Eureka Digital Archive

archim.org.uk/eureka

Eureka Editor
The Archimedeans
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WA
United Kingdom

archim-eureka@srcf.net

Published by The Archimedeans, the mathematics student society of the University of Cambridge

Thanks to the Betty & Gordon Moore Library, Cambridge

Eureka 45 January 1985

ISSN 0071 - 2248

CORRESPONDENCE:
(Clearly marked "*Editor*" or "*Business Manager*")
The Arts School
Bene't Street
CAMBRIDGE CB2 3PY
England

ELECTRONIC MAIL:
(*see opposite*)
archim%camphx@cagq (UK)
archim%camphx%cagq@ucl-cs.arpa (USA)

Your Actuarial Career

Coopers & Lybrand is one of the leading international firms of chartered accountants and business consultants, and have a well established and rapidly expanding Pensions and Actuarial Department.

We are now looking for up to three actuarial trainees – highly numerate students who are expecting a very good mathematics degree and preferably have an interest in statistics – to join our small, highly professional Pensions and Actuarial Department based in London. Here you'll have the opportunity to acquire a broad range of experience, advising clients on all aspects of pensions and related benefits. You will also become involved in general insurance, life assurance, and a certain amount of statistical work.

Although much of the work over the first two or three years will be office-based, there will be extensive opportunities for liaison with staff from other departments of the firm and their clients.

You will be expected to join the Institute of Actuaries and to study for the Institute's examinations with study leave and tutorial costs provided by the firm. Starting salary will be £8,000 per annum or more, depending on the examination exemptions you obtain. Within an expanding department your career progression will be based entirely upon your work performance and examination results and the rewards for the successful student are high.

It is our aim to develop the talents that place those who qualify with us amongst the leaders in their field. Take your first step by contacting your careers advisory service or Elizabeth Warren our National Student Manager at the address below for further information on the services and training provided by our Pensions and Actuarial Department.

Coopers & Lybrand

Abacus House
Gutter Lane
Cheapside
London EC2V 8AH
01-606 4040

Editorial

This is the fifth and final issue of *Eureka* to be produced essentially by those who matriculated in 1979. During these five years the Archimedeans has seen *two* rises and an intervening decline, and, we hope you will agree, *Eureka* has developed a little.

This issue is *apparently* shorter than the last. The primary reason for this is aesthetics, although factors of finance and editorial lethargy have played their part. However you will notice that we have given up the double line spacing used in the past, so each page is in fact longer. Readers' comments on this and other technical matters are welcome.

It was a long time ago that we were forced to give up traditional type-setting methods on grounds of expense, but now the New Technology is beginning (at last) to have a *beneficial* effect on *Eureka*. Articles are, of course, always welcome, but it would be paricularly helpful to future editors if they could be submitted in electronic form if possible; then we shall have the advantage of uniformity of style and our presentation should soon be restored to its former glory.

Of course the fact that the present editors are in the upper decile of the distribution as regards status means that we have found it even more difficult than usual to attract the interest of undergradutes. Nevertheless *Eureka* can only publish what it receives, and if you think its style should be different then it's up to you to write something. On the other hand *Eureka* does *not* want mathematical material at such a low level as to be insulting to its (undergraduate) readership, or "humorous" material which is unsuitable for publication. Judging by the style of his article here, however, Eddy Welbourne should be more successful on this front.

Finally, the founders of *Eureka* (and, for that matter, the Archimedeans) intended it to be a vehicle for discussion of the purpose and nature of mathematical study and teaching, and only secondarily for "the immature researches of undergraduates". It is therefore an entirely proper forum for (even political) debate on the Tripos, the division of the Faculty, moral questions relating to mathematics (cf *Quote Quiz*) and the funding of mathematical research.

* * *

This University, like any other large and socially self-sufficient community, has an extensive and intricate level of structure above that for which it primarily exists. This tends to be given little credit by most of its inhabitants, and even less by those outside, but it's just as important as the bricks and mortar of the University itself: if it thrives then so does the University, if part of it collapses it's just as if a building were to collapse. I refer, of course, to the wealth of clubs and societies which we have, all run *by* students *for* students, of which we all make use.

Sometimes I think it's quite remarkable that we have them at all. For when you realise that the senior officers of a typical society with several hundred members are expected to put in a dozen hours a week, to subsidise its activities out of their own pockets and get nothing but a single-line comment on their CVs and a 2:2 at the end of it, you wonder why they bother. Of course, if you happen to choose an organistion related to a rich institution such as a college, you do a bit better than you do out of a hard-pressed faculty society, but it still doesnt compare with the going rate for office staff, let alone top executives in industry.

From time to time amongst the multitudes of hard-working but unenlightened caretakers of such bodies comes someone with vision. At worst he restores the flagging momentum, but at best he provides inspiration for a decade or more. Often there is someone who believes that some important point is to be made and has such conviction that he is willing to stake all upon making it. But our time here is very short, and most people cant be bothered or dont have the time to weigh up all the arguments fully, and all too frequently there are those who like to have the honest but firm disagreements of others turned into gladiatorial contests. Unfortunately the ordinary members dont understand what they're losing, and the other officers, whilst perfectly willing to reap the rewards of his success, are too naïve or too cowardly to tell him where to stop, or to defend the honest man against the hack.

Paul Taylor, 2/11/82

* * *

The Triennial Dinner

This year is the fiftieth anniversary of the Archimedeans, and to celebrate we are planning a particularly sumptuous **Triennial Dinner.** The Dinner will be held in Hall in St. John's College on the evening of Saturday the ninth of March, and the guest speakers will include Professor Sir Herman Bondi, Master of Churchill College. We particularly look forward to seeing any past members who may be able to attend.

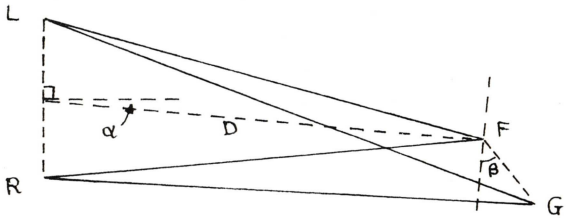
All enquiries about the dinner should be addressed to Ian Hall of St. John's College, Cambridge CB2 1TY.

On Seeing Things

Christopher Longuet-Higgins

Helmholtz once declared that the primary function of vision is to establish a depth map of the visible world - or words to that effect. Stereoscopic vision serves this purpose up to moderate distances, but the theory of stereopsis is not altogether straightforward. In figure 1 *L* and *R* are the left eye and the right eye; *F* and *G* are visible features, and the observer is looking straight at one of them, say *F*. The two retinal images supply the angles between the rays entering each eye, but the observer cannot locate the sources without knowing the directions in which his eyes are looking. There are in fact two undetermined degrees of freedom in the problem, represented by the distance and direction of fixation of the point *F*. The usual hypothesis is that these *viewing parameters* are obtained from non-visual evidence such as the effort required to bring the images into focus or to converge the eyes to the required extent, but it does not square with the fact that people are very bad at estimating the distance of an isolated point source in a dark room. As we shall see, this difficulty can be largely dispelled by recognising that the real world has one more dimension than figure 1; but first let us see what the two-dimensional theory has to say about the perception of the relative distances of neighbouring features.

Fig.1



In figure 1 the distance *D* is measured from the mid-point of *LR* to the point *F*, in units of the distance *LR*; it is assumed to be large enough for its inverse square to be negligible. The angle α is the so-called *angle of gaze* and β is the tilt of the line *FG* relative to the line of sight. If *G* is close to *F* then the ratio of the angles which *FG* subtends at *L* and at *R* will depend only on α, β and *D*; the horizontal magnification $\measuredangle FGR / \measuredangle FLG$ will be $1+H$, where

$$(1) \qquad H = \frac{\sin\alpha + \tan\beta \cos\alpha}{D}$$

This formula accounts quite nicely for the *geometric effect* first observed by the late K.N. Ogle. If one holds in front of the right eye a cylindrical lens which magnifies the retinal image in the horizontal direction only, and looks - with both

eyes - at a surface in the fronto-parallel plane (α=0,β=0), then the surface acquires a pronounced tilt, of magnitude approximately

(2) $\beta = \arctan HD$

provided that D is not too large. What the visual system is presumably doing is substituting the observed value of H into equation (1) to obtain a perceived value for the tilt β. But the question remains: how does the observer know what values to assign to the viewing parameters α and D?

The perceptive reader will have spotted a loophole in the argument that the viewing parameters α and D cannot be obtained from the retinal images alone. The argument tacitly assumes the world to be two-dimensional, so that the pair of rays GL and GR will still intersect somewhere in space even if the pencils to which they belong are rotated slightly in the plane of figure 1. But in a three-dimensional world, where G does not necessarily lie in the horizontal plane LFR, a rotation of either pencil would cause the rays LG and RG to miss one another altogether. So in three dimensions the condition that each ray entering the left eye shall intersect its partner entering the right eye imposes a powerful constraint on the relative orientation of the two eyes, and makes it possible at least in principle for the viewing parameters α and D to be computed from the retinal images alone.

As soon as it was realised that the vertical dimension could play an important role in the binocular estimation of depth, John Mayhew of Sheffield University came forward with a delightfully simple theory of how the computation could be carried out. An object which is nearer to the right eye than the left will cast a taller image on the right retina than on the left retina, and the visual system could very well be sensitive to such differences. Going back to figure 1, think of F as a finger held up nearer the right eye than the left. Then to the first order in D^{-1} the vertical magnification of the right retinal image over the left will be 1+V, where

(3) $$V = \frac{\sin \alpha}{D}$$

A measurement of V therefore imposes one constraint on the viewing parameters; but there is another which can be obtained from the directional variation of V. If one differentiates equation (3) with respect to α, using the relation

(4) $$\frac{1}{D}\frac{dD}{d\alpha} = \tan \beta,$$

one obtains straightforwardly

(5) $$\frac{dV}{d\alpha} = \frac{\cos \alpha}{D} - \frac{\tan \beta \sin \alpha}{D},$$

and if, as often happens, α and β are both small angles, then (5) reduces to

(6) $$\frac{dV}{d\alpha} = \frac{\cos \alpha}{D}$$

By measuring the vertical magnification and its directional derivative the visual system should therefore be able to compute α and D from equations (3) and (6).

But how could one tell whether the visual system makes use of these particular relationships? The answer comes from another experiment by Ogle, called the *induced effect*, which has puzzled psychophysicists for half a century. If one magnifies the right retinal image, not in the horizontal but in the vertical dimension, a fronto-parallel plane acquires a pronounced tilt in the *opposite* direction to that seen with a horizontally magnifying lens. Mayhew's explanation is essentially this: the visual system uses the vertical magnification and its directional derivative to compute the viewing paramters; but rather than presenting their values to consciousness it supplies them to a module which computes the distances of objects from the horizontal disparities between the retinal images. The simplest way in which this could be done is by direct substitution from (3) and (6) into (1), giving

$$(7) \qquad H = V + \frac{\tan\beta \cos\alpha}{D} = V + \frac{dV}{d\alpha}\tan\beta$$

The lens in front of the right eye produces an overall vertical magnification V but will not significantly alter the value of $dV/d\alpha$; so the apparent tilt induced by the lens will be given by

$$(8) \qquad \tan\beta = \frac{(H-V)}{\cos\alpha}\frac{D}{} = \frac{-V}{dV/d\alpha}$$

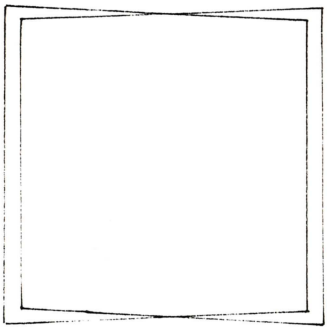
- an equation that adequately describes what is seen when V is not too large or $dV/d\alpha$ too small.

The induced effect is thus seen as a natural result of the visual system's performing a sensible computation on silly data.

Problem 1 Prove equation (1).

Problem 2 Figure 2 shows, superimposed, two halves of a stereogram intended for viewing at a distance of 20cm. How far away does the square seem to be? (You will need a ruler.)

Fig 2.



References

Longuet-Higgins, H.C., *The role of the vertical dimension in stereoscopic vision*. Perception 11 (1982) 377.

Mayhew, J.E., *The interpretation of stereo disparity information: the computation of surface orientation and depth*. Perception 11 (1982) 387.

Quote Quiz

Paul Taylor

This is a collection of some of my favorite quotations from past issues of *Eureka*, although they do not necessarily reflect my own opinions. Can you guess who wrote them and when, and about whom, what or when?

1
In order that the theory and practice may blend harmoniously it is essential that actual practice of one's occupation be combined with more abstract education and research. But is the achievement of this possible in the society in which we live? Except in the case of government or municiple service the means of employment are in the hands of private firms whose prime object is profit and who therefore tend to reduce education of their employees to the "practical" minimum (in the crude sense of the word) and consider only second the wider interests of their staff or society as a whole. It is impossible in a system of private profit for industry to develop its own universities. Only in the Soviet Union, where there is state planning of both education and industry, has the combination of theory and practice been possible,and there it seems to have been a success. How the system works in the Soviet Union is well worth studying.

2
It is plain at any rate that real mathematics (apart from the elements) has no *direct* utility in war. No one has yet found any war-like purpose to be served by the theory of numbers or relativity or quantum mechanics, and it seems very unlikely that anyone will do so for many years.

3
Eureka received some unexpected publicity at the British Student Congress at Leeds, when it was cited by a London student as a good example of cooperation between faculty societies in different universities.

4
Faculty News ... The meeting in the Easter term discussed printed lecture notes, but as the term ended abruptly it was difficult to follow up the recommendations. ... The Committee considered the suggestion of having a room in which informal discussions on mathematics could take place between and after lectures. As a result the Faculty Board have opened Room F in the Arts School.

5
The Archimedeans have had another successful year.

6
Whereas there were then only two other computers in the world, there are now about 100 computers in this contry alone, and well over 1000 in America. Ten years ago one authority thought there might never be a need for more than four or five large computers in this country!

7
It is difficult to avoid the conclusion that the applied mathematician will be the nearest approach to the *univeral man* that the future will be able to offer. It will be fairly easy for him to learn enough economics, anthropology, molecular biology, or any other subject to apply his techniques, whilst it will be very difficult for specialists in these subjects to work on others. The mathematician will be able to reverse the fragmentation of scientific effort, and to obtain results on the shadowy boundaries between disciplines. He may break down the barriers between the *Two Cultures*, and between pure science and technology.

8
University Teaching - a recent graduate's view ... First, non-comprehension of lectures. Every time a lecturer fails to make most of a class understand a topic a huge amount of supervision time is wasted; perhaps a hundred supervisors each cover the ground again, and invariably other problems are neglected. ... Second, unsuitable supervisors. Supervisors who quite cheerfully admit they know nothing whatsoever about the subject! Supervisors who *dont* admit this! Supervisors who never look at your work! Supervisors who set work not yet covered in lectures! Supervisors who sidetrack, and wont solve your problems!

9
The force is there, in the form of new ideas from the younger universities. But the Maths Faculty in Cambridge appears to be an immoveable object. ... The mistake made in the Cambridge maths course is to think that the teaching should be geared to the needs of those who will stay to do research. ... In June and July this year, art students up and down the country were demonstrating in no uncertain manner that they were not satisfied that their courses were appropriate to the work they would do subsequently. Mathematicians tend to be rather less excitable than artists, so there is little liklihood of a student 'sit-in' at the Arts School (the seats are too uncomfortable anyway!). What does seem likely is that before many years are out, no Maths students of any worth will be coming to Cambridge.

10
"Should lecturers distribute detailed summaries of their courses?" Dr. Reid, who had tried this last term, recalled an incident during his own undergraduate days when Dr. Taunt had distributed notes for a course of 9am lectures, and one drowsy student had fallen off a bench halfway through a lecture.

11
Number 1073 took a last look at the familiar outline of the city which, until a few hours ago, had been his home. It was called Camathica now - its original name, like his own, he had forgotten years ago. In fact, at this final hour of victory over The System he felt like going back and giving himself up to the dreaded Tripox police. His thoughts wandered to the future. Perhaps he might not be able to cope with the endless rantings of Agit Ramanjau Mistrat and the rest of the inner clique about the virtues of R and F (as the new super-efficient vocabulary had it). The notion quickly fled his mind. There was no bitterness in his heart towards The System. After all it was just a monolithic machine, self-perpetuating with no ultimate goal in mind except "perfection, perfection, perfection" as he use to hear so often.

Now, in the silence of the summer evening, 1073 tried to think what it was like before The System. He remembered the autumn of 19xx well when he had first arrived in Camathica. The people were docile and the elders of the city showed their appreciation of this. An atmosphere of benevolent despotism reigned and so the tide of revolt which had spread across neighbouring cities left Camathica untouched. Like all arrivals he received his copy of *Varsita*, and there on page 164 was what he was looking for. The small advertisement ran, "Socialist Mathematicians league - The group is in the process of formation...". Here was an opporunity to build up a moderate reforming movement, which would seek to fuse new ideas to ancient traditions. Unfortunately the movement died at its inception. The leaders claimed they had not been serious. All they wanted was a car. Little did they realise that they had missed the last chance to pull back from the brink of what was to follow. After that there was a blank in the memory of 1073; and then, the all-pervading voice of The System.

12
I came up to Oxford in 19xx as a mathematical scholar of Queen's. The city was vastly different from what it is now. Horse-drawn busses and trams provided the public transport. ... There was the old 'classical' algebra, with its theory of equations and congruences, some theory of numbers and determinants, but no matrices ... There was a fair range of pure geometry; it included geometrical conics and the geometry of triangles and circles ... Our calculus was in a state of flux. ... The applied mathematics was the conventional statics, hydrostatics and dynamics done without vectors - these we had heard of, I think, but the wearisome fight about notation had not yet resolved itself and I knew of noone who used them.

Answers on page 24, after the problems drive.

The Galton Laboratory
Department of Genetics and Biometry
UNIVERSITY COLLEGE LONDON
WOLFSON HOUSE
4 STEPHENSON WAY LONDON NW1 2HE

TELEPHONE 01-387 7050

14 august 1983

Dear Paul Taylor,

I apologize for being so long in replying to your letter. Somehow, there always seems to be a four amount to do - I have at the moment 3 PhD theses to read, one quite urgently because the author is due to return soon to China - one (previously unsolved) problem in mathematical genetics to deal with, because a colleague wants to use the answers at a conference in Los Angeles next week, some one else wants some genetical statistical advice next thursday, another PhD student wants to publish 2 papers quickly, because a job review, possibly seriously affecting future prospects - another student, of whom I am supervisor-once-removed, says he can't understand my 1981 paper on the estimation of correlations. It seems a little difficult to realise that (a) this is right in the middle of the vacation, when nothing happens, as everybody knows, and (b) I am supposed to be retired with nothing more useful to do except put up my feet and watch TV. Ha! ha!

I congratulate you on becoming Editor of *Eureka*. It may not be one of the world's best known journals, or have a multi million circulation, but surely it is one of the world's best, and I always look forward to the arrival of more.

I would hesitate a lot before offering too many suggestions. After all, it is now nearly 50 years since I first walked into Trinity as a Freshman.

The fact is, that it doesn't seem more than 3 years, and I don't feel any different – but as my hair has changed from black to white I certainly look different! And an awful lot has happened to mathematics in that time: with categories, and functors, and arrows, and spinors, and bifurcations, and decidability, and computability, and matroids, and two sorts of game theory, and nonstandard arithmetic, and heaven knows what else, it is hardly recognizable any more – and enormously exciting, but also enormously difficult to keep up with. So it is hardly for me to tell modern Cambridge students what to do.

However, I cannot resist expressing a few opinions, though it is certainly your privilege to throw them all into the waste paper basket.

When I visited Cambridge in 1982 (2002) I got the impression that the student societies rather depended too much on the older generation, for talks, articles, etc. It's true that I felt very honored and delighted to be asked to talk to the TMS, and I hope I had something to say that was worth saying – and no doubt the same goes for other academics who give talks. BUT, Cambridge is (or at least it should be) the best university in the world for mathematics (I will refrain from saying which is the best of the Cambridge colleges). And if so one would expect Cambridge students (and possibly also students from other universities) to have something to contribute. Sometimes I notice a lament by a Eureka editor that nobody has sent in any contributions.

Secondly, of course, the societies and Eureka should emphasize their raison d'être, maths is FUN. (In fact, they do.)

Thirdly, there is also a quite serious aspect to mathematics as well, some of which is only now becoming appreciated. When I was a student, almost all ($\equiv$ 95%?) of mathematical graduates became either schoolteachers or civil servants - a few became lecturers - but there were no other job openings. One day, a graduate announced that he had been offered a job in industry as a mathematician - this was a revolutionary proposal! Now, I fear, the position has changed - for too many graduates there will just be no job opening. But at least there is much greater appreciation that maths has a very great impact on the world. To take an instance involving possibly the most important issue of all - whether humanity survives. According to a USA Senate committee, each day on the average there are 5 warnings of a missile attack - and each warning has to be proved false within a few minutes, or else... If, for each warning, there is a small probability ϵ that it is not proved false (even though it is false), then there is approximately a probability 5ϵ that there will be a mistaken belief in a missile attack in 1 day, or $1 - \exp(-5\epsilon n)$ in n days. Somebody should point out to politicians, and those who guide our destinies, that even if ϵ is quite small, $1 - \exp(-5\epsilon n)$ tends to 1 as $n \to \infty$. (How you get this message wrong, I'm not quite sure).

In this connection, it might be worth while for the Archimedeans, or some other society, to invite Dr Paul Smoker, of the Politics Dept at Lancaster, to show how the arms race can be expressed by differential equations, or Dr Malcolm Dando, of the School of Peace Studies, University of Bradford, how the theory of hypergames can be used to model international (and other) relations.

Problems on a less grand scale also require mathematical modeling. The elimination of disease (and, hopefully, smallpox has been eliminated for ever) becomes possible only through the use of suitable models of disease transmission. The feeding of the world depends on models of population growth and species ecology. Maths has a part in some of the most essential issues facing the world today — and if Cambridge is the world's leading mathematical centre (or should be, at any rate), then students at Cambridge — and at other universities — should be aware of this.

Fourthly — and finally — Eureka shouldn't (in general) be looked on as a journal for publishing new results. There are more suitable journals. To this rule there may be very honorable exceptions: the Sprague-Grundy function G, which has revolutionized our ideas not only of games but also of numbers, made its appearance in a very modest little article in Eureka written by Michael Grundy. And Eureka could be proud of that.

It is up to you to decide whether any of this is helpful. Meanwhile congratulations, and best wishes for the future both to you and to Eureka

Yours sincerely
Cedric Smith

A point of contact between Mathematical Logic, Game Theory and Complexity Theory

Thomas Forster

This note has grown out of an observation in my commonplace book that if, in a game of chess, one of the players is looking more half-moves ahead than the other, then that person will probably win. Before embarking on the consequent discussion I shall rehearse some totally elementary machinery from the three areas mentioned in the title.

Suppose you and I sit down to play chess. We each have what one can call a *halfway-decent valuation function* or hdvf for short, which is a function (computable in polynomial time - they're not a great deal of use otherwise!) from positions of the board (considered as states of a machine) to some totally ordered set (which wlog is the integers) which takes a high value if the position is good for white and a low value if it is bad for white. (In fact, we will have to take hdvf's to be *pairs* of functions, since whether a position is good for you or not can sometimes depend crucially on whose move it is. One of the two functions in the pair assigns to each position its value to white if white is to move, the other assigns it its value to white if it is black to move.) A valuation is halfway decent only if the advice it gives you as to what is a good position and what isn't is advice that will make it more likely that you will win by following it than if you played a random move.

I shall assume that the reader knows (or would rather guess than be told) what I mean by the *depth-n minimax strategy*. It is what you are doing when you look n half-moves ahead, and choose your move on the assumption that your opponent will make the best possible reply to each move you make ... and so on out to n moves, where "best" means "puts you in a position with maximal hdvf value to her". Thus a depth n minimax strategy presupposes a hdvf to evaluate the position you look at those n half-moves ahead. Associated with the idea of a depth-n minimax strategy is the idea of the n-fold refinement of a hdvf. The refinement of a hdvf f is that function which assigns to each position A the sup (over all positions B accessible from A) of the infs of {f(C): C accessible from B} - or vice versa, *mutatis mutandis*.

There is a theorem in predicate logic that states that every sentence is logically equivalent to a formula in Prenex normal form (Prenex [5]). A formula in prenex normal form has all its quantifiers at the front, so that it consists of a string of quantifiers, the *prefix*, followed by a formula containing no quantifiers at all, the *matrix*. A formula is said to be $\forall^n$ if its prefix consists of n universal quantifiers, $\forall^*$ if it consists of nothing but (an unspecified number of) universal quantifiers, $\exists^*\forall^*$ if it consists of an unspecified number of existential quantifiers followed by an unspecified number of

universal quantifiers, and so on. The matrix is said to be in *conjunctive normal form* if it is a conjunction of a lot of formulae each of which is a disjunction of atomic formulae. Dually *disjunctive normal form*. Without loss of generality we may take it that the matrix is in conjunctive normal form. Because of Prenex's theorem we may similarly assume that any formula we meet is in prenex normal form.

In complexity theory we are interested in how difficult it is to compute answers to questions - how long it will take to get those answers. A function is *polynomial* or *computable in polynomial time* if the amount of time it takes to get the answer is a polynomial function of the size of the input. Similarly *exponential*. This classification is intimately connected with the number of quantifiers in the prefix of the formula describing the function concerned. Let us think of a *pass* as one scan of the universe, enabling us to examine each atomic sentence once. (An *atomic* sentence is what the word suggests - has no subformulae other than itself.) Thus each pass takes linear time (linear in the size of the universe). If we wish to verify $(\exists x)\Psi(x)$ we need one pass - look at each x as you pull it out of the hat to see whether or not $\Psi(x)$. To verify $(\exists x)(\forall y)\Psi(x,y)$ we need to make one pass (to check that $(\forall y)\Psi(x,y)$) for each x that we pull out, and so on up. This has the consequence that:

If Φ has n quantifiers when in prenex normal form, its truth value is computable in $O(k^n)$ steps, where k is the size of the universe.

A *first-order* variable is a variable taking as values objects *in* the structure under consideration. A *second-order* variable takes as values *substructures* of the structure under consideration. A thing of size n has 2^n subsets, and verifying a second-order property of a thing thus involves search through a barrel of subsets whose number increases exponentially with the size of the number you first thought of. Thus the difference between functions computable in polynomial time and those computable in exponential time corresponds to the difference between first-order and second-order functions.

There is a very good sense in which exponential-time functions are uncomputable, simply that the amount of computer time needed to crunch out values for any arguments other than very small ones rapidly exceeds the age of the universe in microseconds.

Why do we expect to win if we look more half-moves ahead than our opponents? (We mightn't, if the game is stacked sufficiently heavily in their favour.) One thing that is obviously important is that if I am looking n+2 moves ahead, and you are looking n moves ahead, *then I can predict your response to any move of mine and plan accordingly*. Of course this isn't strictly true, as your hdvf might fail to distinguish between certain moves and will thus give rise to a nondeterministic strategy, but I will ignore this in order to tell a good story. I shall consider what happens when, by having available the twofold refinement of the hdvf you are using, I know what your reply will be to any move I make.

I think what is involved here is not so much that my having information about your replies before you make them gives us a subgame that is more likely to contain a winning strategy for me (it may not) but rather that if there are any winning strategies for me they then become vastly easier to find.

The idea is that, normally, my search for a way of getting B from A, given that I alternate moves with you, is a problem that is exponential in the number of possible positions of the game. Why is this? Well, we can represent the game as a game played on states of a machine. I am trying to get the machine into any of a certain family of states, and you are trying to get it into certain others. Consider the two-place predicate "I can get from state A to state B in two moves whatever you do". This involves two quantifiers ("for any move of yours, I have a reply such that...") and will be quadratic in the number of positions. To say "I can get from A to B in four moves whatever you do" needs four quantifiers and correspondingly is a quartic problem, and so on. To say that I can get from A to B whatever you do, without putting a bound on the number of moves I might have to use, is a diagonalisation over all these quadratic, cubic, quartic, ... polynomial problems and so is exponential.

It is quite plausible that in general the problem of finding the best move at some position in a game is exponential. If we think of games as finite trees with endpoints labelled "win for you" or "win for me" *and nothing else* then clearly the problem of finding a winning strategy *in general* is exponential. Indeed by "solving" a game we normally understand a process of understanding it so well that we find a polynomial algorithm for finding the best move at a given position, typically by finding a structure-preserving map of some kind onto an easier object (in chess the object would be the set of possible board positions) which we can describe more simply. It is only if you understand the game in this sense that you can do better than just enumerate all strategies by brute force and try them all out, which is of course an exponential task!

In order to avoid proving a version of this claim that does justice to "in general" I shall discuss a natural game which, because of its deep connection with the liar paradox, cannot be polynomially solvable. The game in question is used by logicians for characterising logical validity.

We shall start by defining what it is for a formula to be *true* in a model. We begin by defining a satisfaction relation between Gödel numbers of formulae and partial assignment functions. Assignment functions are functions from variables (or, rather, to make things easier, and because we have countably many variables, called $x_1 \ldots x_n \ldots$ we may think of a partial assignment function as being a map from a set of integers, being the subscripts of the variables you are interpreting) into the model you have in mind. Assignment functions *assign* objects in the model to variables in the language. A sentence will then be *true* in a model if it is satisfied by every partial assignment function. "is satisfed" in the last sentence will be abbreviated to "sat" which we

must now define. The obvious way to start is

f sat '$x_i \in x_j$' iff$_{df}$ f(i) $\in$ f(j) and

f sat '$x_i = x_j$' iff$_{df}$ f(i) = f(j)

(and similarly for other atomic formulae, whatever they may be) If i or j are not in the domain of f then vacuously f *sat* '$x_i \in x_j$' and f *sat* '$x_i = x_j$'

It is a good habit to put quotation marks round the formula to remind us that the satisfaction relation is really being defined between partial assignment functions and the *names* of formulae (namely their Gödel numbers) rather than the formulae themselves.

Classically (Tarski [4]) *sat* is then defined to be the least relation containing all such initial pairs $\langle f, 'x_i \in x_j' \rangle$ and $\langle f, 'x_i = x_j' \rangle$ as above which is closed under the additional operations:

(i) If f *sat* 'Φ' and f *sat* 'Ψ' then f *sat* 'Φ & Ψ'
and similarly for the other sentential connectives

(ii) If i is not in the domain of f, and for all g such that Dom g = Dom f $\cup$ {i} we have g sat '$\Phi(x_i,\ldots)$' then f sat '$(\forall x_i)(\Phi(x_i,\ldots))$'

and dually for the existential quantifier.

Finally, we say Φ is *true* iff$_{df}$ $(\forall f)$(f *sat* 'Φ')

This "$\forall f$" is a second-order quantifier, and Tarski proved that there is no way of getting rid of it. If "...is true" were first order, then with a little ingenuity we could reconstruct the Liar paradox by formulating a sentence that says of itself that it is false. But there is a more delicate result available which a different approach will reveal. If we restrict the definition of a satisfaction function to formulae of bounded complexity, we can get rid of the second order quantifier. This was first done in Levy [3]. The presentation here derives not from Levy's, though, but rather from Hintikka [2] and Aczel [1] where first I met it.

We can arrive at a different way of defining truth of a sentence in a model if we consider how to resolve a disagreement between you and me about whether a given sentence Φ is true in a model. Suppose I say it is false, you say it is true. What do we do? Well, *I challenge you to show it true.* If it starts with a block of universal quantifers $(\forall x_1 \ldots x_n)$ you are claiming that whatever n-tuple $x_1 \ldots x_n$ I challenge you with you can do some given thing. So I pick an n-tuple $x_1 \ldots x_n$, preferably the one that will give you the most difficulty. If the next block of quantifiers is $\exists y_1 \ldots y_n$ then you must be given a chance to exhibit an n-tuple $y_1 \ldots y_n$ (an n-tuple of "witnesses") that do whatever it is - it would not be fair for me to choose on this occasion too, as I could choose some that were not witnesses. If we are looking at something of the form A & B then you must be able to make them *both* true, so it would be my turn to pick a conjunct (whichever one I think will be more difficult for you). For A v B to be true it is sufficient for one of A, B to be true so it is your turn to choose one. When we reach an atomic sentence the game ends. I have won if it is false, and you have won if it is true. If I have a *winning strategy* in this game then clearly Φ was false, and if you have a winning

strategy then it must be true. A formal description of this game will give us a truth-definition.

The game is played by two players, called *False* and *True*. It will be played on a formula Φ, which we will assume for present purposes to be in prenex normal form, that is to say, all its quantifiers have been pulled to the front, and the matrix (stuff inside the quantifiers) is in conjunctive or disjunctive normal form: this has the consequence that '~' appears in Φ, if at all, only in negatomic sentences. The rules are as follows:

If Φ is of the form $(\forall x_i \ldots x_j)(\Psi(x_i))$ then player *False* picks an n-tuple of objects y,...w and adds the pairs $\langle i,y\rangle \ldots\ldots \langle j,z\rangle$ to a partial assignment function that *False* and *True* are building.

If Φ is of the form $(\exists x_i \ldots x_j)(\Psi(x_i))$ then player *True* picks an n-tuple of objects y,... z and adds the pairs $\langle i,y\rangle$, $\langle j,z\rangle$ to the partial assignment function that *False* and *True* are building.

In either case they strip off the quantifiers and look at what is inside and start again.

If the principal connective of what they are then looking at is '&', then *False* picks one of the conjuncts (and adds nothing to the partial assignment function). If the principal connective is 'v' the *True* picks one of the disjuncts (and adds no ordered pair, as above). They continue in this fashion until an atomic sentence Ψ is reached, when the game ends. On the way, *False* and *True* have built a partial assignment function f. The final rule is this: *True* has won if f *sat* Ψ, otherwise *False* has won. We call this game the *game over* Φ.

Since this is a game of perfect information and every play is of finite length there must be a winning strategy. And if we know how deep the quantifiers and connectives in Φ are nested we can state in a first-order way precisely what it is for *False* or *True* to have a winning strategy. It will be something like "For every move of *False* there is a move of *True* such that..... f *sat* Ψ" How many moves are made and in which order the players play will depend on the structure of the Φ with which we start. So it is only for classes of formulae which all have the same structure that we can say in a first-order way what it is for one of the players to have a winning strategy. For example we can write down a formula that says "*True* has a winning strategy in the game over Φ where Φ is a (say) $\forall^*\exists^*$ formula whose matrix is in conjunctive normal form" *with* Φ *free*. Quite how many more quantifiers this formula will have will depend on such local details as how we define ordered n-tuples (we might have taken them as primitive for example) but we have shown that truth-definitions for formulae with *bounded* numbers of quantifiers can be had, and if necessary we can always use a liar paradox argument to show that a truth definition for a class of formulae Γ does not belong to Γ.

Of course, this is not a proof that the problem of finding a winning strategy in a finite game is exponential, but merely a good reason for us to expect it to be.

However, if I know in advance what your reply will be to any move of mine then my search for a winning strategy is much simpler. I now look at the set Q of all states of the machine, and consider the two-place predicate (let's call it R) we started with above. "I can get from A to B in two moves whatever you do". This predicate is computable in linear (one quantifier - "I have a move to which your reply is..") time from the information that my depth n+2 minimax strategy gives me, instead of being quadratic. $\langle Q,R \rangle$ is now a directed graph, and my search for a winning strategy reduces to finding a path in this graph from where I am to one of the won positions. This problem is quadratic in the number (m, say) of states of the game. For suppose I am at position A and I wish to get to position B. Let $A_0 = \{A\}$ and let A_k be the set of positions I can get to in k moves but not in k-1. At stage k I make one pass for each object in A_{k+1} to find all things in A_k, and I keep doing this till I find B. Each pass costs me m, and I might have to make as many passes as there are objects in $\cup_{k<m}(A_k)$, namely m. Total cost bounded by m^2.

Incidentally none of this depends on my using a valuation function that is halfway decent, but only on my being able to predict your moves.

[1] Aczel P. Inductive definitions and monotone Quantifiers. *Proc 3rd Scandinavian Logic Symposium*. North Holland 1975

[2] Hintikka J *Logic, Language Games and Information* O.U.P., Clarendon Press 1973

[3] Levy A. A Hierarchy of formulas in set theory *Memoirs Am. Maths. Soc.* **57** (1965)

[4] Tarski A The concept of truth in formalised languages translation *in* Woodger (Ed) *Logic, Semantics & Metamathematics* O.U.P 1956

[5] Prenex E Normalformen im Logische Predikatenkalcull *Acta Math. Acad. Kosoviensis* **53** (1905)

The Society

Mike Newman

The Archimedeans are now two thirds of the way through what looks like being a fairly successful year. As usual Easter term had only social events: a croquet afternoon playing against the Faculty, a punt joust against the Dampers, a ramble and picnic and a punt trip to Grantchester. We also held a brief Extraordinary General Meeting at which small, but important, changes were made to our constitution.

Michaelmas term started with a very successful recruitment drive, and a rather less than successful lunch-time meeting at which the speaker, from Acorn Computers, failed to turn up. Disaster was averted when our publicity manager, Eddy Welbourne, stepped into the breach to speak at five minutes' notice. Our other speaker meetings have been, Dr. Neumann "*The Rational World and the Real World*", Professor Rogers "*Geometry Weird and Wonderful*", Professor Sir Michael Atiyah "*Newton Polygons and the theorem of Archimedes*", Professor Schwarzenberger "*The Psychology of Learning Mathematics - Can it Help?*" and at lunch-times Dr. Whiteside "*A Pre-Elliptical Egghead: Kepler and his 'Alternative Circular Orbit for Mars'*", Richard Pennington (a graduate student) "*An Afternoon's Anthropological Amble in the Archimedean Archipelago*", Bob Dowling (an undergraduate) "*Magic Squares*" and Eddy Welbourne (another undergraduate) "*The Dynamic Topology of a Ring of Death*". Other events included a puzzle-hunt, a careers evening with speakers on operational research, actuarial work and meteorology and a Mathematical Call my Bluff with visitors from Oxford and the University of Runcorn Contemporary Dance Society, a film evening showing "*Turning a Sphere inside out*" and "*Space-filling curves*", a Christmas party, a trip to play silly games in Oxford against the Invariants and a visit to the Computer Laboratory.

Lent term should see many more exciting events including a celebration of our fiftieth anniversary in the form of the Triennial Dinner. I look forward to seeing you there.

Problems Drive 1984

Andy Bernoff and Richard Pennington

(Answers on page 50, inside the back cover.)

1 The numbers 1 and 36 have the property that they are both square and triangular, ie they may be expressed as either m^2 or as $n(n+1)/2$ where m and n are integers. What are the next two such numbers?

2 The Archimedeans committee consists entirely of mathematicians (*this is a lie -Ed.*), and may thus be divided into *Pure* and *Applied* mathematicians, or alternatively into *Sane* and *Insane* mathematicians. Pure mathematicians always tell the truth about their beliefs, while Applied mathematicians invariably lie about their beliefs. The beliefs of Sane mathematicians are correct, while those of Insane mathematicians are incorrect.

The following conversation is overheard among three committee members:

A: "B is sane"
B: "C is pure"
C: "A is sane"
A: "B is applied"
B: "A is insane"
C: "B is pure"

Classify the three committee members as Pure or Applied and as Sane or Insane.

3 Calculate $\prod_{2}^{\infty} \cos \pi/2^k$

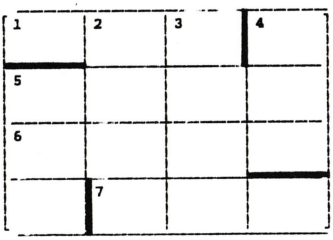
4 For which of the five Platonic solids (tetrahedron, cube, octahedron, dodecahedron and icosahedron) is it possible to assign a number to each face so that, although the numbers assigned are not identical, the sums of the numbers assigned to the faces meeting at each vertex are the same?

5 A rectangular box of noughts is entirely surrounded by a single layer (including corners) of crosses, as in the diagram:

```
XXXXX
XOOOX
XOOOX
XXXXX
```

What are the possible shapes and sizes of the block of noughts if there are the same number of noughts as crosses?

6 Solve the following cross-number; m, n, p, q, r and s are integers and no number begins with a zero.



Across: (1) n^2 (5) s^3 (6) r^3 (7) $q(q+1)/2$
Down: (2) n^3+n (3) m^3+m (4) s^2 (5) p^2

7 In the market at Archimedea several kinds of fruit are on sale at a strictly positive integral number of qarches per fruit (the currency is 100 qarches to 1 eureka). The three people ahead of me in the queue make the following transactions:

oranges	apples	plums	bananas	tangerines	cost
2	2	2	5	3	66q
2	2	2	2	2	48q
5	0	0	9	5	£1

How much should I expect to pay for 12 oranges?

8 The differential equation

$$\frac{d^2y}{dx^2} + x\frac{dy}{dx} + \frac{y}{2} = 0$$

has two linearly independent solutions which may be referred to as A(x) and B(x). Find two linearly independent solutions of

$$\frac{d^2y}{dx^2} + x\frac{dy}{dx} + 1000001\,\frac{y}{2} = 0$$

9 What are the next three terms in each of the following series, and why?

(a) 6, 15, 35, 77, 143, 221
(b) 1, 18, 3, 8, 9, 13
(c) 1, 4, 12, 22, 34, 51

10 The ferries linking the five cities on the shores of the perfectly circular Lake Bathwater all travel in straight lines at a constant speed of 1000 Archimedean cubits per minute. Cauchyville is nearer to Archimedea than Demoivreton is to Archimedea. The ferry from Archimedea to Besselopolis takes 40 minutes. Cauchyville and Demoiveton are each equidistant from Archimedea and Besselopolis. The ferry routes from Cauchyville to Demoivreton and from Archimedea to Eulerberg cross at a point 20000 cubits from Cauchyville and 25000 cubits from Archimedea.

What is the radius of Lake Bathwater and when does the ferry which leaves Archimedea at midday arrive at Eulerberg?

11 Find all ordered pairs of integers (a,b) such that $0 < a < b < 100$ and $0.704 < a/b < 0.705$.

12 An Archimedean anthropologist on a remote island wishes to discover who is the tallest of the natives in the surrounding area. According to a quaint but strictly enforced local custom, he may meet the locals only two at a time. How many comparisons must he make in order to discover which of the 157 natives is the tallest, assuming that he works in such a way as to require as few comparisons as possible? No two of the natives are the same height.

Answers To The Quote Quiz

1 1.6 (Jan 39) by E.T.E., unaware of the Stalinist purges.
2 3.6 (Jan 40) by G.H. Hardy, who must now be turning rapidly in his grave. There's worse later in the same article.
3 4.8 (May 40) by D.J.H. *Eureka* was at that time edited jointly by Cambridge and London students.
4 5.9 (Jan 41) by H.A.E., but this could be any Liaison Committee report.
5 Likewise this is the generic Secretary's report.
6 22.9 (Oct 59) by Martin Fieldhouse.
7 29.3 (Oct 66) Colin Myerscough's editorial.
8 30.3 (Oct 67) and again.
9 31.3 (Oct 68) J.J. Barrett's editorial.
10 31.20 (Oct 68) Report of an "Any Questions" by Peter Johnstone.
11 35.1 (Oct 72) Joseph Conlon's editorial. 19xx=1970.
12 36.11 (Oct 73) W.L. Ferrar on life in 19xx=1912.
[nn.mm is Eureka **nn**, *page* mm; *general apologies to these authors for reminding them of their sometimes rather silly predictions!]*

The Mathematical Association

Rolph Schwarzenberger

The *Mathematical Association* was founded in 1871 as the *Association for the Improvement of Geometrical Teaching* and adopted its present title in 1897. It was the first subject teaching association to be founded in this country and its membership continues to consist mainly of those engaged in the teaching of mathematics at all levels from primary schools to universities.

The Association publishes three journals, the *Mathematical Gazette* (the most erudite - chiefly read by teachers in secondary schools and in colleges and univeristies), *Mathematics in School*, and *Mathematics Round the Country*. Two new journals, aimed at pupils rather than teachers, are planned.

The Association is responsible for the validation of three Diploma courses: *Mathematical Education* (for teachers of pupils in the age range 5-13), *Low Attainers* and *Heads of Department*. It organises regular weekend conferences and issues regular reports, booklists and posters. Members have the opportunity to participate in these activities through a system of local branches, through committees and working parties set up to consider particular issues, through committees running particular events (such as the national mathematical competitions and International Mathematical Olympiad) and through the annual conference at Easter.

Full details of these activities and of current subscription rates (which depend on the journals received) may be obtained from the Executive Secretary at the Association's headquarters, 259 London Road, Leicester, LE2 3BE, (0533) 703877, or though the Archimedeans. There are reduced rates for students.

The Cambridge branch of the Mathematical Association meets about three times a term at the Cambridge Institute of Education in Shaftesbury Avenue. Members of this branch may attend the meetings of the Archimedeans and the College Societies for free, and members of the Archimedeans may attend branch meetings for free.

The 1985 Conference will be held in the University of Dundee from 10 to 13 April. The 1986 Conference will be held in Cambridge, with Hilary Shuard of Homerton College as President. It is hoped to have the active co-operation of the Archimedeans and the Faculty of Mathematics; arrangements for members of the Archimedeans to attend at a nominal charge are under discussion. -Ed.

As Any Brontosaurus could tell you, It's not a Paradox

Eddy Welbourne

The following article concerns a problem thrown at the Adams Society by Dr. Körner [3]. Given any suitably diverse and general collection of data - such as the heights in feet of the hundred highest peaks in Europe, the heights in metres of the fifty tallest mountains in Peru and the populations of the sevety-eight largest cities in Asia - the distribution of the first digits is not uniform but has $f_i=\log_{10}((1+i)/i)$, roughly: this suggests an underlying $1/x$ probability distribution. However $1/x$ is not normalisable, since its integral to infinity (or from zero) is infinite.

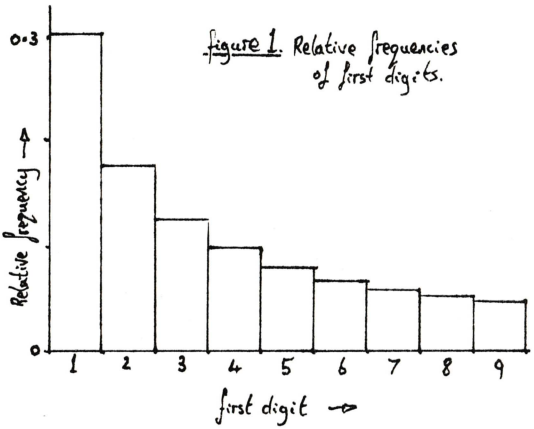


figure 1. Relative frequencies of first digits.

Now, the fact that the first digits distribution takes on this form does not surprise me, or indeed most people who have used a slide rule or logarithm tables: a rather pleasing illustration of roughly the same phenomenon may be found in the English langauge, as Paul Taylor pointed out to me. The language is irregular for much-used words rather than little-used words, and the numbers are somewhat irregular up to twenty, but follow a regular pattern thereafter: we use smaller numbers much more frequently, so that the numbers eleven to nineteen have their own names, rather than ten-and-one, etc., as one might expect from the pattern after twenty.

The problem is not so much that we should expect the distribution to be roughly uniform as that the observed distribution suggests an impossible underlying distribution. I shall, indeed, show that the problem is not so much that the thing is sloped as the way in which it slopes. I shall also endeavour to persuade you that the problem is no problem at all. On the occasion of Dr. Körner's talk, once the meeting

had been declared *trivial*, we had a merry time trying to convince ourselves that, provided the underlying distribution is sufficiently spread out - by which we meant that the 'hump' of the distribution should cover an entire order of magnitude - the observed result will hold. What we *in fact* showed was that, given physically reasonable assumptions, the observed result would hold. What is *needed* is to show that ordinary probability functions admissible to the probability theorists can posess the desired physically plausible properties. Dr. Körner's objection is not that it is perverse of the universe to produce the observed result, but that probability theory is unable to cope with it.

Throughout what follows we must concern ourselves with probability density functions on the positive real line which, in order to describe the sorts of data we are concerned with, rise to a broad peak and then die off. Despite some claims that such a distribtuion is, in fact, the visible portion of a brontosaurus [4], I contend that what we actually see is a boa constrictor which has just eaten an elephant [2]. Although what we see is indeed *thin at one end, much much thicker in the middle and then thin again at the far end* [1], we would have the legs of the brontosaurus in the visible portion and these are not observed.

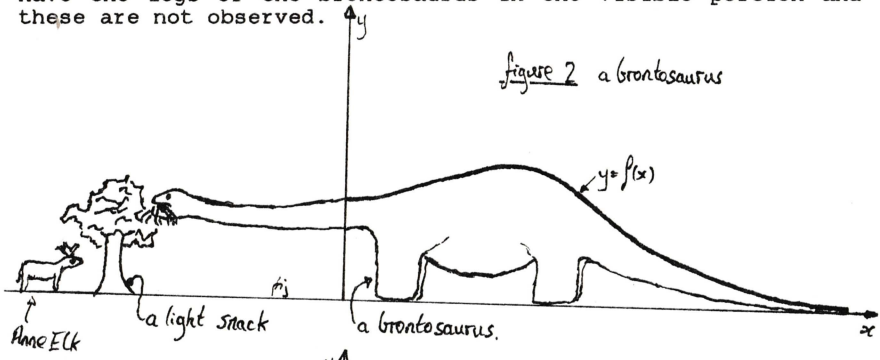


figure 2 a brontosaurus

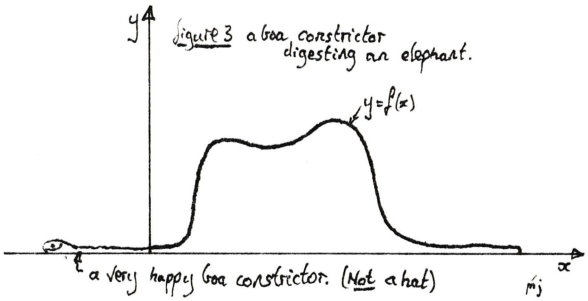


figure 3 a boa constrictor digesting an elephant.

As you can see, the second picture is much nearer the desired form, though the boa may need to crawl to the left a little. Boa constrictors dont have legs, and you cant see the elephant's legs because the elephant is inside the boa.

Given a probability density function, f, we define the probabilities of the various first digits as

$$p_i = \sum_{n=-\infty}^{\infty} \int_{ib^n}^{(i+1)b^n} f(x)\,dx$$

where we are now working base b, and i is any of $1,2,\ldots,b-1$. Note that this sum is necessarily absolutely convergent, for smooth f, because of the properties of probability density functions, and that

$$\sum_{i=1}^{b-1} p_i = 1$$

An important ingredient in what we are considering is scale invariance: our units of measurement being arbitrary, we imagine that a change in our units, i.e. a change of scale, will not affect the values of the p_i. As it turns out, this is a rather weak condition, but it does give the following: given $\alpha,\beta,\gamma,\delta \geq 0$, not all zero, with $\alpha+\beta \geq \delta$, put $\sigma = 6\alpha+6\beta+4\gamma+\delta$, then

$$p_9 = \frac{\delta}{\sigma},\ p_8 = \frac{\gamma}{\sigma},\ p_7 = \frac{\beta}{\sigma},\ p_6 = \frac{\alpha}{\sigma},\ p_5 = p_6+p_7-p_9,$$

$$p_4 = p_8+p_9,\ p_3 = p_6+p_7,\ p_2 = p_6+p_7+p_8,\ p_1 = p_2+p_3$$

provides a set of values consistent with the weak scale-invariance. In this case

$$p_1 = \frac{2\alpha+2\beta+\gamma}{6\alpha+6\beta+4\gamma+\delta} = \frac{1}{3}\left[1 - \frac{\gamma+\delta}{\sigma}\right] = \frac{1}{4}\left[1 + \frac{(\alpha+\beta-\delta)+\alpha+\beta}{\sigma}\right]$$

from which we see, using $\alpha+\beta-\delta \geq 0$, that p_1 necessarily lies between 1/4 and 1/3, each of which may be attained.

However, consider the definition of the p_i. Given the absolute convergence of the sum and the nice behaviour of the integral, we have

$$p_i = \sum_{n=-\infty}^{\infty} \int_{ib^n}^{(i+1)b^n} f(x)\,dx \qquad (\text{put } b^n u = x)$$

$$= \sum_{n=-\infty}^{\infty} \int_{i}^{i+1} b^n f(b^n u)\,du$$

$$= \int_{i}^{i+1} \left[\sum_{n=-\infty}^{\infty} b^n f(b^n x)\right] dx$$

which suggests that we think in terms of the probability density of the "signficant part" of the data when expressed as a number in $[1,b)$ multiplied by b^n for some $n \in \mathbb{Z}$;

$$\Phi(x) = \sum_{n=-\infty}^{\infty} b^n f(b^n x) \qquad \text{for } x \in [1,b)$$

Given this, we have a new and more powerful interpretation of scale invariance, namely that Φ be unchanged under change of scale in our data. This renders

$$\Phi(x)dx = \Phi(u)du \qquad \text{for any change of scale } u=\alpha x$$

so $\Phi(x) = \alpha\Phi(\alpha x)$ for any x,α with $x,\ \alpha x \in [1,b)$

but this gives $\Phi(x) = k/x$ for some k, and considering

$$\int_1^b \Phi(x)dx = 1$$

we obtain

$$k = \frac{1}{\log b}, \qquad p_i = \log_b \left[\frac{i+1}{i}\right]$$

So we now see what Dr. Körner was arguing: the underlying distribution, Φ, is indeed $1/x$: however this does not require f to be $1/x$. As a trivial example, if f were $1/(x \log b)$ on $[1,b)$ and zero elsewhere, we would have this scale invariance. However we may reasonably demand scale invariance relative to any base b', provided b' is not too large, and it then *looks* very much as though we are constrained to a $1/x$ density function in this case. However, I shall seek to persuade you that in fact *any* suitably spread-out density function f will render Φ in approximately the from described.

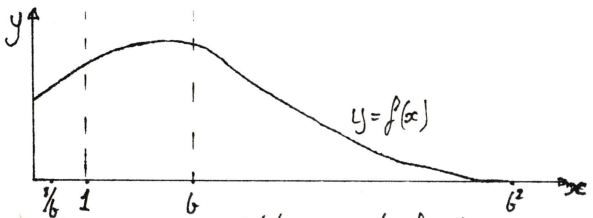


figure 4. Aprobability Density function

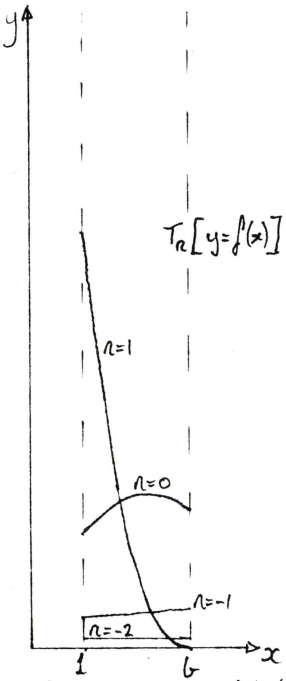


figure 5 The stretched curves

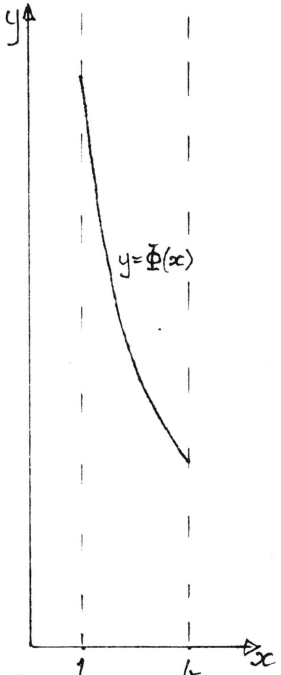


figure 6 Φ, the derived function

The graph $y=b^n f(b^n x)$ is obtained from $y=f(x)$ by the linear transformation

$$T_n = \begin{bmatrix} b^{-n} & 0 \\ 0 & b^n \end{bmatrix}$$

This preserves areas, as we would hope, and increases gradients by b^{2n}. To obtain Φ from f, we take the images of the graph $y=f(x)$ under $\{T_n : n \in \mathbb{Z}\}$ and sum the results on $[1,b)$.

Now as T_n enlarges vertically for $n>0$, ie for $[b,b^2)$, $[b^2,b^3)$, etc., the images of the downwards-sloping portion of $y=f(x)$ are given much more weight in fig. 5 that those of the upwards sloping portions with smaller (in this case negative) n. Thus the final curve, $y=\Phi(x)$, is necessarily downwards-sloping.

Furthermore,

$$b\,\Phi(b) = b \sum_{n=-\infty}^{\infty} b^n f(b\,b^n) = \sum_{n=-\infty}^{\infty} b^{n+1} f(b^{n+1}) = \sum_{r=-\infty}^{\infty} b^r f(b^r) = \Phi(1)$$

so the end-points of our curve lie on a common curve of constant xy. Moreover this result does not depend on the shape of f.

Also, just as T_n increases gradients by b^{2n}, it also increases k^{th} derivatives by b^{k+1}, so we obtain, for boa-shaped curves (having $f^{(k)}(x) \to 0$ from below for k odd, above for k even, as $x \to \infty$), the result that Φ, resembling most directly the right-hand tail of f, has positive even derivatives and negative odd ones, just as $y=1/x$ has.

Although this does not prove that Φ is necessarily close to $1/x$ in shape, I hope you will agree that it looks suspiciously as though it will be tolerably close.

So be warned: just because something looks nasty it doesn't mean it is: what looked at first sight like an incompatibility betwen theory and observation has turned out to be true in general within the theory.

[1] *About Brontosauruses* Miss A. Elk, MPPR (Oct 1972) **A**(2)

[2] *Le Petit Prince* A. de Sainte-Exupéry, Piccolo, 1943, ch.1

[3] *Is Anything Random?* T. W. Körner, 25th October 1983

[4] *Derek the Differentiable Dinosaur* I. Harrison & W. Breckon, 2-Manifold Publications, University of Warwick, 1981.

The Riemann Hypothesis

Mark Coleman

1. Introduction.

In this article I wish to examine a few of the ways in which the so-called Riemann Hypothesis (RH) influences questions about the distribution of primes.

In his memoir of 1859, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* (for an English translation see [1]) B. Riemann showed that the key to investigating the distribution of primes lay in the study of the zeta function.

This is defined for $\sigma>1$ by the Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad [\sigma = Re(s) - Ed.] \tag{1}$$

It has an analytic continuation to the whole complex plane with a simple pole at $s=1$ with residue 1. It is known that $\zeta(s)$ has zeroes at $s = -2,-4,-6,\ldots$, the *trivial zeroes*. We define the *critical strip* to be those $s=\sigma+it$ such that $0\le\sigma\le1$. $\zeta(s)$ has infinitely many zeroes in this strip, symmetric about the real axis.

The importance of $\zeta(s)$ was illustrated by Hadamard and de La Vallée Poussin in 1896 when they proved the *Prime Number Theorem* (PNTh^m).

Let $\pi(x)$ be the number of primes $\le x$. Then the PNTh^m states that

$$\pi(x) \sim x/\log x.$$

And in fact a better approximation to $\pi(x)$ is given by

$$li(x) = \int_2^x \frac{dt}{\log t}$$

This result had been conjectured by Guass from numerical evidence as early as 1793. But the proof by Hadamard and De La Vallée Poussin showed that the PNTh^m is implied by (and actually implies) "$\zeta(s)$ has no zeroes on the line Re $s=1$."
It is easy to see by integration by parts that

$$li(x) \sim x/\log x .$$

So the PNTh^m states

$$\pi(x) = li(x) + o(x/\log x).$$

If we demand that $\zeta(s)$ have no zeroes on Re $s=1$ and also none in a region to the left of this line, we find we can improve the error term $o(x/\log x)$. Yet the best *zero-free* regions we have found are of the form $\{s = \sigma+it : \sigma > 1-\eta(t)\}$, where $\eta(t)\to0$ as $t\to\infty$. It has not been shown that there exists any $\delta>0$ such that there are no zeroes $\rho=\beta+it$ with $\beta>1-\delta$.

Yet the remarkable conjecture of Riemann, which is the only one in his memoire that has not yet been proven, is the...

Riemann Hypothesis: all the zeroes of the Riemann ζ-function lie on the line Re $s = 1/2$, except the trivial ones.

That is, we should be allowed to take $\theta = 1/2$ above.

The implication for the PNThm is that

$$\pi(x) = x + O(\sqrt{x} \log x)$$

But though the RH says all there is to say about the real parts of the non-trivial zeroes, it leaves questions unanswered about the distribution of their imaginary parts.

There is, however, a further conjecture, due to Montgomery, which, with the RH, gives more information about the vertical distribution. Unfortunately, this is too technical to state here.

However, with a form of this conjecture and the RH, Heath-Brown has shown

$$\pi(x) = x + o(\sqrt{x} \log x).$$

So even if the RH were proven, there would remain further questions about the distribution of primes.

2. Generalisation

Let q be a given positive integer, not 1.

A function χ (of an integral variable) is called a *character* (mod q) if it has the following three properties:

(i) $\chi(n) = 0$ iff $(n,q)>1$

(ii) $\chi(n+q) = \chi(n)$

(iii) $\chi(mn) = \chi(m)\chi(n)$

(where (n,q) stands for the highest common factor). The character

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n,q)=1 \\ 0 & \text{otherwise} \end{cases}$$

is called the *principal character*.

It can be shown that the number of characters is equal to $\phi(n)$, the number of integers $0<m<n$ with $(m,n)=1$.

Using these we define the *Dirichlet L-series*,

$$L(s,\chi) = \sum_1^\infty \frac{\chi(n)}{n^s} \qquad \sigma>1$$

These share many properties with the ζ-function. They all have an analytic continuation to the complex plane. But the $L(s,\chi)$ with $\chi \neq \chi_0$ have no poles whereas $L(s,\chi_0) = \zeta(s)\prod_{p|q}(1-p^{-s})$ has a pole at $s=1$. They also have infinitely many zeroes $\rho=\beta+i\tau$ with $0\leq\beta\leq1$, i.e. they have the same critical strip. Yet the corresponding questions of their distribution are much harder. Still we can make a similar conjecture to that of Riemann.

Generalised Riemann Hypothesis (GRH): for all L-functions, for all moduli q, the zeroes that lie in the critical strip actually lie on the line $\sigma=1/2$.

The Dirichlet L-series are fundamental to questions about the distribution of primes in arithmetic progression.

Consider the arithmetic sequence $a, a+q, a+2q, \ldots$, where $(a,q)=1$. Define $\pi(x;a,q)$ as the number of primes $p \leq x$ which lie in this sequence. Similar to the ζ-function above we can show that none of the $L(s,\chi)$, χ defined mod q, have zeroes on Re $s=1$. This implies that

(2) $$\pi(x,a,q) \sim li(x)/\phi(q).$$

We see that the right hand side of this $\to\infty$ as $x\to\infty$. Thus we get *Dirichlet's Theorem*, that there are infinitely many primes in the arithmetic progression $a, a+q, a+2q, \ldots$, where $(a,q)=1$.

As before we can estimate the error in (2) and see how it relates to zero-free regions of the *L-functions*. Unfortunately our knowledge of these regions is nowhere as good as that for $\zeta(s)$. This leads to complicated expressions for the error term, yet with GRH we get

$$\pi(x,a,q)=li(x)/\phi(q)+O(\sqrt{x}.\log x) \quad \text{for } q\leq x.$$

But if we are interested in $x\leq\sqrt{q}$, given that $\phi(x)>x/\log\log x$ for large x, we see that the error term is greater than the main term in this case. So not even an assumption as strong as the GRH will answer all our questions in this area.

3 DIFFERENCE BETWEEN PRIMES.

Above we saw how the R.H and G.R.H influenced *global* questions of the primes, i.e their distribution in the Natural Numbers. Here we are interested in *local* questions, primarily the distance between consecutive primes.

Let p_n be the nth prime and $d_n = p_{n+1}-p_n$.

The *Twin Prime Conjecture* states that $d_n = 2$ for infinitely many n. But we are interested in the order of magnitude of d_n.

Cramer has shown that on R.H

$$d_n = O((p_n)^{1/2} \log p_n).$$

And, with a form of Montgomery's conjecture,

$$d_n = O((p_n \log p_n)^{1/2}).$$

The best unconditional result to date is

$$d_n = O((p_n)^{1/2+1/21}).$$

This problem is intimately connected with that of how small we can take $\eta>0$, such that the interval

(3) $$[x, x+x^{\eta}]$$

contains a prime for all sufficiently large x, i.e $x>x_0$, say.

Cramer's result above shows that on R.H we have a prime in the interval $[x, x+Cx^{1/2}\log x]$, for all x, where C is a large absolute

constant.

But this problem has a number of approximations not available to the first interpretation.

Firstly, instead of looking for a prime in the interval, we could look for a number with at most two prime factors, denoted by P_2. In this case we can take $\eta = 0.455$.

Secondly, instead of the condition "for all $x>x_0$", we consider the result for "almost all" intervals, i.e. the Lebesgue measure of the set of $x<x_1$ such that the interval (3) contains no prime, is $o(x_1)$ as $x_1 \to \infty$.

In this case, Selberg has shown on RH, that "almost all" intervals $[x, x+f(x)(\log x)^2]$ contain a prime if $f(x) \to \infty$.

The best unconditional result, due to Harman, is $\eta = 1/10 + \varepsilon$ for any $\varepsilon > 0$.

We can combine these two approximations to prove that, if $\delta > 0$ is given, then "almost all" intervals of the form $[x, x+(\log x)^{7+\delta}]$ contain a P_2 number.

Returning to questions about d_n, we define

$$E = \lim \inf_{n \to \infty} (p_{n+1} - p_n)/\log p_n.$$

The PNTh^m implies $E<1$.
Hardy and Littlewood, using their Circle Method and the assumption of GRH, showed that $E<2/3$.
If the Twin Prime Conjecture were true then obviously $E=0$.
This has not been achieved on RH alone, yet Heath-Brown has shown $E=0$ using a form of Montgomery's conjecture as well as RH.

The best unconditional result, due to Bombieri and Davenport, is that $E<(2+\sqrt{3})/8 = 0.46650...$

So, even though the unconditional results will be superceded if RH is proved, the techniques and ideas developed to attack these problems have, and will continue to have, important applications to other problems.

4. EVIDENCE: What makes the R.H appealing, apart from its implications in many other problems, is its intrinsic difficulty. The evidence as it stands at present is very weak and circumstantial. It seems impossible to find what mechanism is forcing the infinite number of zeroes in the critical strip onto the line $\sigma=1/2$.

Littlewood even went as far as to write, in 1962, "In the spirit of this anthology of partly baked ideas I should also record my feeling that there is no imaginable reason why the Riemann Hypothesis should be true."

Against such opinion we can only offer such results as that of G.H. Hardy who showed, in 1914, that there are infinitely many zeroes on $\sigma=1/2$. This was improved by Selberg in 1942 to "The number of zeroes on the line from $1/2$ to $1/2+iT$ is at least $KT\log T$ for some positive K, and all sufficiently large T." It

is known that the number n(T) of zeroes $\rho=\beta+i\gamma$ in the critical strip with $0<\gamma<T$ satisfies

$$n(T) \sim (T/2\pi)\log T \quad \text{as } T\to\infty.$$

So Selberg's result shows that a positive proportion of the zeroes in the critical strip lie on Res=1/2. In 1974 N.Levinson showed that this proportion is greater than 1/3.

An extensive calculation by Rosser which showed that the first three and a half million zeroes (ordered by size of ordinate) lie on the line $\sigma=1/2$ has since been superceded by an even more extensive one, showing that the same is true for the first two hundred million and one.

All this may be, for some, sufficient proof of Riemann's Hypothesis, re the old joke about the Engineer proving that all odd numbers are prime.Yet for Mathematicians the search for the proof, or disproof, of the conjecture continues.

Reference.

[1] Riemann's Zeta Function. H.M.Edwards. Academic Press 1974.

Clerihews

The axioms of a clerihew are very simple: it is a poem, normally biographical, of four lines, rhyming AABB. It does not have any restrictions of subject, and mathematicians seem as good as any other. Of one of the greatest of contemporary mathematicians, it is written:

Alexander Grothendieck
Proved a theorem in a week.
Then he wrote a book.
I don't know how long that took.

and

Alexander Grothen-
dieck said "Chess is rotten.
What keeps the mind alive
Is SGA5"

Indeed, many Frenchmen lend themselves to such treatment:

When they told Borel
His theorems were swell,
He said "I think
They stink."

"Och aye, hoots, mon !"
Exclaimed Alain Connes
Discovering a foliation
At Edinburgh station.

Andre Weil
Wrote a book in a deil
But Hermann Weyl
Took quite a wheyl

Jean Dieudonné
Was filled with dismay
When his publishers threatened to freeze
The number of volumes in his Traite d'analyse.

René Thom
Dit "Je dois acheter une gomme:
Mes erreurs analytiques
Sont catastrophiques"

As the above shows, there is no reason why a clerihew should be in English.

Carl Friedrich Gauss
Ging gern niemals aus dem Haus:
Während fünfzehn Jahre sprach er nur mit seiner Katze
Bis fand er den Quadratreciprozitätsatz.

"Il faut cultiver le jardin"
Dit Elie Cartan.
"Les algébres de Lie
M'ennuyient"

Which brings us back to France again, where

J.-P. Serre
Stuck straws in his hair
Took a bath in lager
And went completely GAGA.

In doing this, he was not alone: many mathematicians go bananas.

Saunders MacLane
Went quite insane
And consulted an oracle
About matters categorical

Alan Baker
Was once a Quaker
But went quite mental
And became transcendental

Several clerihews are quite close to home:

Sir Michael Atiyah
Was coming here,
But the fellows of Trinity
Felt no affinity.

Martin Taylor
And Uncle Béla
Are paid for their knowledge
By Trinity College

Thompson and Feit
Tried a problem one night
And became quite voluble
When they found it was soluble

Cayley
Gaily
Opines:
"On a cubic surface there are twenty-seven lines"

Paul Dirac
Said "Put that electron back!
Or there'll be nowhere for me
To bathe in the zero-energy sea"

John Edensor Littlewood
Kept a mistress in Cricklewood.
His "niece" was in fact his daughter:
One rather feels he hadn't ought to.

Bryan Birch
Was left in the lurch
When Peter Swinnerton-Dyer
Went on to things higher.

More often, they are simply drivel.

The Mayer-Vietoris sequence
Occurs with remarkable frequence
But, withal,
It's not spectral

Leonhard Euler
Was a relentless toiler
In the cause of introducing the beaver
To Lake Geneva

J.H.C. Whitehead
Had his later life blighted
By the end of his hope
Of being elected Pope

The Monster that was found by Fischer
Was a most carnivorous creature,
While the one unearthed by Griess
Lived entirely on rice

Hermann Weyl
Had a name that would rile:
Someone else's moniker
Was Krönecker

Georg Cantor
Liked to indulge in light banter:
But caused rather a ruction
Doing it by transfinite induction.

Bernhard Riemann
Fancied himself as a he-man:
His weight-lifting could not have been neater,
But he should have spent more time on the zeroes of zeta.

The following two discoveries were made independently:

Weierstrass and Bolzano
Were playing with Meccano
When they noticed the fact
That it was sequentially compact

The Abbé Bolzano
Liked to play with Meccano.
It was this pastime, one feels,
That led him to prove the connectedness of the reals.

Zorn
Was free when he was born
But now, because of his brains,
Everywhere he is in chains.

Artin and Rees
Proved a theorem apiece
But Roch and Riemann
Proved one between 'em

The consistency of cheese
Was discovered with ease
When Kurt Gödel
Allowed the milk to curdle.

Haar
Worked behind a bar.
In his leisure
He discovered a measure.

Baire
Had very little hair:
Above his face
Was a Banach space

That is quite enough of that. Contributors: Robert Wilson, John Greenlees, Jeremy Rickard, Richard Pinch, Miranda Mowbray, Peter Hall and Gregory Sankaran. Who wrote what is left as an exercise to the reader. So are the unsolved problems of encapsulating Carathéodory, Archimedes, Quillen, Ramanujan (pronounced RamAnujan, please), Pythagoras (preferably in Greek) and Kolmogorov (preferably in Russian) in verse. (And thanks to Bill Rose for proof-reading the German one.)

Why is there an Elementary Proof of the Fundamental Theorem of Algebra?

Martin Hyland

This looks like a daft question: should it not have the answer *because it's there*? But in fact there is no remotely elementary proof in the modern mathematical literature. This note is concerned with showing how one can know *that* there must exist a proof of a certain elementary kind, without knowing *what* that proof is. The following article sketches such a proof: *Gauss' second proof*. By a curious historical accident (cf the case of the prime number theorem detailed below) this was the first essentially unproblematic proof of the theorem.

The *fundamental theorem of algebra* states that any non-trivial polynomial with coefficients in the field **C** of complex numbers has a root in **C**. (Equivalently and more memorably, any polynomial over **C** factors completely into linear factors.) A field with this property is said to be *algebraically closed*. Now algebraic closure is an *elementary property* of fields in the technical sense that it can be expressed by a set of statements in the *first order* langauge of fields: for $n=1,2,\ldots$ we take

$$a_0,\ldots,a_n(a_n\neq 0 \rightarrow x(a_nx^n+\ldots+a_0=0))$$

Furthermore as **C** is obtained algebraically from **R** (**C** is **R**[i], that is **R**x**R** with pointwise addition and the usual multiplication $(a,b)(c,d)=(ac-bd,ad+bc)$), that **R**[i] is algebraically closed is an elementary property of **R**.

R has the following properties which are firmly founded in Analysis I:

(i) for any non-zero a, exactly one of a and $-a$ has a square root;

(ii) any odd-degree polynomial has a root.

A field with these properties is said to be *real closed*. Real closure is again an elementary property in the technical sense.

Now we appeal to *one or other* of the following facts:

(1) ALGEBRAIC LOGICAL FACT The first order theory of real-closed fields is *complete*: that is, for any sentence ϕ, either the theory proves ϕ or it proves $\neg\phi$ (the negation of ϕ). [This needs a piece of substantial though elementary algebra called *Sturm's Algorithm*.]

(2) ALGEBRAIC FACT Any real closed field k has $k[i]$ algebraically closed. [E. Artin's proof of this is sketched at the end of Paul Taylor's article].

From either of these we can deduce that there must exist a first order proof from the axioms for a real closed field of the elementary fact (ie collection of elementary statements) that by adjoining a square root of -1 we get an algebraically closed field.

From (1): each elementary statement is either provable from the axioms or inconsistent with them. The latter possibility is ruled out since (we know that) $\mathbf{R}(i)$ *is* in fact algebraically closed.

From (2): By an appeal to the completeness theorem for first order logic. Every model for the axioms (of a real closed field) is a model for the elementary fact that adding a $\sqrt{-1}$ gives an algebraically closed field. Therefore there is a first order proof.

What we have discovered is a characteristic phenomenon in mathematical logic. Proof theoretic considerations often show that given ϕ is true or has been proved in a particular way then there must be a highly elementary proof of ϕ. For example the prime number theorem is provable in a fragment of analysis which only involves arithmetic comprehension: therefore (by "cut elimination") there is a purely number-theoretic proof. But the interesting question in all such cases is, *is there an interesting or comprehensible* elementary proof? (There is one of the Prime Number Theorem.)

I told the story from the second paragraph on to Professor Cassels a couple of years ago, commenting that I had never seen an elementary proof, and he responded at once, "But wasn't Gauss' second proof elementary in this sense?" I was taken aback as I regarded Gauss' second proof (in line with the modern literature) as essentially identical with Artin's, and that is far from elementary (at least in the technical sense). Indeed when we went to the library to settle the point we were frustrated: we could find no account of Gauss' proof. A day later I received a note directing me to Felix Klein, *Vorlesungen über die Fritwicklung der mathematik in 19 Jahrhundert*, which on pp 55-56 sketches a late 19th century version of Gauss' proof: *this* proof *is* elementary. Finally Paul Taylor has gone back to our roots and has laid out the original proof for our delectation.

In conclusion I should say that many subtle issues in the history and philosophy of mathematics are raised by the relation between the Gauss and Artin proofs. Also this relation throws light on the well-known mathematicians' joke that "it is all essentially in Gauss".

Gauss' Second Proof

Paul Taylor

The fact that any non-trivial polynomial equation has a root in the field of complex numbers will be familiar to all readers of *Eureka*, just as it became familiar to Mathematicians at some stage between the end of the Dark Ages (ie the publication of the *Ars Magna* in 1540) and the mathematical birth of Gauss in 1796. The best known proof of it occurs in Part IB Complex Variables: for sufficiently large values of the indeterminate, the highest degree term (z^n) dominates and by Rouché's theorem the polynomial has the same number of zeroes as this single term, viz. n. This is not the proof that interests us, however: we want a purely *algebraic* proof for real closed fields. (See the previous article.)

Later I shall give the modern two-line proof of this (due to Artin), using Galois' and Sylow's theorems, which must somehow be a descendant of the one given here. However the connection is difficult to spot, and the precise genealogy could easily form the subject of a PhD thesis in the history and philosophy of science, or indeed the basis of a book on the history of modern algebra since the lemmas I shall state without comment hint at the foundations of most branches of the subject. I should be delighted to hear from any reader who can throw light on some of the connections.

This article is a précis of my translation of Gauss' paper [2]; I should like to thank Bernard Leak for his corrections to my rusty Latin.

Proposition 1 (*Euclid's algorithm for polynomials*) Given two polynomials $Y(x)$ and $Y'(x)$, there are polynomials $Z(x)$ and $Z'(x)$ such that $ZY+Z'Y'$ is the greatest common divisor of Y, Y'.

Corollary Y, Y' have no common factor iff $ZY+Z'Y'=1$ for some Z, Z'.

Proposition 2 Any symmetric polynomial in n variables $a,b,\ldots$ may be expressed uniquely as the result of substituting $\sigma_1=\Sigma a$, $\sigma_2=\Sigma ab$, $\ldots$, $\sigma_n=\Pi a$ for $s_1,\ldots,s_n$ in some polynomial in $s_1,\ldots,s_n$.

This result is frequently proved using independent transcendentals in a Galois Theory course; Gauss gave an easier, prettier, constructive and more convincing proof which the reader is invited to find for itself. Gauss' paper consists largely of repeated use of this result, and employs the convention that

Y is the polynomial $x^m - S_{m-1}x^{m-1} + \ldots \pm S_0$ with particular determined coefficients and (possibly) roots A,B,...,

y is the polynomial $x^m - s_{m-1}x^{m-1} + \ldots \pm s_0$ with indeterminate coefficients and no roots, and

v is the polynomial $(x-a)(x-b)(x-c)\ldots$ with coefficients $\sigma_1, \ldots \sigma_n$ and roots $a,b,c\ldots$

Other corresponding upper case Latin, lower case Latin and lower case Greek letters are used similarly.

The *discriminant* of a polynomial v is the product $\pi = (a-b)(a-c)\ldots(b-a)(b-c)\ldots$ and correspondingly those of Y and y are P and p respectively. Y', y' and v' are used for the formal derivatives of Y, y and v with respect to x.

Proposition 3 Y and Y' have a common factor iff P=0.

Gauss takes the opportunity here of being rude to his inferior contemporaries. Of course the result is obvious for v, ie if the polynomial factorises, but that is begging the question (*petitio principii*). He spends several pages on the proof (bringing various clever formulae out of a hat), but the result is easy for us with abstract algebra (we do not suffer from the handicap of *believing* in the real numbers) since it's a triviality to construct field extensions containing the required roots. We need only that Y and Y' factorise in *some* field containing **R**, not necessarily **C** itself.

Given a polynomial (say of degree $2^\mu k$ with k odd) with zero discriminant (which is really trying to say that it has a repeated root), we may extract from it the common factor with its derivative. Continuing this process inductively, any polynomial may be split (rationally) into factors each of which has a nonzero discriminant. Moreover the degree of at least one of these factors will be $2^\nu l$ with l odd and $\nu \leq \mu$. The proof will proceed by induction on the multiplicity of 2 as a prime factor of the degree, whilst the degree itself will increase astronomically.

Gauss now introduces a little elementary group theory (in the form of a discussion of symmetric polynomials) before proceeding in his usual fashion with a brilliant unmotivated proof using another indeterminate u. Subscripts $_u$ and $_x$ will be used for partial derivatives.

Let ζ denote the product of all $u-(a+b)x+ab$ excluding repetitions, and Z, z the polynomials corresponding in the usual way. By similar methods as before he proves

Proposition 4 If $P \neq 0$ then the discriminant of Z with respect to u cannot be identically zero as a function of x.

For those who are at this point wondering where we are going, I have to tell you that there are many more complicated calculations still to do. Moreover it is not until the very last section that the real-closed hypotheses make their appearance.

Lemma Let $\phi(u,x)$ denote a product of any number of factors, into each of which the variables u,x enter only linearly, ie which are of the form $\alpha+\beta u+\gamma x$, $\alpha'+\beta' u+\gamma' x$, $\alpha''+\beta'' u+\gamma'' x$, ..., and w be another variable. Then the polynomial $\Omega = \phi(u+w\phi_x(u,x),\ x-w\phi_u(u,x))$ is divisible by $\phi(u,x)$.

This lemma is clearly applicable to the polynomial ζ, which we may write as $f(u,x,\sigma_1,\sigma_2,\ldots)$ so that

$$f(u+w\,\frac{\partial\zeta}{\partial x},\ x-w\frac{\partial\zeta}{\partial u},\ \sigma_1,\sigma_2,\ldots)$$

is exactly divisible by ζ: the quotient, which will be a polynomial in $u,x,w,a,b,c,\ldots$ symmetric in $a,b,c,\ldots$, we may write as $\psi(u,x,a,b,c,\ldots)$. Hence

$$f(u+w\frac{\partial z}{\partial x},\ x-w\frac{\partial z}{\partial u},\ s_1,s_2,\ \ldots) \ = \ z\ \psi(u,x,w,s_1,s_2,\ldots)$$

and

$$f(u+w\frac{\partial Z}{\partial x},\ x-w\frac{\partial Z}{\partial u},\ S_1,S_2,\ldots) \ = \ Z\ \psi(u,x,w,S_1,S_2,\ldots)$$

Then we may more simply write the polynomial Z as $F(u,x)$ so that

$$F(u+w\frac{\partial Z}{\partial x},\ x-w\frac{\partial Z}{\partial u}) \ = \ F(u,x)\ \psi(u,x,w,S_1,S_2,\ldots)$$

If we put $u=U$, $x=X$, so that, say, $\partial Z/\partial x=X'$, $\partial Z/\partial u=U'$, then we shall have

$$F(U+wX',\ X-wU') \ = \ F(U,X)\ \psi(U,X,w,S_1,S_2,\ldots)$$

Then as long as U' doesnt vanish, we may set $w=(X-x)/U'$ to get

$$F(U+\frac{X}{U'}\frac{X'}{}-\frac{x}{U'}\frac{X'}{},\ x) \ = \ F(U,X)\ \psi(U,X,\frac{X-x}{U'},S_1,S_2,\ldots)$$

Hence if in Z we put $u = U + XX'/U' - xX'/U'$ it becomes

$$F(U,X)\ \psi(U,X,\frac{X-x}{U'},S_1,S_2,\ldots)$$

When, in the case that $P\neq 0$, the discriminant (wrt u) of the polynomial $Z=F(u,x)$ is a nonvanishing function of x, clearly the number of definite values of x for which the discriminant of Z can be 0 will be finite, so that there are infinitely many choices for x giving a nonvanishing discriminant. Let X be such a (real) value, so that the discriminant of the polynomial $F(u,X)$ will be nonzero and so $F(u,X)$ and $F_U(u,X)$ have no common factor. Now let us suppose that there is some definite (complex) value, say U, of u satisfying $F(u,X)=0$, ie such that $F(U,X)=0$, so that $(u-U)$ will be a factor of the polynomial $F(u,X)$ and not of $F_U(u,X)$. Let the latter take the value U' for $u=U$, so $U'\neq 0$. Let X' be the value of $F_X(u,x)$ for $u=U$, $x=X$. Then by the above result Z will vanish identically by the substitution $u = U + XX'/U' - X'x/U'$ and so Z is divisible by the factor $u + X'x/U' - (U + XX'/U')$.

Hence $F(x^2,x)$ is divisible by $x^2 + xX'/U' - (U + XX'/U')$ and so has roots

$$\frac{-X' \pm \sqrt{4UU'^2 + 4XX'U' + X'^2}}{2U'}$$

in **C**. Moreover *it may easily be shown that* for the same values of x the polynomial Y must also vanish; for clearly $f(x^2,x,\sigma_1,\sigma_2,\ldots)$ is the product of all $(x-a)(x-b)$ excluding repetitions and so equal to v^{m-1}. Hence it immediately follows that $F(x^2,x)=Y^{m-1}$, which cannot vanish unless Y itself vanishes.

With the help of the preceding discussion, the solution of the equation $Y=0$ of degree n (where the discriminant of Y is nonzero) is reduced to that of $F(u,X)=0$. It is appropriate to observe that if all of the coefficients in Y are real quantities then so are those in $F(u,X)$, since it is possible to make X real. The degree of the secondary equation $F(u,X)=0$ is $n(n-1)/2$, in which 2 occurs as a prime factor once less often than in n (assuming n even).

If the discriminant of Y is zero, then as remarked above it may be split into factors whose discriminants do not vanish, and it suffices to find a root of any of these.

We thus obtain a sequence of polynomial equations of degrees $2^{\mu_0}k_0$, $2^{\mu_1}k_1,\ldots$ with $\mu_0>\mu_1>\mu_2>\ldots$, and hence ultimately one of odd degree which may be solved by hypothesis (or, *obviously* in **R**). Moreover any solution to the last yields one for the previous ones and hence the original equation, as required.

Now let us attempt to understand how this proof works in modern terms. First, one may easily show from the Euclidean algorithm in the same way as for **Z** that

Proposition 5 Any polynomial in one variable over an arbitrary field factorises into irreducibles, uniquely up to permutation and multiplication by nonzero scalars.

Of course Gauss will have been well aware of this, and it is a little surprising thet he doesnt use the word irreducible. The result may now be restated as follows:

Theorem 6 (Gauss) A non-trivial irreducible polynomial over **R** is a scalar multiple of $x^2 + 2ax + (a^2+b^2)$ and hence factorises over **C**.

At this point I shall make use of our 170-year head start on the master, which is the means by which I have already reduced propositions 3 and 4 to trivialities and hence cut down Gauss' paper by three quarters. Let k be any field and $f(x)$ an irreducible polynomial over k. Let α be a new indeterminate and denote by $k(\alpha)$ the vector space of polynomials in α over k of degree less than that of f; this has a multiplicative structure given by setting multiples of $f(\alpha)$ to zero.

Proposition 7 $k(\alpha)$ is a field containing k in which $f(x)=0$ has a root α. Moreover if L is another field containing k and a root β then there's a unique embedding of $k(\alpha)$ into L which preserves k and identifies α with β.

The reader is invited to formulate and prove the uniqueness of $k(\alpha)$. It is an easy matter to show (in the same sense) that

Proposition 8 Let k be any field and $f(x)$ any polynomial over it. Then there is a smallest field K containing k in which f splits into linear factors.

K is called the *splitting field* of f over k; a field extension (ie an inclusion of one field in another) is said to be *normal* if it is of this form. A field extension is normal iff every polynomial which is irreducible over the smaller field but has a root in the larger actually splits in the larger ("*one out - all out*").

Suppose then we have a non-trivial irreducible polynomial $Y(x)$ over **R** with splitting field K; we aim to show that $K\cong\mathbf{C}$, ie the dimension of K as a real vector space (which is called the *degree* of the extension K:**R**) is 2.

Now consider Gauss' secondary polynomial $F(u,X)$. This clearly splits in K, so its splitting field L is contained in K. On the other hand the roots of the original polynomial are obtained from those of $F(u,X)$ by solving some quadratics, which is the same as saying that K is obtained by adjoining some square roots to L. Hence, whilst the secondary equation may have much larger degree, it is in some sense no more difficult to solve, and indeed possibly easier.

Repeating Gauss' construction, we obtain a descending sequence of field extensions contained in K:**R** which is such that each is obtained from the next by adjoining square roots and the last is the splitting field for an odd-degree polynomial.

Gauss' construction is a little stronger than this. In order to construct K we do not need the splitting field of the whole of the secondary polynomial $F(u,X)$, but only of a non-trivial irreducible factor. This is because Gauss only asks for a single root of the secondary polynomial in order to get a root of the orininal one, and since K is normal this is all we need. Hence at the last stage it is sufficient to consider the linear factor which an odd-degree polynomial is guaranteed to have; the splitting field of this is of course just **R**.

Hence K, the splitting field of the original polynomial, is obtained by adjoining square roots to **R** itself. But we can only do this once because the existence of square roots in **C** is an easy exercise. Hence K is indeed just **C**.

Now I shall give Artin's proof, quoting major theorems from two Part II courses; the word *separable* is included for purely legal reasons, the condition being automatic for fields containing **Q**.

Theorem 9 (Galois) [4] Let $K:k$ be a normal separable extension of finite degree and let G be the group of field automorphisms of K which fix each element of k. Then there is an order reversing bijection beteen the subgroups H of G and the fields L lying between k and K; moreover the degree of $L:k$ is equal to the index G:H.

Theorem 10 (Sylow) [3] Let G be a finite group of order $p^a m$ where p is a prime not dividing m. Then G has subgroups of order p^b for each $0 \leq b \leq a$.

Applying this to the case in hand with $p=2$, $K:\mathbf{R}$ being the splitting field of an irreducible polynomial Y, there is a field L lying between **R** and K such that the degrees of K:L and L:**R** are respectively a power of 2 and odd. L must be obtained from **R** by adjoining roots of irreducible odd-degree polynomials (which is impossible) and K from L by solving quadratics. Hence $L=\mathbf{R}$ and $K=L(i)=\mathbf{R}(i)=\mathbf{C}$.

Two problems I shall leave to the reader are spotting the theorem of the primitive element and the proof of Sylow's theorem for $p=2$ (I believe one can generalise Gauss' method to a proof of Sylow's theorem in general). Of course Gauss does not prove Galois' theorem because in Artin's proof this serves merely to translate Sylow's theorem from (permutation) groups to fields (and hence polynomials), whereas if one speaks the local language fluently oneself one does not need an interpreter.

References

The first of these is an addendum to my previous article [5], kindly supplied by Walter Ledermann.

[1] Frobenius, G., Über lineare Substitutionen und bilineare Formen, *Journal für die reine und angewendte Mathematik* (Crelle's Journal) **84** (1878) 1-63

[2] Gauss, C.F., Demonstratio nova altera theorematis omnem functionem algebraicam rationalem unius variabilis in factores reales primi vel secundi gradūs resolvi posse. *Gauss Werke* **3** 33-56

[3] Johnstone, P.T., *Algebra I example sheet 3*, DPMMS, 1982

[4] Stewart, I.N., *Galois Theory* Chapman & Hall

[5] Taylor, P., The Uniqueness of the Quaternions, *Eureka* **44** (1984) 63-68

Authors

Christopher Longuet-Higgins is Royal Society Research Professor at Sussex Univesity. He is attached to the Laboratory of Experimental Psychology and is currently working on computer vision and automatic speech recognition. His interests also include the automatic transcription of music from the keyboard.

Cedric Smith fondly imagines that he is at present Emeritus Professor of Biometry, UCL, Chairman of the Conflict Research Society, Joint Editor of Colson News (Two-way Numbers), Joint Editor of Annals of Human Genetics, son-in-law of a Hungarian expert on Summability, and an Out-Patient in University College Hospital. He thinks that he once was TMS Secretary, porter at Addenbrookes Hospital, Chairman of the British region of the Biometric Society, Secretary of the Research Section of the Royal Statistical Society, Treasurer of the Friends Peace and International Relations Committee, and a Youth Hosteller. He also thinks he is interested in Graph Theory, Theory of Games, Phonetics, Subjective Probability, Elliptic Functions, Iteration, Finger Prints, Orthology and Matroids. However, all that can only be self-delusion, because an authoritative paper by Descartes in the Journal of Recreational Mathematics demonstrated conclusively that C.A.B. Smith is only a CAmBridge myth, being no more than one of many pseudonyms adopted by the prolific Italian mathematician, Prof. Carla Rossi of the University of Rome.

Thomas Forster is a reformed Philosopher and Physiologist turned Mathematical logican. He spends half his time in New Zealand where he (still) teaches philosophy, wears a grass skirt and awaits armageddon in comfort.

Richard Pennington is a graduate student at the Institute of Astronomy, Cambridge, before which he followed an undergraduate career as a physicist, also at Cambridge. He claims to know no mathematics below Part III level, but this has not so far prevented him from helping to set three Problems Drives!

Eddy Welbourne is mentioned elsewhere under various hats. Previous published works amount to one: a *'treatise'* in *2-Manifold* on punting. Best known for his brief spell as Trinity Rag (and later as the fourth Lunaticus Magnus), or possibly for the frequency of his encounters with the Cam (or maybe for the laugh), he is frequently to be seen wearing scarves which might scare people out of their *souls*.

Furthermore, our secret agents suspect him of being an undercover member of the New Pythagoreans, as well as the TMS.

Mark Coleman is a graduate of Imperial College, London, well into his third year here. His research interests would appear to be wandering around the Complex Plane, and up and down the Real Line looking for primes. In this vein of ambulatory activity, he is an active member of the C.U. Youth Hostel Association.

Martin Hyland is a Fellow of King's College and a Lecturer in the Department of Pure Mathematics and Mathematical Statistics in Cambridge. He has recently been coerced by the Editor of *Eureka* not only into writing this article but also into the application of mathematical logic to computer science.

Paul Taylor is a graduate student with the above-mentioned research interests. As an undergraduate he was founding editor of *QARCH*, for which crime he was sentenced to being President of the Archimedeans; however this was commuted after a Fermat prime number of days.

Answers to Problems Drive

1 $1225 = 35^2 = 49 \times 50/2$ $\quad 41414 = 204^2 = 288 \times 289/2$

2 A is Applied and Sane
B is Pure and Insane
C is Applied and Insane

3 $2/\pi$

4 Possible for cube, octahedron and icosahedron

5 Block is 6x4 or 10x3 (either way round)

6

1 3	2 6	3 1	4 3
5 5	8	3	2
6 2	7	4	4
9	7 8	2	0

7 96 qarches

8 The 500000th derivatives of $A(x)$ and $B(x)$, or linear combinations of these

9 (a) 323, 437, 667 products of consecutive primes
(b) 5, 4, 5 *ARCHIMEDES* with A=1, B=2, etc.
(c) 100, 121, 144 squares in base seven

10 The radius of Lake Bathwater is 42500 cubits;
the ferry arrives at 1.17 pm

11 $\frac{31}{44}$ $\frac{43}{61}$ $\frac{50}{71}$ $\frac{62}{88}$ $\frac{69}{98}$

12 156. He needs one *winner* and 156 *losers*