakin gives to the question of what is the probability that an astrologer who enters in a room with twelve people inside, each of the twelve having a different starsign, and when asked to say which starsign goes with each person got all of them wrong.

We reproduce here the article by Brian Davey who introduces logic and logical reasoning to explain what he does as a mathematician and how this comes to be a very enjoyable activity and at the same time has extremely useful applications.

The *History of Mathematics* column is somehow related to the previous article. It shows—through the example of existence theorems—how sometimes activities undertaken by mathematicians which are regarded by many as of little value, provide in fact the foundation to important results.

Increasingly many of us are used these days to pull down menus or other images appearing on top of the current image on our computer screen. Have you ever thought how this is achieved? You will find out if you read the article by Peter Grossman about swapping values of variables.

Thankyou to the readers who sent the solutions to the problems. We include a few more to keep you entertained until our next issue.

* * * * *

STARSIGNS, STATISTICS AND 1/*e*

Michael A B Deakin

Recently, as some of us sat round after lunch, one of our number told a rather curious story. Apparently an astrologer had entered (been invited to enter?) a room with twelve people inside, each of the twelve having a different starsign, and asked to say which starsign went with each person. According to the story, the astrologer got all twelve wrong. We had a bit of fun with this, and a bit of a chuckle at the astrologer's discomfiture, for none of us are the sort to take astrology's claims at all seriously.

However, I got to thinking that, on a purely random basis, it is really quite likely that this would be the result. Think of things from the opposite angle, and for the moment ignore the information that the starsigns were all different. The probability of getting every one of twelve starsigns *right* is one in 12^{12}, and this is a very small number indeed. In fact it works out to be $1.121566548\times10^{-13}$. [Here I am assuming that each starsign is equally likely; this is not *quite* correct, but it is an excellent approximation, and so from now on I will continue to use it without any further comment.]

So if every identification had been *right*, the probability of this happening purely by chance is minuscule, and we would have very strong evidence of the astrologer's powers.

We can go beyond this simple calculation to find the probability of each number of correct responses all the way from 12 down to zero. If n is the number of correct identifications, then the probability of our seeing this is given by the **binomial distribution**. The formula is

$$\text{Prob}\,(k) = \binom{12}{k}\left(\frac{1}{12}\right)^{k}\left(\frac{11}{12}\right)^{12-k}$$

On the next page is a table of the probabilities.

NUMBER CORRECT	PROBABILITY
12	1.12157E-13
11	1.48047E-11
10	8.95683E-10
9	3.28417E-08
8	8.12832E-07
7	1.43058E-05
6	0.000183592
5	0.001731008
4	0.011900679
3	0.058181096
2	0.191997615
1	0.383995231
0	0.351995628

The table makes it clear that the probability of twelve *incorrect* responses is actually quite high. In fact it's the *second most likely* outcome of such an experiment. We can specify precisely this probability either by using the formula given or else by working things out from first principles. Either way we find

$$\text{Prob}(0) = \left(\frac{11}{12}\right)^{12}$$

and this number may be checked from the table above.

But we may write the number on the right of this equation in the form

$$\left(1-\frac{1}{12}\right)^{12}$$

and *this* in its turn is a special case of the number

$$\left(1-\frac{1}{n}\right)^{n}$$

This last is a number that has long been studied in its own right, because as n gets larger, its value tends towards the number $1/e$, where e is the base of the natural logarithms. (See the article in *Function, Vol* 22, *Part* 2, p. 57.) Now $\frac{1}{e} = 0.367879441$, and this is to be compared with the value given at the bottom of the table. Although we have only reached the relatively small value $n = 12$ we are already within 0.016 of the limiting value of $1/e$.

In a general scenario in which there were n houses in the zodiac, the chance of getting all n wrong in an analogue of the experiment reported upon tends to $1/e$ as n gets larger and larger. This is quite a surprising result, because we tend to think that the probability of getting *every* guess wrong should be small. In fact, it is the second most likely outcome (after the event of getting exactly one right), whatever the value of n.

But now let's get back to the original scenario which had twelve people in a room and each of them with a *different* starsign. Let E_1 be the event that all the starsigns were different, and let E_2 be the event that the astrologer got all the starsigns wrong. We are interested in the probability of E_2 given E_1. The understanding is that the astrologer will nominate 12 different starsigns.

First let us work out the probability of event E_1. If we were to take 12 people at random, then there would be 12 possible starsigns and so there are 12^{12} possible combinations, as noted above. But if the starsigns are to be all different then the first may be chosen in 12 ways, but the second in only 11, the third in 10, etc, so that this time there are 12! allowable combinations, where 12! is an abbreviation for the product of the first 12 natural numbers.

Although 12! is a very large number (479 001 600 to be exact), it is nonetheless much smaller than 12^{12}. The ratio of the two numbers, which is the probability of event E_1, is 0.000 0537..., so E_1 is most unlikely to occur by chance. It sounds very much as if the astrologer was being set up.

[Before we move on, it may be as well to pause here to notice a way in which this probability could have been approximated quite easily. There is an approximate formula for $n!$ called Stirling's Formula and it goes like this.

$$\frac{n!}{n^n} \approx \sqrt{2\pi n}\, e^{-n}$$

In our case, $n = 12$ and the right-hand side is 0.000 0533... , which is reasonably accurate.]

Now consider the number of ways in which the 12 different starsigns can be redistributed among these twelve people in such a way that no-one has their correct starsign. This is the problem known as "complete permutation" (or "derangement"). There is a formula for the number of complete permutations of n objects, and this is what we need.

For a good discussion of complete permutations, see the website:

www.telospub.com/journal/MIER/Piele/Vol5No2/piele52.html

which is part of the on-line advertising for the Computer Algebra package *Mathematica.* The account given there is drawn from that published in the book *Introduction to Probability Theory and Computing* by J L Snell (Prentice-Hall, 1975). Here, in different notation, is the argument.

Let $f(n)$ be the number of complete permutations of n objects. Then $f(2)=1$, $f(3)=2$ and after that

$$f(n)=(n-1)\,[\,f(n-1)+f(n-2)\,] \qquad (1)$$

The first two of these formulae are easy to see. Here is a paraphrase of Snell's argument for the third.

Suppose we want to find the number of ways n people can have hats none of which are their own. Suppose $n-1$ of these people have already arrived at the "hat-swapping venue" when the last person, say Ann, arrives with her own hat, and all the other $n-1$ people have other people's hats. Ann can change her hat with any one of the other $n-1$ people, and then everyone will have someone else's hat. The $n-1$ people can have each other's hats in $f(n-1)$ ways, and Ann has $n-1$ people she can exchange with. Thus there are $(n-1)\,f(n-1)$ ways that this can be done.

However, there are other possibilities. There could still be one of the group of $n-1$ people with his or her own hat, but the remaining $n-2$ all having other people's hats. Thus Ann need only exchange hats with the person whose hat still needs exchanging and everyone will now have someone else's hat. This other possibility can occur in $(n-1)\,f(n-2)$ different ways. There is no duplication in the two methods for Ann to give up her hat, since if we undo the process, in the first

case we end up with only one person (Ann) having her own hat and in the other case two such people. These are the only ways that Ann can give up her hat; hence the recursion relationship is proved.

This last technical description, "recursion relationship", describes how $f(n)$ is to be calculated. We begin with the known values $f(2)=1$, $f(3)=2$ and then proceed in a stepwise fashion to compute from equation (1)

$$f(4)=9,\ f(5)=44,\ f(6)=265,\ \ldots,\ f(12)=176214841.$$

Such a rule allows us to compute $f(n)$ for any value of n, but if n is large it can become tedious, and moreover it lacks the immediacy and the theoretical advantage of an explicit formula. In order to find such a formula, we may proceed as follows.

First, take as an estimate of the number of complete permutations the total number of *all* permutations. This is 12! Now clearly, this is an *overestimate* as it includes permutations that are not complete. So now let us adjust it. To do this, consider the set of permutations that leave one element where it is (one hat with its rightful owner) and scramble the rest. We may choose the single element in 12 different ways and scramble the remaining 11 in 11! different ways. So our new guess is to be 12! – 12.11! This actually works out to be zero, so we are still not right. We now have too few possibilities.

It is easy to see the source of the problem. In counting the permutations that left one element in place, we also included twice all those that left two elements in their right places. So we took away too large a number. So now we must add back in the number of permutations that leave *two* elements intact and permute the remaining ten. We may choose the two elements in $\binom{12}{2}=\frac{12!}{(12-2)!2!}$ ways (compare the binomial formula given earlier) and permute the remaining 10 elements in 10! ways. So we add back in a number $\frac{12!}{(12-2)!2!}10!$, ie. $\frac{12!}{2!}$.

But now we have gone too far the other way, because we have added in as well those permutations that leave 3 elements unaltered and scramble the remaining 9. So now we must subtract a number that works out to be $\frac{12!}{3!}$. But even now we have overshot our goal and must add back in a number that works out to be $\frac{12!}{4!}$.

And now we must subtract $\frac{12!}{5!}$. And so on. Eventually we add back in $\frac{12!}{12!}$, and our work of correction is finally done.

The end result is $12! - 12.11! + \frac{12!}{2!} - \frac{12!}{3!} + \frac{12!}{4!} - \frac{12!}{5!} + \ldots + \frac{12!}{12!}$ which we can write more succinctly as $12!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{1}{12!}\right)$. (By convention, $0! = 1$.) More generally,

$$f(n) = n!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots \pm \frac{1}{n!}\right)$$

where the final term has a + sign if n is even and a – sign if n is odd. Strangely this formula is not given at the website I listed earlier.

We can check that this result actually satisfies equation (1), although the details are a little tricky. [One good approach is to use mathematical induction – see *Function*, *Vol* 22, *Part* 3, p. 92.] It is, however, easy to check those extra conditions $f(2) = 1$, $f(3) = 2$. And indeed, we can also see that $f(1) = 0$.

So now we can answer the question asked earlier: what is the probability of E_2 given E_1? (Given that the 12 people all had different starsigns, what is the probability of the astrologer getting all 12 wrong?) The answer is just $f(12)/12!$ and this works out to be

$$\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ \ldots \ + \frac{1}{12!}$$

a number that equals 0.367 879 to six decimal places.

More generally, we find $f(n)/n!$ and this is

$$\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ \ldots \ \pm \frac{1}{n!}$$

This number is known to tend toward $1/e$ as n gets large. In fact it very rapidly comes close to the limiting value of $1/e$; to six decimal places we have $1/e = 0.367879$, the value found just a minute ago.

So either way the poor astrologer was quite likely to be entirely wrong!

By setting up the situation so that all the starsigns were different, the probability of total error was marginally increased, but not significantly so in the social context here described. However, notice that if we were *computing* $1/e$, then the formula

$$\frac{1}{e} \approx \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots \pm \frac{1}{n!}$$

gives significantly better accuracy than the formula

$$\frac{1}{e} \approx \left(1 - \frac{1}{n}\right)^n$$

So, although the two expressions both approach $1/e$ as n gets bigger, one does so more rapidly than the other.

* * * * *

... just as the astronomer, the physicist, the geologist, or other student of objective science looks about in the world of sense, so not metaphorically speaking but literally, the mind of the mathematician goes forth in the universe of logic, in quest of the things that are there, exploring the heights and depths for facts—ideas, classes, relationships, implication, and the rest; observing the minute and elusive with the powerful microscope of the Infinitesimal Analysis; observing the elusive and vast with the limitless telescope of his Calculus of the Infinite; making guesses regarding the order and internal harmony of the data observed and collocated; testing the hypotheses, not merely by the complete induction peculiar to mathematics, but, like his colleagues of the outer world, resorting also to experimental tests and incomplete induction; frequently finding it necessary, in view of unforseen disclosures, to abandon one hopeful hypothesis or transform it by retrenchment or by enlargement:—thus in his own domain, matching point for point, the processes, methods and experience familiar to the devotee of natural science.

—Keyser, Cassius, J in *Lectures on Science, Philosophy and Art*

YOU'RE A MATHEMATICIAN!

OH! I NEVER WAS MUCH GOOD AT MATHS

Brian A. Davey*

I wish I had a dollar for every time I have heard the title of this article or something very similar to it. The fact that you're reading this indicates that you would almost certainly not say this yourself. Nevertheless the unfortunate fact remains that somewhere in their education most people have a negative experience with mathematics which has a lasting effect upon them. Preventing this from happening is probably the most important problem facing mathematics educators.

I don't intend to tackle this problem here. Rather, I'd like to tell you about the rest of the conversation. Typically, it goes something like this (since the natural abbreviation for my name is *BAD*, let's call the other person *GOOD*):

GOOD: "What do you do for a crust?"

BAD: "I'am a mathematician."

GOOD: "You're a mathematician! Oh! I never was much good at maths!"

BAD: "Unfortunately lots of people say that. Actually it's lots of fun. I get a real kick out of my research."

GOOD: "Fun, you've got to be kidding! And how can you do research in mathematics? Surely it's all been done. What do you actually do?"

BAD: "If you've got three hours I'll tell you. Actually it isn't hard to explain, but to do it justice would take a bit of time even if you'd already done some maths at uni. If you'd really like me to try, I'd be glad to; you can choose anything from a 10 minute snapshot to the full three-hour crash course."

* This article was published in *Function Vol* 12 *Part* 2.

Some people decide not to go any further and the conversation quickly changes to more important topics like "When will Collingwood win its next flag?" Most people opt for the 10 minute snapshot. On three occasions I've been asked for and delivered the three-hour crash course! What I'm about to give you is something in between. I should mention that I am a pure mathematician and the maths that I do is closer to philosophy than to engineering. Consequently, somewhere along the way *GOOD* usually asks, *"What is all this good for?"* I then explain that I do what I do because I enjoy it and don't seek or expect any applications. It comes as a surprise to me (and to *GOOD*) to discover that electronics engineers and computer scientists are actually interested in these ideas—but that's not why I study them.

Two-valued logic

In our everyday life we work with two-valued logic, by which I mean that any statement which makes sense is either *true* or *false*. Statements like *"Two plus two equals four"* or *"There are seven days in a week"* are true. Statements like *"Two plus two equals five"* or *"There are six days in a week"* are false. It might be hard to decide whether a statement like *"President Reagan is a good actor"* is true or false, but this is only because we haven't decided what "good actor" means. Once this is decided the statement will be either true or false.

Let **STATE** be the (rather large) collection of all English statements which make sense. Just as there are natural operations "+" (plus), "." (times) and "–" (negative) on the number line which produce new numbers from old ones, there are natural operations on **STATE** which produce new statements from old ones: they are "$\vee$" (or), "$\wedge$" (and) and "$\neg$" (not). Consider the following statements:

p: *"I will play basketball tomorrow"*

q: *"It will rain tomorrow"*

Then $p \vee q$ is the sentence *"I will play basketball tomorrow OR it will rain tomorrow"*, and $p \wedge q$ is the sentence *"I will play basketball tomorrow AND it will rain tomorrow"*.

Note that $p \vee q$ is true provided p is true or q is true (or both): $p \wedge q$ is true provided both p and q are true; $\neg p$ is true exactly when p is false. This is most easily expressed in some form of table. We let 1 stand for *"is true"*, 0 stand for *"is false"*; then the *truth tables* for $\vee$ (or), $\wedge$ (and) and $\neg$ (not) are as given in Figure 1.

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	$\neg p$
1	0
0	1

Figure 1

If you look at these tables they give us operations on the (rather small) collection consisting of just 1 and 0: the first line of the $\vee$-table says $1 \vee 1 = 1$, (which is said "1 or 1 equals 1") the third line of the $\wedge$- table says $0 \wedge 1 = 0$, etc. In this way we produce the more compact tables of Figure 2.

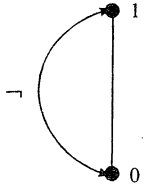
$\vee$	1	0
1	1	1
0	1	0

$\wedge$	1	0
1	1	0
0	0	0

	1	0
$\neg$	0	1

Figure 2

Finally we note that on 1 and 0, the operation $\vee$ is just "maximum" and the operation $\wedge$ is "minimum" while $\neg x$ equals $1 - x$. this gives us a diagramatic way of visualizing the three operations $\vee$, $\wedge$ and $\neg$ on 1 and 0 as shown in Figure 3. (The vertical line from the blob representing 0 to the blob representing 1 is there to remind you that 0 is less than 1 when you do calculations like $0 \vee 1 = \max\{0, 1\} = 1$ and $1 \wedge 0 = \min(1, 0\} = 0$.)



$$x \vee y = \max\{x, y\}$$
$$x \wedge y = \min\{x, y\}$$
$$\neg x = 1 - x$$

Figure 3

The operations $+$, $\cdot$ and $-$ on the number line satisfy certain natural laws such as :

$$x + y = y + x, \qquad x \cdot y = y \cdot x,$$
$$x \cdot (y + z) = x \cdot y + x \cdot x, \qquad x + (-x) = 0.$$

Similarly the operations $\vee$, $\wedge$ and $\neg$ on the truth values 1 and 0 satisfy certain laws known as the (rather pompous) *Laws of Thought of Laws of the Propositional Calculus* and nowadays better known as the laws of *Boolean algebra.* (These are named after George Boole who, in the middle of last century, was the first to attempt to give an algebraic formulation of the "laws of thought".) Below are some of the laws, which hold for $\vee$, $\wedge$ and $\neg$ on the truth values 1 and 0: for all x, y and z we have

$x \vee (y \vee z) = (x \vee y) \vee z$	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	(*associative*)
$x \vee y = y \vee x$	$x \wedge y = y \wedge x$	(*commutative*)
$x \vee x = x$	$x \wedge x = x$	(*idempotent*)
$x \vee (x \wedge y) = x$	$x \wedge (x \vee y) = x$	(*absorption*)
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	(*distributive*)
$0 \vee x = x,\ 1 \vee x = 1$	$0 \wedge x = 0,\ 1 \wedge x = x$	(*zero – one*)
$x \vee \neg x = 1$	$x \wedge \neg x = 0$	(*complementation*)

The laws state that no matter how you put in the truth values 1 and 0 for x, y and z, when you calculate the left-hand-side and the right-hand-side they will be equal. When checking the distributive law $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ there are 8 possible ways of assigning 1 and 0 to the variables x, y and z; as the truth table below shows, in each of these eight cases the left-hand-side and the right-hand-side are equal. (complete the proof by using Figure 2 or Figure 3 to calculate the missing entries. Then go on and construct the truth tables for each of the other laws.) You should also be able to see what these laws mean back on the collection **STATE** of statements. For example, the commutative law $x \wedge y = y \wedge x$ says that if p and q are statements, then the compound statement $p \wedge q$ (ie *"p and q"*) has exactly the same meaning as the compound statement $q \wedge p$ (ie *"q and p"*).

x	y	z	$x \wedge (y \vee z)$	$(x \wedge y) \vee (x \wedge z)$
1	1	1	1	1
1	1	0		1
1	0	1	1	
1	0	0	0	0
0	1	1		
0	1	0	0	
0	0	1		
0	0	0	0	0

This is where I come in! I am an algebraist. I study algebraic systems like the number line with its operations $+, \cdot$, and $-$ (high-school algebra) and equally well the collection **STATE** with its operations $\vee$, $\wedge$ and $\neg$ or the much smaller algebra of truth values 1 and 0 with the operations $\vee$, $\wedge$ and $\neg$ *(Boolean algebra)*. Most of the questions that I would consider are unfortunately beyond the scope of this short article, but here are a couple of starters.

Question 1

We have listed 18 laws of Boolean algebra. Is this list minimal? (The list will be minimal provided none of the given laws follows from the others.) The answer is certainly "no". For example, the idempotent laws follow from the absorption laws:

$$x = x \wedge (x \vee x) \qquad \text{(absorption with } y = x\text{)}$$
$$\therefore\ x \vee x = x \vee (x \wedge (x \vee x))$$
$$= x \vee (x \wedge y) \qquad \text{(where } y = x \vee x\text{)}$$
$$= x \qquad \text{(absorption)}$$

As a somewhat trickier exercise you might like to show that, given the associative, commutative, idempotent and absorption laws, each of the distributive laws follows from the other. Thus both idempotent laws and at least one distributive law can be deleted. Reducing the list of 18 laws to a minimal list is a non-trivial exercise.

Question 2

We have listed 18 laws of Boolean algebra. Is this list complete? That is, given any other law of Boolean algebra (which has been shown to be true by working our the corresponding truth table), does it follow (can it be proved) from the 18 laws already listed? (For example, below on the left is the truth table calculation (with some gaps for you to fill in) which shows that $(x \wedge y) \vee (x \wedge \neg y) = x$ is a law of Boolean algebra, and on the right is a proof that it follows from the original list of laws.) The answer to this question is "yes". Again this is not at all obvious and required, for example, a careful definition of what we mean by a "proof" like the one on the right-hand-side of the examples below.

x	y	-y	$(x \wedge y) \vee (x \wedge \neg y)$	x
1	1	0		1
1	0	1	1	1
0	1	0	0	0
0	0	1		0

$$y \vee (\neg y) = 1$$
$$\therefore x \wedge (y \vee \neg y) = x \wedge 1$$
$$\therefore (x \wedge y) \vee (x \wedge \neg y) = x$$

At this state *GOOD* usually throws in the first *"What's all this good for?"* To which I'm able to reply that a computer is "just" a massive collection of two-valued switches. Each switch is either closed, and so lets an electrical current flow through it, (this corresponds to the truth value 1), or open, and so does not let the current flow through it (this corresponds to the truth value 0). Connecting switches in parallel corresponds to the operation $\vee$ while connecting switches in series corresponds to the operation $\wedge$. Thus Boolean algebra is used to determine the flow of the current through the computer. Boolean algebra is fundamental to both electronics and computer science. The mention of applications to computing always seems to placate *GOOD* and we are able to continue.

Three-valued logic

I hope by now we have taken two steps forward and you have some feeling for the sort of mathematics which I, as an algebraist do. But we must also take one step backwards, for I have to admit that everything we've discussed so far about 2-valued logic and Boolean algebra was worked our late last century and early this century and (therefore) dates from before my birth. (It is important to note that it also predates the invention of the computer which to the modern pragmatist, like our

friend *GOOD*, is Boolean algebra's raison d'être). So what sort of algebra do I actually do? Read on.

There are various philosophical objections to two-valued logic. The most contentious of our 18 *"laws of thought"* is

$$x \vee \neg x = 1$$

which says that is p is any meaningful statement, then either p or its negation $\neg p$ is true. Put more simply, this says that any meaningful statement is either true or false —this is known as *"the law of the excluded middle"* since it allows no middle ground between the two extremes of falsity and verity (= truth). Consider again the statement

q: "It will rain tomorrow"

It could well be argued that, while we will know by the end of tomorrow whether the statement q is true or false, at the moment it should be assigned some other truth value which stands for *"don't know"*. We shall return later to this three-valued logic in which the law of the excluded middle fails. First let's look at a more subtle argument against the law of the excluded middle.

Consider the following proof that 1/0 is not a number. (In other words, you can't divide by 0.) In this proof 0 and 1 are representing the numbers "zero" and "one", not the truth values "false" and "true". We need the following facts about numbers.

(a) If y is any number, then $y \cdot 0 = 0$.

(b) If x and $1/x$ are both numbers, then $(1/x) \cdot x = 1$.

Let p be the statement *"1/0 is not a number"*. We wish to prove that the statement p is true. Suppose that p is false; then 1/0 is a number. Hence

$0 = 1/0.0$ by (a) with $y = 1/0$,

$= 1$ by (b) with $x = 0$.

Thus the assumption that p is false leads to the contradiction $0 = 1$. Consequently p is not false; that is, p is true.

This form of argument is very common within mathematics but quite rare in everyday arguments and so may seem a little strange to you. It is called *reductio ad absurdum* or simply *proof by contradiction.* In order to show that a statement p is true, we show that the assumption that p is false leads to a contradiction (like $0 = 1$) and hence p must be true. This definitely uses the law of the excluded middle, since we need to know that if p is not false then it is true.

There is a school of philosophical thought known as *intuitionism.* Intuitionists believe that if I wish to prove the existence of some thing or other, then I must actually produce it; in a sense they insist that I be able to walk into the room and show it to them. At first sight, that probably seems like a perfectly reasonable viewpoint. But if you accept it then you must, in general, reject proofs by contradiction (and consequently you must also reject the law of the excluded middle), as the following example illustrates.

In the game of Hex, which is marked by Parker Brothers Inc., two players, black and white, take turns to place pieces of their colour onto a diamond-shaped board with the aim of forming an unbroken chain of their pieces from one side to the opposite side. It is quite easy to show that there can never be a draw. Our intuition would tell us that the first player should have an advantage and indeed it can be proved that there is a winning strategy for the first player; that is, there is a set of instructions which, if followed by the first player, will always lead to a win for that player. Unfortunately, the only known proof of the existence of this set of instruction is a proof by contradiction—if we suppose that no such set of instructions exists, then we can derive a contradiction. An intuitionist will not accept such a proof, since the set of instructions has not actually been produced. (A detailed discussion of the game of Hex along with a sketch of this proof may be found in Martin Gardiner's *"Mathematical Puzzles and Diversions"*, published by Pelican).

The two-valued logic based on the laws of Boolean algebra is known as *classical logic*; all others are known as *non-classical logics.* The non-classical logic which replaces Boolean algebra in the intuitionist's view of the world is an important one, but is too complex to describe here. Let's now return to the "non-classical, three-valued logic with truth values *"true", "false"* and *"don't know"* to which we alluded earlier.

As before, let 1 stand for *"is true"* and 0 stand for *"is false"*, and now let ½ stand for *"don't know"*. We still have the operations $\vee, \wedge, \neg$ standing for *"or"*, *"and"*, *"not"* and our first task is to work out their three-valued truth tables, as we did for the two-valued case back in Figure 1. On 1 and 0 the operations $\vee$, $\wedge$, and $\neg$ should act exactly as they did for two-valued logic. What about $p \vee q$ if p is true and q is don't know, for example? Since $p \vee q$ will be true provided at least one of p and q is true, in this case $p \vee q$ will be true since p is true. Similarly, if p is true and q is don't-know, then $p \wedge q$ must be don't-know, since $p \wedge q$ is true only if both p and q are true. If p is don't-know, then $\neg p$ must also be don't-know. Arguing in this way we obtain the truth tables given n Figure 4. As in the two-valued case we can

p	q	$p \vee q$
1	1	1
1	½	1
1	0	1
½	1	1
½	½	½
½	0	½
0	1	1
0	½	½
0	0	0

p	q	$p \wedge q$
1	1	1
1	½	½
1	0	0
½	1	½
½	½	½
½	0	0
0	1	0
0	½	0
0	0	0

p	$\neg p$
1	0
½	½
0	1

Figure 4

View $\vee$, $\wedge$ and $\neg$ as operations on 1, ½, 0 as shown in Figure 5.

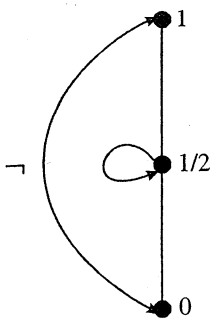
$\vee$	1	½	0
1	1	1	1
½	1	½	½
0	1	½	0

$\wedge$	1	½	0
1	1	½	0
½	½	½	0
0	0	0	0

	$\neg$
1	0
½	½
0	1

Figure 5

Note that, as in the two-valued cases, on 1, 1/2 and 0 the operation $\vee$ is *"maximum"* and the operation $\wedge$ is *"minimum"*, while $\neg x$ equals $1 - x$. This leads to the diagrammatic visualization of $\vee$, $\wedge$ and $\neg$ on 1, 1/2 and 0 shown in Figure 6.



$$x \vee y = \max\{x, y\}$$
$$x \wedge y = \min\{x, y\}$$
$$\neg x = 1 - x$$

Figure 6

The law of the excluded middle certainly fails here, since

$$1/2 \vee \neg 1/2 = 1/2 \vee 1/2 = 1/2 \neq 1.$$

Nevertheless the associative, commutative, idempotent, absorption, distributive and zero-one laws still hold. (You could check these laws and the laws given below by writing down all the three-valued tables, but it's slicker to observe each of these laws expresses a natural property of max and min.) In order to obtain a complete set of laws for our three-valued logic (in the sense of question 2 from the previous section), we must replace the complementation laws by

$\neg(x \vee y) = \neg x \wedge \neg y \quad \neg(x \wedge y) = \neg x \vee \neg y$ (de Morgan)

$\neg(\neg x) = x$ (double negation)

$(x \wedge \neg x) \wedge (y \vee \neg y) = x \wedge \neg x$ (Kleene)

The de Morgan laws are named after the 19th century mathematician Augustus de Morgan and may be familiar to you from set theory, while the Kleene law is named after the logician Stephen Kleene, who introduced this three-valued logic in 1938. As a slightly tricky exercise you might like to show that from these 20 laws it follows that $\neg 0 = 1$ and $\neg 1 = 0$.

In my research I have developed a general theory which applies, in particular, to this three-valued logic and yields interesting and useful information about it.

About now I either discover that *GOOD* is a closet philosopher and is fascinated by the concept of many-valued logics (Why stop at 3?) or I hear yet again *"What's all this good for?"* Well, as it happens, back in 1980 when I was doing this research, I was amazed to discover that there was a Japanese electronics engineer working on the same topic. Using completely different methods, we had obtained overlapping results. For me it was a piece of pure research motivated by a simple quest for knowledge, while for him it was a practical piece of research related to the building of computers based on three-valued switches rather than the usual two-valued ones.

BAD: "So now you've got some idea of the sort of things I work on."

GOOD: "Are there many algebraists who work on non-classical logics?"

BAD: "There aren't many who work exclusively on them. In fact I tend to use non-classical logics as testing grounds for general algebraic results. I actually spend most of my time doing research in universal algebra."

GOOD: "What on earth is *universal algebra*?"

BAD: "If you've got three hours I'll tell you ..."

* * * * *

Don't Be Anxious – Be Subtle

"Histories make men wise; poets, witty; the mathematics, subtle; natural philosophy, deep; moral, grave; logic and rhetoric, able to contend."

—Francis Bacon

"Anxious inquiry into ... mathematical problems leads away from the things of life, and estranges men from a perception of what conduces to the common good".

—Juan Juis Vives

* * * * *

NEWS

The 2000 Maths Festival at Melbourne University

Andrew Thornton, Mt Eliza

I just don't know where to start! It's been four days of imagination, hands-on activities, speeches across a spectrum of sheer earnestness to complete frivolity, and throughout the "festival" the very enjoyment that this word suggests. The festival was in the old arts building at Melbourne University; a building that took me an hour to find, so I inform you that any theory about mathematicians such as myself 'always' having good spatial map-reading abilities is apocryphal nonsense! The festival is part of the wider World Mathematical Year 2000, in which similar festivals and conferences will occur throughout the world.

The four days, from January 10 to 13 inclusive, had a theme unique to each day. Monday, sponsored by the Australian Mathematical Society, covered pure and applied mathematics in general. Tuesday, sponsored by the Institute of Actuaries of Australia, was designated "young mathematician's day" for students from primary and secondary school. Wednesday, sponsored by Hewlett Packard, was mainly about computer and calculator extensions for mathematics. Thursday's theme, sponsored by the Australian Computer Society, was along similar technological lines. Without any "cash for comments", I used one of Hewlett Packard's graphing calculators in a hands-on-lecture on the Wednesday. I had never touched one before, yet I was amazed at how easy it was to use! The lecturer, who is a mathematics teacher in Brisbane, said that in Queensland schools it is normal for year 9 students to use a graphing calculator daily in classes.

He was one of many teachers who lectured at the Festival. Indeed, if there was one theme that occurred throughout all four days it was that of mathematics education. Tertiary education—Professor Elijah Polak from the University of California gave a tutorial about engineering mathematics; applications to thermal devices for the treatment of prostate cancer, buildings that can withstand earthquakes, aeroplane design and much more. The mathematics was extremely advanced. It was too advanced for me at times! Secondary education—Bevan Penrose, a math teacher at Marsden State High School, outlined a teaching method that he'd developed. Marsden, a "rough, outer suburban Brisbane school" in which he spends the majority of his time in "student crowd control" (newsspeak for a bouncer?) sounds like quite a teaching challenge. Nevertheless, his method, which he calls constructivism, is achieving astonishing results. Students who "have never

which he calls constructivism, is achieving astonishing results. Students who "have never handed in a single assignment in their lives" are, after his method has been applied, actually asking for more assignments and passing their maths subjects comfortably. Primary education – William Spear from the University of Nevada discussed the subtleties of teaching mathematics at a primary school level. For instance, he asked everyone in the audience to draw a rectangle. Nearly everyone drew the "standard" rectangle on its long side. We are all taught in primary school that this is the *premier* rectangle! William Spear said correctly that mathematically a square in also a rectangle.

The 2000 Mathematics Festival was a thoroughly enjoyable experience! Every person who attended received a compendium of all the lectures, so any missed lectures can at least be read about. My favourite lecture was the "Coradi Intergraph" talk. Before electronic calculators were available, in the 1940's, the Coradi was a non-electronic manual device that performed calculus. I had never heard of this device, which looks like a giant 1 metre long pair of compasses. Melbourne University owns one such device and the lecturer placed it on the table in front of us. A sheet of paper is placed underneath it, and a pencil is put into a holder, and the pencil draws the desired integral answer upon the paper.

* * * * *

> We mathematicians who operate with nothing more expensive than paper and possible printer's ink are quite reconciled to the fact that, if we are working in a very active field, our discoveries will commence to be obsolete at the moment they are written down or even at the moment they are conceived. We know that for a long time everything we do will be nothing more than the jumping off point for those who have the advantage of already being aware of our ultimate results. This is the meaning of the famous apothegm of Newton, when he said, "If I have seen further than other men, it is because I have stood on the shoulders of giants."
>
> —Norbert Wiener
> in *I am a Mathematician*, Garden City: Doubleday, 1956.

* * * * *

Letter to the Editor

Dear Editor,

I found D F Charles' article *Ruler and Compass Constructions* very absorbing and enjoyed his last illustration in particular as I have not seen it before. His construction for $\sqrt{x}$ valid for $2 < x < 4$ was also intriguing. But since two further constructions were needed for $0 < x < 2$ and $x > 4$, I was wondering whether there could be a single construction which is valid for all positive x. Indeed there is!

Construction

First draw a line segment $\overline{BDC}$ with $BD = 1$ and $DC = x$. Next, bisect this segment at M. With BM as radius erect a semicircle with BC as diameter, as shown in Figure 1. Lastly, construct $\overline{DA}$ perpendicular to $\overline{BC}$ and intersecting the circle at A. Then $AD = \sqrt{x}$. This is valid for all $x > 0$.

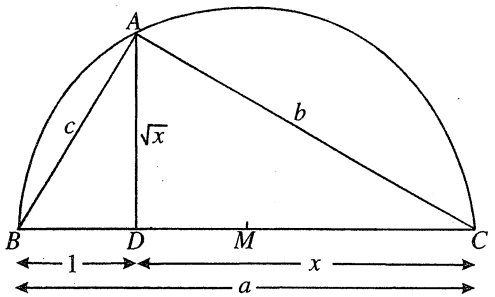


Figure 1

Proof

We first realise that ΔABC must be right angles at A as its hypothenuse is the diameter of our semicircle. So we have three right angled similar triangles:

$$\Delta ABC\,,\ \Delta ABD\,,\ \Delta ADC$$

For ΔABC we have by Pythagoras

$$b^2 + c^2 = a^2 = (x + 1)^2 \tag{1}$$

similarly for ΔABD we find

$$AD^2 + 1 = c^2 \tag{2}$$

And in ΔADC we obtain

$$AD^2 + x^2 = b^2 \tag{3}$$

Adding (2) and (3) yields

$$b^2 + c^2 = 2\,AD^2 + x^2 + 1 \tag{4}$$

Using (1) in (4) provides

$$x^2 + 2x + 1 = 2AD^2 + x^2 + 1 \tag{5}$$

which simplifies to $AD = \sqrt{x}$, valid for $x > 0$.

* * * * *

It is easier to square the circle that to get round a mathematician.

—A De Morgan in *Budget of Paradoxes*, London, 1872

* * * * *

HISTORY OF MATHEMATICS

Existence Theorems

Michael A B Deakin

It would be misleading to describe the biologist J B S Haldane as a mathematician, but equally it would be a mistake to ignore his important and interesting mathematical work. He lived from 1892 to 1964 and is usually referred to as being a biochemist, a physiologist and a geneticist. In all these fields he was concerned to place the Science on a firm mathematical footing, an endeavour he himself would have referred to as "quantitative biology". We begin with one of his biomathematical investigations. In a series of scientific papers published over the years from 1924 onwards, he explored the consequences of natural selection in the light of Mendel's genetic discoveries.

Suppose a gene can exist in either of two forms (the technical term for these is "alleles"), *A* and *a*. Because individuals each possess two copies of each gene, three possibilities exist: *AA*, *Aa* and *aa*. Suppose (as often is the case in practice) that the combinations *AA* and *Aa* give rise to indistinguishable and normal individuals, but the combination *aa* is lethal. We then have the case of a fatal genetic defect. To analyse this case further, suppose that of the genes present at the *n*th generation, a proportion q_n are of the "bad" type. We may now follow the extinction of this form by means of a difference equation

$$\Delta q = q_{n+1} - q_n = \frac{-q_n^2}{1+q_n}$$

This equation has the solution

$$q_n = \frac{q_0}{1+nq_0}$$

where q_0 represents the initial proportion (before any generations have been subjected to the force of natural selection).

However, this is a very special case, and in more general situations, the difference equation has a more complicated form, and it is no simple matter to write down a formula for the solution.

It was this situation that Haldane later referred to when he wrote of his disappointment with the mathematicians he consulted over his problem.

He wrote:

> "... the few professional mathematicians who have interested themselves in such matters have been singularly unhelpful. They are apt to devote themselves to what are called existence theorems, showing that the problems have solutions. If they hadn't, we shouldn't be here, for evolution would not have occurred."

There are problems in arguing (as Haldane here is) from applications of mathematics to mathematics itself, but I won't go into this here. Rather let me make the point that the general denigration of existence theorems is more than a trifle unfair. Existence theorems have a very important place in mathematics.

To see this, consider the last two of these history columns. My most recent dealt with the attempts to prove Euclid's "parallel postulate" from his other axioms, and we saw that it turned out that no such proof was possible. The column before that described Wantzel's proof that the classic problem of angle trisection was likewise impossible in the terms in which it had been posed; there is no classic ruler and compass construction that can trisect a general angle.

We might refer to these results as "non-existence theorems"! They are clearly very important and tell us not to waste our time in pursuits that ultimately turn out to be futile.

One of the most famous of all recent mathematical advances could likewise be characterised as a "non-existence theorem". This is Fermat's Last Theorem, whose story John Stillwell told in *Function*, *Vol* 18, *Part* 2. This tells us that if a, b, c and n are positive integers, then there is no solution to the equation

$$a^n + b^n = c^n$$

if $n > 2$.

So an existence theorem at least assures us that we are not off on a wild goose chase!

At the high school level of mathematics, perhaps we see the need for existence theorems first when we encounter surd equations, equations involving square roots. Take as an example the equation

$$\sqrt{x}+\sqrt{x+3}=3.$$

I leave it to the reader to solve this equation and to check that there is a single solution $x=1$, and to check by substitution that this actually *is* a solution. But now compare this with the equation

$$\sqrt{x}-\sqrt{x+3}=3,$$

which is readily seen to have no solution.

[When I first encountered surd equations, I read in the textbook we then used the perceptive remark that equations were "statements of hope" rather than "statements of fact". I now wish I could recall who it was that made this very insightful remark, and where it was said. It is certainly very much to the point in the context of this column: things we hope for have to be shown to be realistic expectations.]

Readers will also be familiar with the situation with quadratic equations. Suppose we have the equation

$$ax^2+bx+c=0.$$

If we think of x as being a *real number*, then this equation has exactly two (distinct) real roots if $b^2>4ac$, one real root if $b^2=4ac$, and none at all if $b^2<4ac$.

If we move on to *cubic equations*, the situation gets more complicated. I will not go into it in all its detail. However if we take the cubic equation

$$ax^3+bx^2+cx+d=0,$$

we can easily show *that there is necessarily at least one real root.* The simplest way to show this is to divide through by a (which is not zero, because if it were we wouldn't have a cubic!) and then to show that, as x increases from large negative values to large positive values, the expression on the right-hand side goes from negative to positive and so, for some suitable x, must be zero.

A similar argument shows that any polynomial of odd degree must possess at least one real root.

This information is of little *immediate* help in solving the equation, but it can be used to assist in the search for solutions. But now consider what happens if we look not for real solutions, but rather for complex ones. Take a general polynomial equation

$$a_n z^n + a_{n-1} z^{n-1} + \ \ldots + a_1 z + a_0 \ = \ 0,$$

where we have written z in place of x to emphasise that it is to be thought of as complex, and the symbols a_n, etc are just shorthand for "the coefficient of z^n" and so on.

In fact we may simplify this last equation a bit by supposing we have already divided through by a_n (as we envisaged in the simpler, cubic, case) and so may write the general polynomial equation as

$$z^n + a_{n-1} z^{n-1} + \ \ldots + a_1 z + a_0 \ = \ 0. \qquad (1)$$

We now have a remarkable existence theorem first proved by Carl Friedrich Gauss (1777–1855), one of the very greatest of all mathematicians ever to live. So important is this theorem that it is now referred to as "the fundamental theorem of algebra". It states that equation (1) necessarily possesses a solution. The proof is difficult, but it has distant affinity with the earlier proof that cubic equations possess real roots.

Once the fundamental theorem is proved, we may deduce some remarkable and beautiful consequences. If equation (1) has a root, call this root α_1 (short for "first root"). It is now possible to factorise the left-hand side of equation (1), and so reach

$$(z - \alpha_1)(z^{n-1} + b_{n-2} z^{n-2} + \ \ldots + b_1 z + b_0) \ = \ 0.$$

(That such factorisation is possible was known before Gauss, and is much easier to prove than is the fundamental theorem.)

But now this new form of the equation may be split into the two possibilities $z = \alpha_1$ and $z^{n-1} + b_{n-2} z^{n-2} + \ \ldots + b_1 z + b_0 \ = \ 0$. The first of these possibilities

retrieves the root we have already found; the second is another polynomial equation of the same form as equation (1), so that it too must obey the fundamental theorem. So this new equation has a root which we can call α_2 (for "second root").

And so we may proceed, until we have found exactly n roots (not necessarily distinct, however). We thus have the result:

> In complex algebra, every polynomial equation of degree n has exactly n roots.

I hope you agree with me that this is a very elegant result!

Indeed I hope you agree with me also on a more general point: that existence theorems have an important place in mathematics. All the same, Haldane's frustration with them has some force. Let me illustrate this with a brilliant piece of mathematics, which nevertheless contrives to leave us unsatisfied. It has appeared before in *Function*, but it bears repeating.

We shall set out to show that there are irrational numbers a and b such that a^b is rational. The proof asks us to think first about the number $\sqrt{2}^{\sqrt{2}}$. Now either this number is rational or else it is irrational.

If it is rational, then we have found what we set out to discover and so we need look no further.

If on the other hand, it is irrational, then we may set $a = \sqrt{2}^{\sqrt{2}}$ and put $b = \sqrt{2}$, and then form $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$. And this is clearly rational. So either way, we are done.

However, this proof, elegant as it undoubtedly is, tells us nothing about the number $\sqrt{2}^{\sqrt{2}}$ itself. We are left wondering whether it is irrational (as we might suspect) or is, after all, rational. The proof is silent on this matter, and we need to use other (and difficult) means to discover that $\sqrt{2}^{\sqrt{2}}$ is, after all, irrational.

So perhaps we can retain a sneaking sympathy with Haldane and his impatience with existence theorem.

COMPUTERS AND COMPUTING

An XOR-cise in Swapping

Peter Grossman

Swapping the values stored in two memory locations is a fundamental task in computing. For example, many of the algorithms used for sorting records (into alphabetical or chronological order, say) operate by carrying out a sequence of swaps, where each swap exchanges a pair of records.

Let's suppose we have two variables, x and y, whose values we wish to swap. The first thing we might think of doing is the following:

1. $x \leftarrow y$
2. $y \leftarrow x$

The left-pointing arrow is used here to denote *assignment*: $x \leftarrow y$ means "take the value stored in y, and store it in x". (Many programming languages use an ordinary equals-sign for assignment; however, the arrow serves as a useful reminder that assignment is a process, not a statement that two quantities are equal.)

Of course, this simple-minded approach won't work. The problem is that the value originally stored in x is lost in Step 1 when x is assigned a new value. Then, in Step 2, the value assigned to y will be the new value of x (i.e., the original value of y), rather than the original value of x.

A solution to the problem is readily found: use a temporary variable, t, to store the original value of x. The modified algorithm looks like this:

1. $t \leftarrow x$
2. $x \leftarrow y$
3. $y \leftarrow t$

This procedure is widely used, but is it the only way of carrying out a swap? In particular, can a swapping algorithm be constructed that avoids having to use extra memory by creating a temporary variable? If the only operation used in the algorithm is assignment, then the answer to this last question is no. If other operations are permitted, however, it turns out that it can be done. There is a method for swapping two records without using any extra memory; it uses the fact that all

data is stored in a computer as strings of bits (zeros and ones), and it employs a logical operation known as an *exclusive-or* that can be applied to the bits.

The word "or" is used in English in two ways. If someone offers you tea or coffee, you naturally assume that you may have one or the other, but not both! This is an example of "or" used in the *exclusive* sense. On the other hand, if a discount is available to anyone who is a student or a senior citizen, you would expect the discount also to be available to someone who is both a student and a senior citizen. In this instance, "or" is used in the *inclusive* sense. In both computing and mathematics, "or" is always understood to mean inclusive-or, unless the contrary is stated explicitly. Thus, if A and B denote any two propositions, then "A or B" (denoted $A \vee B$) means "either A or B or both A and B". If we mean exclusive-or, we must say "exclusive-or". Exclusive-or is sometimes called "xor", and is denoted by $\oplus$: thus, $A \oplus B$ means "either A or B but not both". The properties of "or" and "xor" are summarised in the truth table in Table 1, in which 1 denotes true and 0 denotes false.

A	B	$A \vee B$	$A \oplus B$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	0

Table 1

We have introduced the exclusive-or operation by giving 0 and 1 a particular interpretation: the truth values "false" and "true". However, a 0 or a 1 stored in the memory of a computer could mean any of a number of things: it could be a bit in the binary representation of a number, part of the code for a character in a piece of text, part of a graphic image, or indeed one bit of information of any kind. Regardless of whether 0 and 1 denote truth values or something else, we can use Table 1 to define an operation, denoted by $\oplus$ and still called "exclusive-or". That is what we will do from here on.

Now suppose we want to swap two variables, x and y, where each variable stores just one bit (0 or 1). The following algorithm does this, without using a temporary variable:

1. $x \leftarrow x \oplus y$
2. $y \leftarrow x \oplus y$
3. $x \leftarrow x \oplus y$

You can convince yourself that the algorithm works, by checking each of the four possible combinations of values of x and y. For example, if $x=0$ and $y=1$ initially, then x and y take the values shown in Table 2 as the algorithm proceeds.

	x	y
Initially	0	1
After Step 1	1	1
After Step 2	1	0
After Step 3	1	0

Table 2

We can see from the last line of Table 2 that the values of x and y have been swapped in this case. The other three cases are left for you to verify for yourself.

What should we do if x and y contain strings of bits, rather than just a single bit each? (We assume x and y contain the same number of bits, because if they didn't, it would not be meaningful to swap them.) The answer is simple: apply the algorithm "bitwise". In other words, if x and y contain the bit strings $x_1x_2\ldots x_n$ and $y_1y_2\ldots y_n$ respectively, then $x \oplus y$ is the bit string $(x_1 \oplus y_1)(x_2 \oplus y_2)\ldots(x_n \oplus y_n)$.

The exclusive-or method of swapping is not generally used in algorithms for sorting. There is another situation, however, in which exclusive-or swapping is commonly used. Suppose a temporary object (such as a menu, a message box, or even the mouse pointer) is to appear on your computer screen on top of the current screen image. As soon as the object is removed, the original screen image should reappear. This is achieved in the following way. The screen image is stored in a memory location called the *screen buffer*. The temporary object is stored in another memory location called a *backing store*. To show the object on the screen, the contents of the part of the screen buffer where the object is to appear is swapped with the contents of the backing store. To remove the object from the screen, the contents of the two memory locations are swapped again. For efficiency reasons, this swapping is generally implemented in the computer's hardware. This is done using the exclusive-or method, since an exclusive-or operation is simple to implement in a digital circuit, and, unlike a purely assignment-based swap, it avoids the need to use a third memory location.

* * * * *

Fair shares

PROBLEM CORNER

PROBLEM 23.4.1 (from Crux Mathematicorum with Mathematical Mayhem)

Prove that if m, n are natural numbers and $n \geq m^2 \geq 16$, then $2^n \geq n^m$.

SOLUTION

Let n, m be natural numbers with $n \geq m^2 \geq 16$. Let $x = \sqrt{n}$, we show that $x^2 \leq 2^x$. From this result it then follows that $n^m \leq (x^2)^x \leq (2^x)^x = 2^n$. In order to establish $x^2 \leq 2^x$ we note that

$$x^2 \leq 2^x \Leftrightarrow 2\log_2 x \leq x \Leftrightarrow \frac{2\ln x}{\ln 2} \leq x \Leftrightarrow \frac{2}{\ln 2} \leq \frac{x}{\ln x}$$

Now if we define $f(x) = \frac{x}{\ln x}$, then $f'(x) = \frac{\ln x - 1}{(\ln x)^2}$ so that $f'(x)$ is certainly positive for $x \geq 4$. But $f(4) = \frac{2}{\ln 2}$ so we have $f(x) \geq \frac{2}{\ln 2}$ for $x \geq 4$. This establishes the last inequality above and hence we have established that $x^2 \leq 2^x$ for $x \geq 4$.

Other solutions were received from Keith Anker, Carlos Victor and Julius Guest.

PROBLEM 23.4.2 (from Crux Mathematicorum with Mathematical Mayhem)

A certain country contains a (finite) number of towns that are connected by unidirectional roads. It is known, that, for any two such towns, one of them can be reached from the other one. Prove that there is a town such that all the remaining towns can be reached from it.

SOLUTION

Let $S(n)$ be the claim that if a country has n towns connected by unidirectional roads with the property that for any two towns one of them can be reached from the other, then there is a town that can reach all other towns. We establish that $S(n)$ is true for all n by induction.

The result is immediate for the cases with $n \leq 2$.

For the induction step we assume that $S(n)$ holds for all $n < k$ and we show that $S(k)$ also holds. Let $t_1 \ldots t_k$ be the towns, and let M be the set of all towns (excluding t_1) that can be reached from t_1, and let N be the set of towns that cannot be reached from t_1. So every town in N can reach t_1 and there is no route from a town in M to a town in N. If N is empty then t_1 is the desired town. If N is not empty then for any two towns in N, one can be reached from the other and furthermore this route cannot include a town in M. The number of towns in N is less than k so we can apply the induction hypothesis to give us a town t^* that reaches all towns in N. This town also reaches t_1 so all towns in M can also be reached from t^*. This completes the induction step.

Other solutions were received from Keith Anker and Carlos Victor.

Problem 23.4.3 (adapted from Crux Mathematicorum with Mathematical Mayhem)

An "n-m party" is a group of n girls and m boys. An "r- clique" is a group of r girls and r boys in which all of the boys know all of the girls, and an "r-anticlique" is a group of r girls and r boys in which none of the boys knows any of the girls. Show that there is a number m_0 such that every 9–m_0 party contains either a 5-clique or a 5-anticlique.

SOLUTION

Since there are 9 girls present each boy can either nominate 5 girls he knows or 5 girls unknown to him. Suppose that to each boy we associate an ordered pair, the first member being a subset of 5 girls all of whom he knows or all of whom he does not know, and the second member being a zero or a one according as the girls are known to him or not known. There are ${}^9C_5 * 2 = 252$ possible pairs. Now if there are more than 252*4 = 1008 boys present then at least 5 boys must be associated

with the same ordered pair, and so that if $m_0 = 1009$ there must be either a 5-clique or a 5-anticlique.

Other solutions were received from Keith Anker and Carlos Victor.

PROBLEM 23.4.4 (Part (a) proposed by Julius Guest, East Bentleigh)

(a) Evaluate $\int_0^1 \frac{x^4}{(1+x^2)^3}\,dx$

(b) Generalise the result for the integral in part (a) to

$$\int_0^1 \frac{x^{2m-2}}{(1+x^2)^m}\,dx, \quad \text{where} \quad m = 1, 2, 3, \ldots$$

SOLUTION

(a) (Julius Guest, East Bentleigh)

The substitution $x = \tan\theta$ leads to the integral $\int_0^{\frac{\pi}{4}} \sin^4\theta\, d\theta$, and then using $\sin^4\theta = \frac{1}{8}(\cos 4\theta - 4\cos 2\theta + 3)$, we find $\int_0^{\frac{\pi}{4}} \sin^4\theta\, d\theta = \frac{3\pi - 8}{32}$.

Solutions were also received from Keith Anker, J.A. Deakin, Bill Tetley and Carlos Victor.

(b) There were two approaches to this problem, one using the substitution $x = \tan\theta$, the other employing integration by parts.

(i) Using the same substitution as in part (a) leads to the integral $\int_0^{\frac{\pi}{4}} \sin^{2m-2}\theta\, d\theta$. This can readily be evaluated for any positive integer m by the well known reduction formula for $\int \sin^n\theta\, d\theta$.

(ii) Observing that $\frac{d}{dx}(1+x^2)^{1-m} = \frac{2x(1-m)}{(1+x^2)^m}$, for $m > 1$, we can write the integral in the form $I_m = \frac{1}{2(1-m)}\int_0^1 x^{2m-3}\frac{d}{dx}(1+x^2)^{1-m}\,dx$ and then integration by parts leads to the recurrence formula.

$$I_m = \frac{2m-3}{2m-2}I_{m-1} - \frac{1}{2^m(m-1)}, \quad m>1.$$

This recurrence formula allows us to find I_m for $m > 1$ by using the case $I_1 = \frac{\pi}{4}$.

Solutions were received from Keith Anker, Carlos Victor, J.A. Deakin, Bill Tetley and Julius Guest.

PROBLEM 23.4.5 (adapted from 1986 Qualifying Round of the Swedish Mathematics Olympiad)

Prove that $(1999!)^{\frac{1}{1999}} < (2000!)^{\frac{1}{2000}}$.

SOLUTION (J.A. Deakin, Shepparton, Victoria)

From the inequality $1.2.....n < (n+1).(n+1).....(n+1)$ we see that $n! < (n+1)^n$, and multiplication by $(n!)^n$ gives us the inequality $(n!)^{n+1} < ((n+1)!)^n$. Now raising both sides of this last inequality to the power $\frac{1}{n(n+1)}$ gives $(n!)^{\frac{1}{n}} < ((n+1)!)^{\frac{1}{n+1}}$. Take $n = 1999$ and we have the desired result.

Solutions were also received from John Barton, Carlos Victor, Keith Anker. Another approach based on Stirling's approximation was proposed by Julius Guest.

PROBLEMS

PROBLEM 24.1.1 (from The AMATYC Review)

Let p be prime number. Prove that p is of the form $8n \pm 1$ if and only if there exists an integer k such that $p = \sqrt{48k+1}$.

PROBLEM 24.1.2 (from Mathematics and Informatics Quarterly)

Let $n \geq 2$ be a positive integer and let $P(n)$ denote the product of the positive divisors (including 1 and n) of n. Find the smallest n for which $P(n) = n^{10}$.

PROBLEM 24.1.3 (from Mathematics and Informatics Quarterly)

Using my pocket calculator I divide one positive integer by another giving answer 0.5876578. Both integers were less than 1000. What were the two integers?

PROBLEM 24.1.4 (from Mathematical Spectrum)

Determine the value of the definite integral $\int_2^3 \frac{dx}{\sqrt{(5-x)}+\sqrt{(x-1)}}$

* * * * *

And who can doubt that it will lead to the worst disorders when minds created free by God are compelled to submit slavishly to an outside will? When we are told to deny our senses and subject them to the whim of others? When people devoid of whatsoever competence are made judges over experts and are granted authority to treat them as they please? These are the novelties which are apt to bring about the ruin of commonwealths and the subversion of the state.

—Galileo Galilei, in the margin of his own copy of *Dialogue on the Great World Systems*

* * * * *

Published by Department of Mathematics & Statistics, Monash University