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

The Archimedeans Journal

ISSN 0071-2248

Editorial

Observant readers will have noticed the overwhelming bias toward Pure Mathematics in this edition of Eureka. This reflects not so much a consistent editorial policy as an almost complete absence of articles received on Applied Math! There has also been a very poor supply of articles from undergraduates. If Eureka is to continue as the journal of the Archimedeans and not become just another journal on Mathematics we need some good original articles from undergraduates. We hope to produce another edition of Eureka in the near future; let's hope we can have some undergraduate articles in it this time!

C J Budd St Johns

N Boston Trinity

Acknowledgements

The Department of Pure Mathematics and Mathematical Statistics Tracy Kelly.

The Archimedeans

by J. Rickard

It was on a Wednesday afternoon in early March. The small crowd who had gathered in the Arts School for the Archimedeans A.G.M. had not come for the President's report, the constitutional changes or the election of the new committee, but they knew that these were the price that they would have to pay for this, the moment they had all been waiting for. You could have heard a pin drop as the outgoing Junior Treasurer took the stage; the respectful audience remained silent as he presented the accounts with his inimitable style and nerve, but they could not hold back a gasp of admiration as he reached the breathtaking climax and wrote on the blackboard: TOTAL INCOME - £66. In the excitement another interesting outcome of the meeting went almost unnoticed; for the first time in the memory of even the oldest undergraduate, there were no members of Trinity College on the new committee!

The Easter Term saw the usual mad whirl of social events designed to erase the word 'examination' from the consciousness of maths undergraduates. The croquet afternoon achieved a new record for the close-packing of players on a croquet lawn, and a flotilla completed the annual punt trip to Grantchester and back, breaking one record for incompetence at punting and one punt pole. On a wet Sunday afternoon rain stopped play at the punt joust against the Dampers. Because of the lack of shelter, spectators and Archimedeans, a new date was arranged, but the Dampers insisted that the President and the Secretary should also joust there and then; although we were none too keen, we felt honour bound to accept the challenge, making it a sort of punts and duty now. Later that week, the rematch went ahead successfully.

At the beginning of the new academic year, the committee sprang into action to organise the annual recruiting drive for the Societies' fair. The generosity

of one of the editors of Eureka in lending us a computer to liven up our stall was somewhat neutralised by the mechanical incompetence of the committee in operating it, and the fact that we were next door to the Computer Society stall.

Speaker meetings have been very successful this year with an extremely large number of members turning up for the (literally) colourful talk by David Singmaster on the "Rubiks Cube', and also increasing attendances at the lunch time meetings. The College Societies have also had many exciting talks. In the Michaelmas Term the second inter-galactic Mathematical Call My Bluff competition took place in Cambridge, with teams from Oxford, Warwick, Southampton and Kings College London taking part. Cambridge spurned the obvious ways of winning (i.e. skill and cheating) and instead successfully used the statistical method of fielding three times as many teams as anyone else. We also had an expedition to Oxford to play games against their Maths Society - the Invariants.

Other aspects of the Society have also been successful, such as the computer group, the telephone exams results service and especially the bookshop, whose new manager has made a great financial success of it (rumour has it that he will soon be making a bid for Heffers).

Finally thanks are due to all people who have helped to make the Archimedean and the College Societies continuing successes this year.

Errata in Edition Number 42

The article "Achieving the Skinny Animal" in Eureka, number 42, contained [illegible] errors and was printed without its references. Eureka wishes to [illegible]pologise to Professor Harary and its readers for these mistakes.

Below are listed the corrected board and move numbers of proved winners (the game given in section 3, 'Achieving Skinny', is thus in error). In [illegible]addition we list the omitted references.

[illegible] 1. The board and move numbers of the proved winners.

	b	m
[illegible]	1	1
[illegible]	2	2
[illegible]	4	3
[illegible]	3	3
[illegible]	7	8
[illegible]	4	4
[illegible]	5	4
[illegible]	3	5
[illegible]	7	9
[illegible]	7	8
[illegible]	6	6

References

1. E.R. Berlekamp, J. Conway, R.K. Guy, Winning Ways. Academic Press, London (1982).

2. M. Gardner, Mathematical Games in which players of Ticktacktoe are taught to hunt bigger game. Scientific American, 240 (April 1979) 18-28.

3. S. Golomb, Polyominoes. Scribner's, New York (1965).

4. F. Harary, The cell growth problem and its attempted solutions. Beiträge zur Graphentheorie (H. Sachs et al., eds.) Teubner, Leipzig (1968) 49-60.

5. F. Harary, Recent results on generalized ramsey theory for graphs. Springer Lecture Notes Math. 303 (1972) 125-138.

6. F. Harary, An achievement game on a toroidal board. Springer Lecture Notes Math. (M. Sysio, ed.), to appear in 1983.

7. F. Harary, Achievement and Avoidance Games (in preparation).

8. F. Harary and E.M. Palmer, Graphical Enumeration. Academic Press, New York (1973).

Some Simple Games We Still Can't Solve

by R K Guy

Classical game theory has its origins and applications in economics and military strategy: business games and war games. Its interest stems almost entirely from the existence of chance moves, the lack of complete information and the possibility of coalitions when there are more than two players. The "completely determined game" between two players, with no chance moves and complete information, is of no interest to the classical game-theorist. The existence of an optimal strategy for each player renders play pointless. No-one is interested in playing Chess or Go! Well, perhaps a few people are, since the number of strategies to be examined is, at present, beyond the reach of the computer.

Yet some of us, the authors of [1] for example, are interested in very much simpler games! Here we'll look only at impartial games (the same set of options is available to each of the two players), with normal play (last player wins: if you can't move, you lose), which finish in a finite time. Sprague [5] and Grundy [3] gave a complete analysis of these games. Any position in any such game is equivalent to a heap, with an appropriate number of beans, in the game of Nim!

And we all know how to play Nim. There are several heaps of beans. At your turn, choose a heap and remove as many beans as you like: at least one, maybe the whole heap. If you take the last bean, you win. Bouton [2] showed how to find a good move, if there is one. Imagine each heap broken into unequal powers of two. Pair off equal powers of two (from different

heaps). If they all pair off, it's a $\mathcal{P}$-position (previous player wins), so hope it's not your move. If they don't pair off, then you can find a move which reduces one of the heaps so that the new powers of two do all pair off.

Sprague and Grundy gave a simple recursive algorithm for finding the size of the nim-heap that's equivalent to a position in an impartial game. Find, for each option, the size of the equivalent nim-heap. Take the mex of these sizes; the least non-negative integer that's not among them.

The importance of this nim-value is that the nim-value of the sum of several games is the nim-sum of their nim-values. To make a move in the sum of several games, choose one component game and make a legal move in it. Of the many ways of playing games simultaneously, the sum is often the most natural.

For example, the move in Grundy's Game is to divide a heap of beans into two *unequal* (non-empty) heaps. So each move produces an extra component in the sum. Since heaps of one or two can't be split into unequal heaps, there are no options. The mex of the empty set is zero, so the nim-values for heaps of one or two are zero. The nim-values for heaps of 0,1,2,...50 beans in Grundy's Game are easily calculated by the Sprague-Grundy algorithm:

000 102 102 102 132 132 430 430 430 412 312 412 412 415 415 415 410

We think that these values will eventually settle down in a periodic pattern, but we haven't found it yet. To see why we believe this, read about sparse spaces and common cosets on pp.109-111 of [1].

Guy and Smith [4] found periodic patterns for the nim-values of several simple take-away games. They also gave a code which describes games whose rules are all of the following kind. At your turn, take k beans from a heap, leaving the rest in exactly a or b or c or ... non-empty heaps (a,b,c,... distinct). The code digit d_k is then defined as $2^a + 2^b + 2^c + \cdots$ for each $k = 1,2,3,\ldots$. The game is then coded as $\cdot d_1 d_2 d_3 \cdots$. For example, in Dawson's Chess, $\cdot 137$, since $1 = 2^0$, $3 = 2^0 + 2^1$, $7 = 2^0 + 2^1 + 2^2$, you may take 1 bean and leave 0 heaps, i.e. take 1 bean just if it's in one heap on its own; 2 beans and leave just 0 or 1 heap, i.e. 2 beans from the end of a row of 2 or more; 3 beans and leave 0,1 or 2 heaps, i.e. 3 consecutive beans from anywhere in a row of 3 or more.

Dawson's Chess and Kayles ($\cdot 77$, take one bean or two consecutive ones from anywhere in a row) turn out to have ultimately periodic nim-values (there are a few irregularities near the beginning). The (ultimate) periods are 34 and 12 respectively. But let's play Treblecross or 1-dimensional Tic-Tac-Toe. I won't say Noughts-and-Crosses, because both players use crosses. The object is to get three consecutive crosses so, if you're sensible, you won't play next, or next-but-one, to an already-played cross. It's not hard to see that Treblecross is just $\cdot 007$ (James Bond) in disguise! Take turns to place 3-square "trominoes" on the strip, without overlapping. The nim-values, for strips of 0,1,2,... squares are

0001112203 3111043332 2244055222 3305011133 356...

Do these values eventually settle down into a periodic pattern? We don't know!

Here are the codes for sixty simple "octal" games for which we still don't know the answer to this question (·04 is another equivalent to ·007):

·04	·06	·14	·16	·36	·37	·56	·64	·74	·76
·004	·005	·006	·014	·015	·016	·024	·026	·034	·054
·064	·104	·106	·114	·125	·126	·127	·135	·136	·142
·143	·146	·162	·163	·164	·166	·167	·172	·174	·204
·205	·206	·207	·224	·244	·245	·264	·324	·334	·336
·342	·344	·346	·354	·362	·364	·366	·371	·374	·376

One or two of these may be cases of laziness or carelessness, and one or two more may yield to the persuasion of a computer. Let me know if you have any luck. I suspect that most of them will keep their secrets for many years to come, though in my wilder moments I conjecture that they're all ultimately periodic.

References

1. E.R. Berlekamp, J.H. Conway & R.K. Guy, Winning Ways for your Mathematical Plays, Academic Press, London & New York, 1982.

2. Charles L. Bouton, Nim, a game with a complete mathematical theory, Ann. of Math., Princeton (2), 3 (1901-2) 35-39.

3. P.M. Grundy, Mathematics and games, Eureka, 2 (1939) 6-8; reprinted *ibid.* 27 (1964) 9-11.

4. Richard K. Guy & Cedric A.B. Smith, The *G*-values of various games. Proc. Cambridge Philos. Soc., 52 (1956) 514-526; M.R.18,546a.

5. R.P. Sprague, Über mathematische Kampfspiele, Tôhoku Math. J., 41 (1935-36) 438-444; Zbl.13,290.

Problems Drive 1983

By R Kerry and J Rickard

1. p and q are integers. r is the remainder on dividing $p^{40} + q^{40}$ by 100 ($0 \leq r < 100$). How many possible values are there for r?

2. In a game of noughts and crosses, played on a 5 x 5 board, at the end of which lines of length three exactly are counted, what is the maximum score you can obtain if you go first? Show a solution giving the maximum score.

3. What is the next number in each of these sequences, and why?

   i) 15145, 202315, 2081855, 6152118, 69225, ...

   ii) 32, 17, 41, 18, 52, ...

4. Complete the following league table.

	P	W	D	L	F	A	Pts.
England	3	1			7		
Wales				0		2	2
Ireland			2		1		2
Scotland		1			1	4	

There is one match left to play, the result of which does not affect the final order. What was the result of the England-Wales match?

5. Show how to arrange as few planes as possible so as to dissect a cube into congruent tetrahedra.

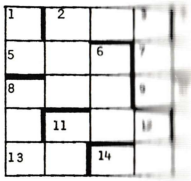
6. Solve this crossword.

ACROSS

2. 11A - 17
5. 10D - 13A - III
7. 1D - 1
8. Even permutation of 14A
9. L2
10. 8D - 5A
13. 18 46 ? 63 52 61
14. 3D + 2 x 7A

DOWN

1. 2D - 2A
2. Three consecutive digits
3. Odd permutation of 345
4. 7A x 3
6. 11A + 13A
8. M - 81
10. 999 - 2A
11. $(11A - \alpha)/(\alpha - 1)$, $\alpha \in \mathbb{N}$
12. Sum of digits of 8D

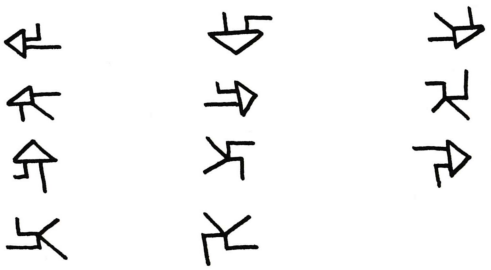


7. Is it possible to have a polyhedron all of whose faces are triangles, and at each of whose vertices 6 edges meet? Justify your answer.

8. Farmer Giles has a rectangular plot of land. On his death it is divided unequally by a straight line among his two sons in such a way that, although the ratio of the longer sides to the shorter sides is the same for both sons, his elder son has twice as much perimeter fencing as the younger. What was the ratio of the longer sides to the shorter sides of the original plot of land? Justify your answer.

9. For how many ordered pairs (m,n) of integers, $0 < m,n \leq 1415$, do $m\sqrt{2}$ and $n(2 + \sqrt{2})$ have the same integer part?

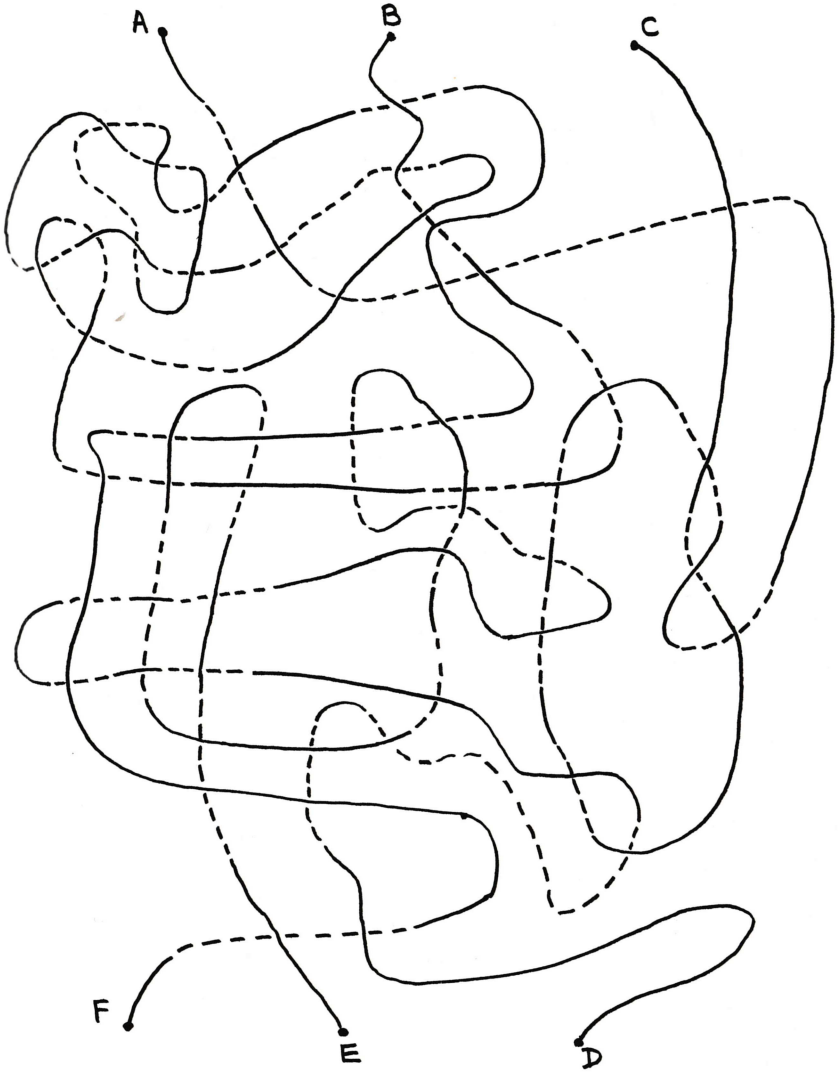
10. The following are 11 items out of a set of 12; what is the missing one?



11. Express each integer from 3 to 12 inclusive, using each of the seven symbols 1,2,3,4,+,x,- exactly once in each expression, using only parenth

uses in addition to these.

Which of the six points do you pull outward, keeping the other ends fixed, to form a straight string with no knots in it?



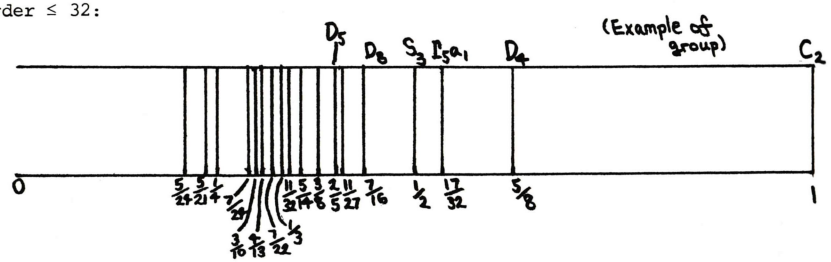
Nearly Abelian Groups

By N Boston

Just how non-abelian is a non-abelian group? To answer this question we might calculate the proportion of the $\frac{1}{2}n(n+1)$ unordered pairs of elements of a group G of order n that consist of elements that commute, i.e. $|\{\{x,y\}:x,y \in G, xy = yx\}|/\frac{1}{2}n(n+1)$. As the reader can verify, this in fact yields $(h+1)/(n+1)$, where h is the number of conjugacy classes of G .

For our purposes it will be convenient to set $a(G) = \frac{h}{n}$. In particular the set $S \subset [0,1]$ of all such values is closed under multiplication, for if H and K have h,k conjugacy classes resp., then $H \times K$ has hk , so $a(H\times K) = a(H).a(K)$.

The diagram below indicates the elements of S obtained from groups of order ≤ 32:



So what can we tell about S and in particular its irreducible elements (i.e. $x \in S$ such that if $x = ab, a,b \in S$, then either $a = 1$ or $b = 1$)? Well, there is not unique factorisation, since $(\frac{1}{2})^2 = \frac{5}{8}.\frac{2}{5}$: all lying in S by the above diagram and all irreducible by the following theorem (which shows that the largest reducible element is $(\frac{5}{8})^2$) :

Thm. 1. The largest element of S less than 1 is $\frac{5}{8}$.

Pf. Let G be nonabelian with centre $Z(G)$. Then h is maximised by having $Z(G)$ as large as possible with the remaining conjugacy classes of

... 2 . $G/Z(G)$, however, cannot be cyclic, since if it were, then G ... have a set of generators each pair of which commuted, so would be ...elian. Thus $|Z(G)|$ is at most $\frac{n}{4}$, leaving $\frac{3n}{8}$ conjugacy classes of ... 2 in the optimal case. This makes $h = \frac{5n}{8}$, attained e.g. for ... D_4 or the quaternion group of order 8 .

Calculation of further elements of S seems to become increasingly ...plicated. As an indication of the methods available to the interested ...ader, I offer the following contribution to the theory:

...m 2. The elements of S greater than $\frac{1}{2}$ are precisely

$$(2^{2n} + 1)/2^{2n+1} \quad , \; n = 0,1,2,\ldots$$

... By thm. 1 we can restrict our attention to $(\frac{1}{2},\frac{5}{8})$.

One can verify that the group G_n generated by $x_1,\ldots,x_{2n},y$ subject ... $x_i^2 = y \neq 1$, $y^2 = 1$, $x_i x_j = y x_j x_i \; (i \neq j)$, has order 2^{2n+1} and ...ass number $2^{2n} + 1$, so $\lambda_n = (2^{2n} + 1)/2^{2n+1} \in S$.

Now let G be a group of order n with centre of order m , a_i ...reducible characters of degree i , and with $\lambda_s n - k$ conjugacy classes ... 1) . We shall assume (1) $0 < k \leq n(\lambda_s - \lambda_{s+1})$, so it is enough to ...show $k = n(\lambda_s - \lambda_{s+1})$.

From character theory,

(2) $a_1 + 4a_2 + 9a_3 + \ldots + r^2 a_r = n$ (suppose $a_r \neq 0$) ,

(3) $a_1 + a_2 + a_3 + \ldots a_r = \lambda_s n - k$,

(4) $\frac{n}{m} \geq r^2$.

Counting conjugacy classes,

$m + 2(\lambda_s n - k - m) \leq n$, whence $k \geq (\lambda_s - \frac{1}{2})n - \frac{m}{2}$ (5) , so by (1)

$(\lambda_s - \frac{1}{2})n - \frac{m}{2} \leq n(\lambda_s - \lambda_{s+1})$, $\frac{n}{m} \leq \frac{1}{2}/(\lambda_{s+1} - \frac{1}{2}) = 2^{2s+2}$ (6) , so by (4)

$r \leq 2^{s+1}$.

Next I show $a_1 = \frac{n}{2}$ and deduce that we can assume G a 2-group. Eliminating a_2 between (2) and (3) ,

$$3a_1 = (4\lambda_s - 1)n - 4k + 5a_3 + \ldots + (r^2 - 4)a_r$$

$$\geq (4\lambda_s - 1)n - 4n(\lambda_s - \lambda_{s+1}) = (4\lambda_{s+1} - 1)n ,$$

so $a_1 \geq \frac{(2^{2s+1} + 1)n}{3.2^{2s+1}} > \frac{n}{3}$.

But $a_1 (=[G:G'])$ divides n , so $= \frac{n}{2}$.

Now no conjugacy class can have size greater than $|G'| = 2$, since if $g,x \in G$, then $gxg^{-1} \in G'x$. Hence $[G:C_G(x)] = 1$ or 2 , so $x^2 \in Z(G)$ $\forall$ $x \in G$. In particular any element of odd order lies in $Z(G)$, so $G/Z(G)$ is a 2-group so nilpotent. Thus G is nilpotent, so isomorphic to a direct product of its Sylow subgroups, say $P_1 x \ldots x P_t$. Now $a(G)$ irreducible implies $a(G) = a(P_i)$ for some i , so we may assume G is a p-group and $|G'| = 2$ ensures $p = 2$.

I wish to show $r = 2^{s+1}$. Suppose otherwise.

Then putting $b_i = a_{2^i}$, noting $b_o = \frac{n}{2}$, (2) and (3) become:

(7) $4b_1 + 16b_2 + \ldots + 2^{2s} b_s = \frac{n}{2}$

(8) $b_1 + b_2 + \ldots + b_s = (\lambda_s - \frac{1}{2})n - k$ (where b_s might be 0) .

Eliminating b_s ,

$$0 \leq (2^{2s} - 4)b_1 + \ldots + (2^{2s} - 2^{2s-2})b_{s-1}$$

$$= (2^{2s}\lambda_s - 2^{2s-1} - \tfrac{1}{2})n - 2^{2s}k = -2^{2s}k < 0 .$$

a contradiction so $r = 2^{s+1}$, whence by (4) and (6) $\frac{n}{m} = 2^{2s+2}$, and by (5) and (1) $k = n(\lambda_s - \lambda_{s+1})$, as desired.

This theorem (originally Bristow's conjecture after a friend's interpretation of the data for groups of order at most 32) should, I think, extend to give the elements of S just below $\frac{1}{2}$ as $(2^{2n-1} - 1)/2^{2n}$, $n = \ldots,4,3,2,$ possibly followed by $\frac{11}{27}$ and $\frac{2}{5}$. Thereafter we're delving into decidedly murky waters.

I leave the reader with a few open questions.

(I) Is S nowhere dense, or does there exist some interesting number $\alpha > 0$, maximal subject to $[0,\alpha]$ lying in the closure of S?

(II) What are the accumulation points of S? For example, d^{-2}, $d = 2,3,\ldots$ all are, by taking by Dirichlet's theorem on arithmetic progressions infinitely many primes $q = 1 \pmod d$ and considering the semidirect product $C_q \rtimes C_d$. In fact sequences of p-groups exist with accumulation point p^{-1}, so are the accumulation points simply 0 together with S_n^{-1}, for $n = 2,3,4,\ldots$, or are there more?

I would be interested to hear of anyone's investigations.

Letter to the Editors

Girton College,
Cambridge,
1983 March 1

To the Editor of Eureka

Sir,

It is a matter for some surprise that no protest from Johnians has appeared following Mr Paul Taylor's strictures on John Couch Adams. In QARCH III August 1980 we read that he was "the man who should have discovered Neptune with the telescope still in regular use by undergraduates to-day" and there is a shortened version in Eureka, Summer 1982, No. 42. The story is complicated enough without mis-statements of this kind. It was Professor Challis, of Mr Taylor's* own College, Trinity, who was asked by the Astronomer Royal, Airy, to search for a new planet in the place predicted by Adams' calculations and who after the discovery had been made by Galle in Berlin (1846 September 18) found sadly that "he had observed the planet on three different occasions without, of course, suspecting its planetary status at least on the first two occasions" (Smart, 1947). Adams' work was purely theoretical and it may be noted that at the time when he decided to embark on it he was twenty-two, roughly, I surmise Sir, the present age of Mr Taylor and yourself. References are given below to discussions of Adams' work by Littlewood and Lyttleton.

I can add some information to Mr Taylor's article on the College Societies. In the Girton Review, December 1888, it is recorded that "A Mathematical Club was formed this term. At the first meeting which was held on November 22nd Miss Meyer read a paper on "Early Astronomical Theories and Discoveries". (Miss Meyer was a College lecturer from 1888 to 1918). With over three hundred years start as a College the original foundation of the T.M.S. may

---

*For the informed reader there will be no confusion with the Rev. Brook Taylor of the Theorem; he was a Johnian.

well have been earlier. At the Girton Club papers were read by senior and junior members of the College. One notable exception is G.H. Hardy in 1915 on "Prime Numbers". In 1890 there was a paper on "Standard units of Weight and Measure" by Grace Chisholm. Later she was the first woman to be allowed a degree in Prussia, a Ph.D. of the University of Göttingen, and was the co-author with her husband, W.H. Young, of "The theory of sets of points" (C.U.P. 1906, Chelsea reprint 1972).

In 1926 and 1927 we had joint meetings with the Adams Society. I was away from Cambridge from 1928 to 1938. At some time in that period the Girton Club was absorbed into the New Pythagoreans and my recollection is that when I returned I found that one had to discourage undergraduates from attending mathematical societies on every night of the week.

I remain, Sir,

Yours reminiscently,

Bertha Jeffreys

Bertha Jeffreys.

References

Littlewood, J.E. 1953. A Mathematician's Miscellany, pp. 117-134. Methuen, London.

Lyttleton, R.A. 1968. Mysteries of the Solar System, Chapter 7. Clarendon, Oxford.

Smart, W.M. 1947. Occasional Notes R. astr. Soc., Number 11, Vol. 2, p.60.

Topos Topics

by
P. T Johnstone

One of the most exciting developments in the foundations of mathematics during the last twelve years or so has been the emergence of the concept of topos. But what is a topos? It's surprisingly hard to give a straight answer to that question, because toposes occur in so many different contexts and are used in so many ways; when one tries to give a brief description of what a topos is (as opposed to a formal definition, which is very simple - but not all that enlightening), one is reminded of the story of the five blind men who were asked to describe an elephant, and each gave a wholly different description depending on the part of the animal that he had been allowed to touch. So in this article I shan't try to answer the question "What is a topos?"; instead I shall describe some of the leading examples of toposes, and try to explain why they have proved to be important. I shall try to keep the explanations as non-technical as possible, but readers who wish to follow all the details will need to have at least a vague idea of what a category is (see [1], for example).

1. Spaces and Sheaves. Let X be a topological space, that is a set with a structure which gives us a well-behaved notion of continuity for functions defined on X. In considering (say) the continuous real-valued functions on X, we may wish to consider not only the "global" functions defined on the whole of X, but also partial functions defined on some open subset - for example if X itself is the real line, we may wish to consider $1/x$ (defined on $\mathbb{R} - \{0\}$) and $\log x$ (defined on the positive reals) as well as global functions like x^2 and $\exp x$. The collection of all such partial functions, together with the "restriction maps" which cut down a given function to an open subset of its domain,

motivates the definition of a sheaf on the space X ; conversely there is a representation theorem (the fundamental theorem of sheaf theory) which says that every sheaf on X can be regarded as an algebra of partially-defined continuous functions on X (with values in a space which depends on the particular sheaf under consideration).

The notion of sheaf was introduced around 1945 by the French topologist Jean Leray, as a tool for unifying various ideas then under development in algebraic topology; subsequently it proved to be extremely useful in geometry and complex function theory, as well. (For a detailed history of sheaf theory, with copious references, see [2].) From our point of view, the importance of sheaves is that they provided the matrix from which the notion of topos was born.

Consider the totality of all sheaves on a given space X , together with all maps between them. This forms a category, within which is coded up quite a lot of topological information about X ; although one does lose some information (one cannot, for example, distinguish a one-point space from an indiscrete space of more than one point), enough is retained for one to develop the most important concepts and theorems of topology purely in terms of these categories, rather than the original spaces. This point of view was first popularized by Alexander Grothendieck around 1960; his motive was that current work in algebraic geometry required the study of objects which were clearly sheaf-like, but whose "domain of definition" was something more general than a space. By focussing attention on the category of sheaves, these new "generalized spaces" could be accommodated within the same axiomatization as the traditional spaces, and the name "topos" was chosen as a deliberate back-formation to emphasize the fact that a category of generalized sheaves was seen as something more fundamental than a topological space. Since the 1960's, much work has been done on the development of topology in terms of toposes rather than spaces; what is perhaps surprising is that this

development has paid dividends even within traditional topology, in the form of improved versions of old theorems. (See [3] for a recent survey.)

2. Independence Theorems. There is another way of looking at categories of sheaves, which was never more than implicit in the work of Grothendieck, but which became of primary importance in the refoundation of topos theory achieved by Bill Lawvere and Myles Tierney in 1969. Sheaves are very like abstract sets, in the sense that we can perform on them a lot of the standard constructions of set theory, without going outside the category of sheaves over a fixed base space X. Thus, corresponding to the power-set construction in set theory, one can build "the sheaf of all subsheaves" of a given sheaf (whereas, for example, the totality of all subgroups of a given group does not naturally form a group). So one can regard the topos of sheaves on X as a universe of "generalized sets" which have built into them the possibility of variation over the given domain X. (As an example, the sheaf of continuous real-valued partial functions, with which we began, turns out to be nothing more than the "set of real numbers", constructed by the Dedekind-cuts method, within this "X-varying set theory".)

From this point of view, topos theory becomes a powerful weapon in the search for independence proofs in set theory. If we wish to show that some assertion (the axiom of choice, for example, or the continuum hypothesis) cannot be proved from the usual axioms of set theory, we may try to build a model for the usual axioms in which the given assertion is false. But models of set theory are very hard to construct, because of the "rigid" nature of the axioms; the first independence proofs of this kind (by Paul Cohen in 1963) were an intellectual tour-de-force, and although the techniques have been greatly simplified and extended since then, they are still by no means easy. In contrast, new examples of toposes are very easy to construct, because of the powerful topological and categorical techniques available, and they can be used to give independence proofs which are much

perspicuous than their set-theoretic counterparts. (A good example is Peter Freyd's proof [4] of the independence of the axiom of choice.)

1. Generic Models. Suppose we have a mathematical theory (such as the theory of groups, or partially ordered sets, or fields) whose axioms have been expressed in a suitable formal language. We shall assume that the axioms are "geometric", which is a technical term for a certain kind of bound on their logical complexity; in fact the great majority of theories actually studied by mathematicians can be axiomatized geometrically. In general, such a theory will have lots of different models within the universe of sets; and, using the set-like internal structure of toposes, we can also study its models in any topos.

What concerns us here is the idea, which began to emerge in work of André Joyal and Gonzalo Reyes around 1973, that the theory itself may be identified with a certain topos (sometimes called the classifying topos of the theory) which contains a model of the theory which is generic in the sense that any other model (in any topos) is a "continuous image" of it. If we view toposes as generalized spaces, then the classifying topos is the "space of all models" of the theory; from the alternative viewpoint that a topos is a universe of sets, what we have done is to take our original universe and "freely adjoin" a model of the theory (in the same way that one freely adjoins an indeterminate t to a ring R to form the polynomial ring R[t]).

Statements made about the generic model of a theory (and expressed in the geometric fragment of the formal language) will be true precisely if they are true in all models of the theory; this leads to a particularly simple formulation of the completeness theorem of classical model theory. But we can also study the non-geometric properties of the generic model, which frequently turn out to be more interesting than one might expect; the first example of this was given in 1975 by Anders Kock, when he used properties

of the generic local ring to develop a "universal projective geometry" - an idea which led ultimately to a radically simplified "synthetic" approach to the fundamentals of differential geometry, recently exposed in [5]. We can also construct generic models of theories which have no models at all in our original universe of sets; an interesting example (due to Joyal) is the theory of a covering of the unit interval [0,1] by open intervals of total measure $\leq \frac{1}{2}$ - whose classifying topos yields an independence theorem which asserts that the Heine-Borel Theorem has no constructive proof.

4. Free Toposes. As already indicated, the construction of classifying toposes can be seen as the free adjunction of models of given theories to a given universe of sets. But topos theory also allows us to construct a universe of sets which is free in an absolute sense, or free subject to certain additional axioms (i.e. restrictions on the internal logic). Computations within such free toposes tell us about the proof theory of higher-order logic; that is, the assertions which are true in the free topos are just those which are provable in an appropriate formal system. The internal structure of such free toposes is very complicated; but there are categorical techniques (originally developed, in a geometrical context, by Michael Artin, and adapted to the present context by Peter Freyd) which enable us to give simple "external" proof of the internal logical properties, and hence of theorems in higher-order proof theory. See [6] for a general account of this line of research.

5. Recursive Realizability. A recursive function (from natural numbers to natural numbers, say) is one whose values could be generated by some finite program for an "idealized" computer. Since there are only countably many such programs, it's easy to see that not all functions are recursive. The theory of recursive functions has its own (non-classical) logic, which was first emphasized by Stephen Kleene; the basic idea is that

an assertion (say) of the form "for all x, there exists y such that $\phi(x,y)$" is "recursively realizable" if its truth is witnessed by some recursive function, i.e. there is a recursive f such that $\phi(x,f(x))$ holds for all x. Not surprisingly, this logic occurs naturally in theoretical computer science; and recently Martin Hyland [7] has shown that it is just the internal logic of a certain topos, called the effective topos. In fact, Hyland's construction gives rise to a whole class of similar examples of toposes, which may well turn out to be important in other fields as well; as yet, work on these is still at a very early stage, but there are some important indications of what may be possible in [8].

To close, a couple of suggestions for further reading. [9] is a reasonably elementary account (readable by a bright third-year undergraduate) of the basic definitions and theorems of topos theory -- but the range of examples it discusses is relatively small. For more detailed information, and only comprehensive reference is [10]; but one should be warned that this book is written for the specialist, and is not intended to be easy reading.

References

[1] P.T. Johnstone, "Little Arrows", Eureka 39 (1978), 23-28.

[2] J.W. Gray, "Fragments of the history of sheaf theory", Springer Lecture Notes 753 (1979), 1-79.

[3] P.T. Johnstone, "The point of pointless topology", Bull. Amer. Math. Soc. 7 (1982), to appear.

[4] P.J. Freyd, "The axiom of choice", J. Pure and Applied Algebra 19 (1980), 103-125.

[5] A.J. Kock, "Synthetic Differential Geometry", L.M.S. Lecture Notes Series no. 51 (1981).

[6] J. Lambek and P.J. Scott, "Intuitionist type theory and the free topos",

J. Pure and Applied Algebra 19 (1980), 215-257.

[7] J.M.E. Hyland, "The effective topos", Proceedings of the Brouwer Centenary Conference, to appear.

[8] A.M. Pitts, "The theory of triposes", Cambridge Ph.D. thesis (1982).

[9] G.C. Wraith, "Lectures on elementary topoi", Springer Lecture Notes 445 (1975), 114-206.

[10] P.T. Johnstone, "Topos Theory", L.M.S. Mathematical Monographs no. 10, Academic Press 1977.

Mathematical Call My Bluff

Compiled by C J Budd

"Wise men speak because they have something to say,
Fools because they have to say something."

In an attempt to prove this well known theorem of Plato - or at least to find evidence for the second half of the statement - the Archimedeans has for two years organised a game of Mathematical Call my Bluff.

The game has so far attracted entries from Southampton, Warwick, Kings college London and the 'Other Place', yet, in unsporting fashion Cambridge has won two games out of two. Could this be another possible Blues Sport I hear you ask?

The basic format of the game is for each team to give, in turn, three different definitions of some obscure Mathematical term theorem or diagram. The other teams try to guess the correct definition and one team has to attempt to justify its decision. We see therefore that the game has a dangerous similarity to taking a Tripos Examination. (Incidentally, the word Tripos can also have some pretty odd meanings as observant readers of this journal may have noticed).

To test your skill and provide some training for future contests here are some examples from the two competitions. Remember that these come from a highly competitive examination, you are up against the legendary 'Cambridge Deerstalkers' and also the Kings College team who have forever altered my entire concept of the theory of translations.

(1) The Tarry Point

(a) This point was discovered by that well known Mathematician Nicolas Tarry. Given an earth-moon-sun-spaceship system the Tarry point is that point where a body (eg. Nicolas Tarry) would be in equilibrium.

(b) The Tarry point of a triangle is the point on its circumcircle opposite its Steiner point. The Steiner point of a triangle is the point of intersection of the lines through the vertices of the triangle parallel to the corresponding sides of the first Brocard Triangle. The Brocard Triangle is the triangle whose vertices are on the points of intersection of the lines from the vertices of the triangle to the Brocard points. The two Brocard points of the triangle ABC are the point X st. $\angle XAB = \angle XCA$, and the point Y st. $\angle YBA = \angle YAC$.

(c) Given a dynamical system the Tarry point is the point at which the rate of growth of the system ceases to be exponential - although polynomial growth is still permitted.

(2) Ungers Translation

(a) Ungers translation is a device discovered by Unger and now widely used in the engineering industry. It transforms a problem in potential theory to another which (if you are lucky) may be easier to solve.

(b) Given a series of simultaneous nonlinear partial differential equations which you desire to solve you may decide instead, to try to nail jelly to the ceiling, alternatively you may use Ungers Translation which transforms the whole system to a non euclidean geometry where at least it looks prettier even if it may still be insoluble.

(c) Ungers translation is of course a translation by Unger of a work by Hilbert.

(3) A Room Design

(a) Should you wish to play in the noble game of Bridge you could learn all sorts of exotic bidding schemes. Being Mathematicians you might whilst doing this muse on other problems such as how you might organise the set of movements in a tournament. Precisely this was done by a Mr Room who thus by formalising the system discovered the 'Room Design'.

(b) Around about the year 1939 a group of Trinity Mathematicians who had obviously nothing better to do, decided to find a way to dissect a square into smaller squares of different side length. Being clever chaps they succeeded in this undertaking and the resulting pattern is termed a room design - the smaller squares being the rooms of the large square.

(c) The concept of a room design was worked out by P. Viadyanathaswamy of the university of Bombay. Tile a cuboid in $\mathbb{R}^n$ regularly by subcuboids. Mark certain faces in such a way as to ensure that no subcuboid has > 3 faces marked. Then if it is possible to go from one subcuboid to another entirely by marked faces then we have a room design where the subcuboids are the rooms and the marked faces the doors.

(4) A Mouse

(a) Take a tetrahedron. On each face construct another tetrahedron of side one third of the original. On this tetrahedron construct a further tetrahedron of side one third that of the one it's sitting on. Continue this process for ever. When you have finished, project the sides of each of the tetrahedra which you have formed. What you end up with is a mouse. A finitely small yet infinitely furry little animal.

(b) A mouse is, naturally, a subset of a Cat, - a connected absorbing topology! A mouse is any subset of a cat which has a tail i.e. a proper one dimensional subset, this tail must of course be unique and no two mice are permitted to have the same tail. (Note - this definition should not be confused with tail events which are, of course, only used in probability and have nothing to do with mice).

(c) A mouse is, as is well known, a specialised Premouse. A premouse is an admissable set with an ultrafilter which thinks that the ordering it gets from the ultra filter is a well-ordering. If the ordering is close enough to

let us iterate on the ultrafilter we have an iterable premouse. If this is well behaved we have a critical iterable premouse. A mouse is a critical iterable premouse for which every sub pre-mouse is also critical.

Some other words which you may muse over as to possible definitions are 'The rotten banana at infinity', the 'Topple Set' and the 'N-Con'.

Any hopeful future contestants should contact the present committee of the Archimedeans, who may require written evidence of (in)sanity.

Answers

(1) b (2) c (3) a (4) c Thanks to all taking part who dug up these definitions. Further exotic examples available in any department library.

Geometrical Methods in Geometrical Optics

by A Tan

Traditional college physics experiments employ various algebraic equations from which the desired quantities may be calculated by various means such as log tables, slide rules and pocket calculators. Occasionally these equations can also be solved by geometrical or graphical methods, requiring only ruler, compass and graph paper. In this article, some of these methods are described. Since geometrical methods are most appropriate for geometrical optics, the following methods are restricted to geometrical optics experiments only.

(1) Determination of refractive index of glass by pin method. In this experiment, a rectangular glass slab is placed on white paper and the incident and emergent rays are obtained by planting pins on both sides of the slab such that the pins appear to be on a straight line. The slab is then removed and the refracted ray drawn from the incident and emergent rays and the outline of the slab. In the usual procedure, the angle of incidence i and the angle of refraction r are measured by a protractor, their sines are taken and the refractive index calculated from the relation

$$n = \frac{\sin i}{\sin r} . \qquad (1)$$

Figure 1 shows the geometrical method. Here CO is the incident ray and OB the refracted ray. Measure off OA = 1 on a graph paper. Draw AB$\perp$OA so that AB meets OB at B. With O as centre, draw an arc of radius OB, which intersects OC at C. Draw CD$\perp$DO. Then DO gives the value of the refractive index. The proof is straightforward and is left to the reader.

(2) Determination of refractive index of the material of a prism by the minimum deviation method. This method employs a spectrometer. After the position of minimum deviation of light through the prism is found experimentally, the angle of minimum deviation D is obtained from the reading of the telescope. The angle of the prism can be measured with a protractor from an outline of the prism. The refractive index is calculated from the relation

$$n = \frac{\sin \frac{A+D}{2}}{\sin \frac{A}{2}} . \qquad (2)$$

Figure 2 shows the geometrical method. Angles BOE and COE are drawn equal to A/2 and (A+D)/2 respectively. Measure off OA = 1 and draw AB $\parallel$ OE so that AB meets OB at B. With O as centre and OB as radius, draw a circular arc BC, which intersects OC at C. Draw CD $\perp$ OD. Then OD gives the value of the refractive index. The proof is again straightforward and left to the reader.

(3) Determination of radius of curvature and focal length of a concave mirror. A concave mirror produces real image whenever the object distance is greater than the focal length of the mirror. In the usual u-v method, the position of the image is determined by the parallax method. The radius of curvature r of the mirror is calculated from the mirror equation

$$\frac{1}{u} + \frac{1}{v} = \frac{2}{r} , \qquad (3)$$

where u and v are the object and image distances. Figure 3 shows the proposed graphical method. Draw OA = AB = u and OC = CD = v , the angles OAB and OCD being right angles. Join BD and draw OE $\perp$ AC. Then the length of OE gives the radius of curvature of the mirror. Half of this length is the focal length of the mirror. If we join AD and BC, they will intersect at the midpoint F of OE. Whence OF = EF = f, the focal length. The proof is again simple and left as an exercise.

(4) Determination of focal length of a convex lens. This experiment is similar to the previous one. A convex lens produces real image for object distance greater than the focal length f of the lens. The object and image distances u and v are determined by the method of parallax and the focal length calculated from the lens equation

$$\frac{1}{u} + \frac{1}{v} = \frac{1}{f} . \qquad (4)$$

Graphically, we might proceed as follows. As shown in Fig.4, draw AB = BC = u and AD = v, angles CBA and BAD being right angles. Join AC and BD, which intersect at E. Draw EO$\perp$AB. Then either of OA and OE gives the value of f.

Proof: Letting OE = x, we have from the pairs of similar triangles (BOE, BAD) and (AOE, ABC)

$$\frac{x}{v} = \frac{BO}{BA} , \qquad (5)$$

and

$$\frac{x}{u} = \frac{OA}{BA} . \qquad (6)$$

Adding (5) and (6) and dividing by x, we get,

$$\frac{1}{u} + \frac{1}{v} = \frac{1}{x} . \qquad (7)$$

Comparison with the lens equation (4) gives x = f. Further, from the similar triangles OAE and CBA, OA = OE = f.

It may be mentioned that OE will always give f no matter what BA is. The option of choosing BA = u gives an additional length OA which is equal to f.

(5) Determination of the focal length of a concave lens by the combination method. A concave lens does not, by itself, produce a real image. Hence the usual u-v method cannot be used to determine its focal length. However, if a convex lens of focal length shorter than that of the concave lens is available, then the combination of the two lenses placed in contact behaves

as a single convergent lens and the focal length of the combination f can be determined by the u-v method. If f_1 is the focal length of the concave lens and f_2 that of the convex lens, then

$$\frac{1}{f} = \frac{1}{f_1} + \frac{1}{f_2}, \tag{8}$$

or,

$$\frac{1}{f_1} = \frac{1}{f} - \frac{1}{f_2}. \tag{9}$$

The focal length of the concave lens is thus determined from those of the convex lens and the combination. Figure 5 shows the geometrical method. Draw OA = AB = f and OC = f_2. Join BO and AC and produce them to meet at D. Draw DE⊥AOE. Then either of OE and ED gives the value of f_1. The proof is similar to that of the previous one. Note that the sign of f_1 is negative.

(6) Determination of the focal length of a conves lens by the displacement method. When a luminous object and a screen are placed a distance D greater than four times the focal length of a convex lens, then for two positions of the convex lens, real inverted images of the object can be cast on the screen. If the distance between the two positions of the lens (called the displacement) is d, then the focal length f of the lens is given by the equation

$$f = \frac{D^2 - d^2}{4D}. \tag{10}$$

The geometrical method is shown in Fig.6. Draw AO = OB = D. Draw OC = d, so that AC = D - d and BC = D + d. Next draw AD = AC and BE = BC, DAC and CBE being right angles. Join AE and BD, which intersect at F. Then half of CF gives the focal length of the convex lens.

Proof: Let CF = x. Then we can show as in the construction of experiment (4) that

$$\frac{1}{x} = \frac{1}{D + d} + \frac{1}{D - d}. \tag{11}$$

Simplifying, we get, x = 2f.

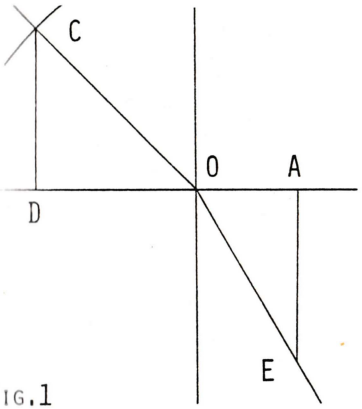


FIG.1

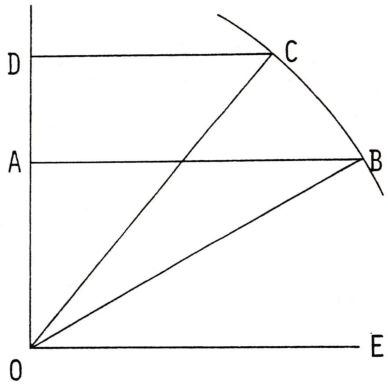


FIG.2

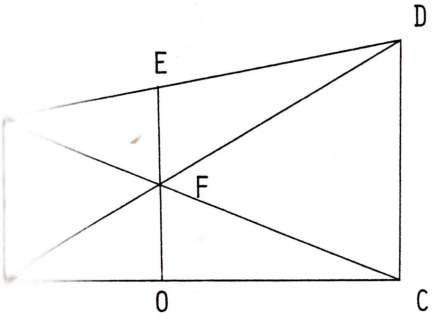


FIG.3

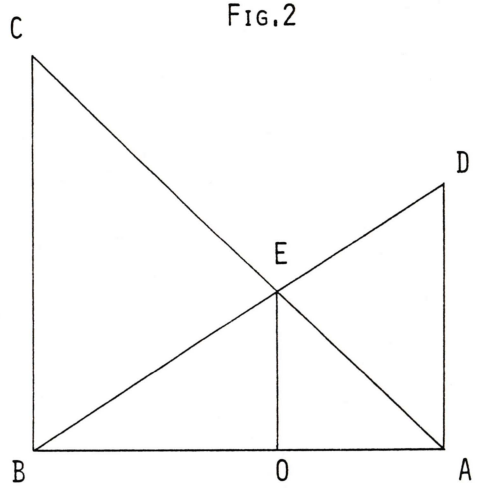


FIG.4

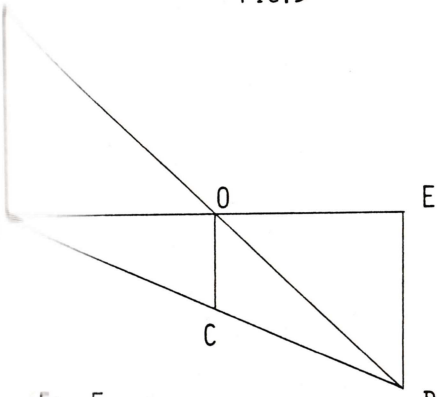
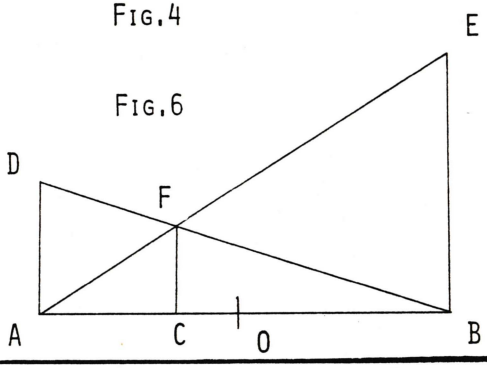


FIG.5

FIG.6



Editorial Note: the Liaison Group article in Eureka 42 was a composite of separate articles by Paul Taylor and Peter Tompkins and so is not fully representative of the views of either author.

Taking More To Heart The Society's Original Objects

by P.Taylor

> "The Archimedeans, taking more to heart the Society's original objects, began to involve itself actively in promoting members' interests within the Faculty ..."

As you will have gathered from an editorial note*, this quotation from Eureka 42 (1982) 31-32 did not come from my pen. I propose in this article to explain my objection to it and put forward some ideas for a direction in which it might go in the near future.

It is in fact very difficult to determine what the Society's original objects actually were, and I should very much like to hear from any readers of Eureka who were in on the foundation either of the Archimedeans or of our sister society the Invariants. The oldest constitution which I have seen dates from 1950, and the only business minutes book I know to have survived covers the years 1961-80. One clue comes from a Michaelmas 1939 programme card kindly sent to me by Mr C.H.E. Warren, who was President of TMS that term, which informs us that Rule 3 required that

> "each meeting of the Society shall whenever possible include a general discussion of the questions raised by the principal speakers."

This custom, I'm pleased to say, still continues, although I frequently find myself the only person willing to venture a question.

More significantly, the then Archimedeans President, in her answer to the question, "What is the Archimedeans for?" in Eureka 3 (1940) 2-5 tells us that the objects were set forth in the Rules as,

> "to study the social, cultural and economic aspects of mathematics and its relation to the other sciences, and the history, philosophy and teaching of mathematics in various countries."

(this is also quoted and discussed by Terry Wall in his editorial in Eureka 20 (1957) 3.) This seems to tie in with what Prof. Cedric Smith told me, namely that it was envisaged that whereas the college societies concerned themselves with imparting mathematical knowledge, the Archimedeans should provide a social and discursive forum for its members, as reflected in the content (almost devoid of mathematics) of the first seven issues of Eureka, which are well worth reading if you can find them.

Thus I would argue that the Founders would concur with me in my belief (which was the principal reason for setting up QARCH three years ago) that the Society should concern itself with making as much contact with mathematicians in other universities (both in this country and abroad) and in industry as possible. During the war there were strong links with Bedford College (which was evacuated here) and King's College London, with the latter of whom we have recently regained contact. Indeed several of the early issues of Eureka were edited jointly in London and Cambridge.

On this front the Society has made progress recently, and not just in the appearance of the Invariants at this year's Problems Drive for the first time in five years. Much of the credit for building up these contacts must go to Miranda Mowbray, but had it not been for the enterprise of two Warwick students, Ian Harrison and Bill Breckon, who turned up out of the blue at a college society meeting a year and a half ago, this might never have got anywhere. Some readers may have seen their magazine 2-Manifold and their notes featuring Eric the pet algebra and Derek the Differentiable Dinosaur.

In other respects it cannot be said that the Society has been successful in recent years. Some two years ago the first major revision of the constitution for twelve years was undertaken, leaving it the worse in every conceivable respect: the evidence of that tragic exercise will be found (under restricted access) in the University Library. The principal theory -- in which I still believe -- was to reduce the size of the executive committee

whilst providing a structure in which many more people could be involved doing important but not central jobs in the Society, but the 1981 constitution failed completely in implementing that theory.

The main problem with a society such as ours is personnel. Without the glamour of, say, the Union Society, we are mercifully spared the hackery associated with it, except when a determined hack happens to be reading mathematics. But that also means that we don't have the regular supply of would-be officers. Nevertheless, if the Society is active and responsive to the views and interests of its members, sufficient people can be found to maintain a high level of activity. One tactic is to encourage as many (particularly first year) members as possible to join the officers and speakers for coffee after Friday evening meetings, raising Society activities frequently in conversation. We have a valuable system of college representatives whose services go unsung: if they had an annual tea party not only would the Society become more responsive to its membership, but also additional organising talent may be brought into it. In a friendly and broadly-based Society it is quite possible for much to be achieved without significant taxation upon the time of its officers, so long as the President has the necessary flair, efficiency and discipline to hold it all together.

Besides gaining the interest of first-years, in which the Society rarely performs disastrously, we must maintain that interest throughout and beyond their career in Cambridge. As a graduate, I find that I must go out of my way to find college society officers in distant parts of the University simply in order to find out where a meeting is to be held, and senior members are never told anything at all. All too often the Society assumes that third-years and graduates are no longer interested, and so it's not surprising that they do no longer take an interest. Perhaps our rules should require there to be at least one graduate on the committee; indeed on the subject of positive discrimination, a little feminine participation might not go amiss.

Apart from graduate students in Cambridge, there are past members

distributed across the globe. Some, laudably, will be reading this article, having gone to the trouble to subscribe to Eureka. But most are forgotten about and hence forget this Society, thereby losing us that vital contact with the outside world which our Founders thought so important. Whilst we have elaborate rules providing for Former Members to take up their membership on returning to Cambridge after an absence, we have records of membership only back to 1976.

Clearly the Committee should pay more attention to advertising Eureka to those about to leave and to providing senior members with copies of the programme card, but to gain the full benefit of the potential good-will outside the University we need a system of representatives or correspondents in universities and industrial research institutions throughout the country. We might consider incentives, providing, say, free Associate Membership to those selling at least thirty copies of Eureka a year.

The feedback gained from this would greatly enrich the service provided by the Society.

In terms of what the Society does in Cambridge, it is widely agreed that there are too many mathematical lectures and too few other events. Fifty speaker meetings a year earns us the envy of mathematics students elsewhere, and it's almost a condition of employment for lecturers to give such talks from time to time. This aspect of our activities had considerable inertia, and continues even when all other activity stops, although attendance and accurate reportings in the programme card in September are signs of a good society secretary. Nevertheless I believe we probably have one too many college society (although I'm not proposing that any be dissolved) and a much greater proportion of the meetings should be given over to undergraduate or graduate papers, or to topics much further from the Tripos.

Another thing which betrays a good secretary is the quality of his minutes: the very best of them present the material more lucidly and accurately than the original lecture. The four oldest college societies have maintained this custom faithfully since foundation, although the minute books of the

Quintics from 1939-42 and all of those belonging to the New Pythagorenas from before the war are missing. The Archimedeans effectively abolished the minutes secretary last year (a job so wisely taken off the Secretary in the constitutional revision of 1961) by removing him from the Committee, and the minute books from before the mid sixties were lost by the Statistics Library many years ago. This is despite the obvious historical value to future biographers of providing some indication of who the active members were: I have twice been approached by people interested in past members of the TMS. The excellent set of minutes that the TMS, for instance, possesses, running to ten volumes, enables its members to see themselves in relation to their now famous colleagues from previous decades.

Another change which the 1981 constitution foisted upon the Society without any discussion whatsoever was to remove the ancient right of college societies to nominate a representative on our Committee. Had this not been done, the present Committee, as it happens devoid of Trinitarians or Johnians, might not have elected to ignore my advice in Eureka 42 (1982) 5-7 that this Society should avoid at all costs being seen to be giving money to college societies, for fear that the TMS and Adams Society might have their grants cut by their respective colleges.

It may be replied that our excellent programme of speaker meetings has not suffered recently, and at least half of the first year mathematicians each year join the Society. These things I have acknowledged, but I have also argued that even in these respects we fall behind the standards we should set for ourselves. However my thesis is that we are failing in our original objects, which were not to provide an extension to the Tripos, in that we make little or no attempt to retain our potential contacts with the outside world, thereby preventing our members from studying those social, cultural and economic aspects of mathematics so dear to our Founders' hearts. With our fiftieth anniversary coming up the year after next, perhaps we might strice to have something to celebrate, of which they might be proud.

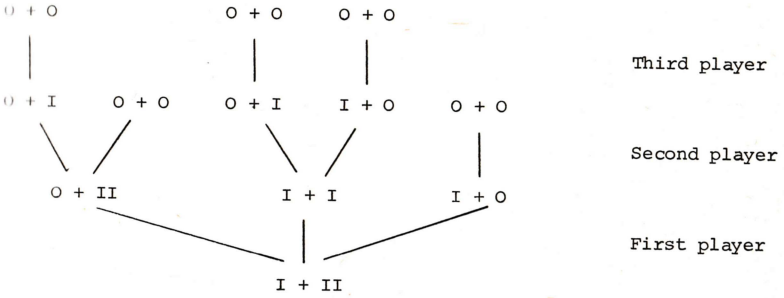
Nim for Three – an Overview and an Offer of Alcohol

by J. Propp

I assume you all know how to play normal Nim [1] in the sense of knowing the rules - even if your knowledge of how to win at Nim amounts to a vague recollection that "it has something to do with base two". But what if there are three players?

Consider the Nim game whose starting position is

a one-bean heap plus a two-bean heap; call the game I + II. Its game tree (to be read from bottom to top) is



Here 0 denotes the empty heap, and is included only for clarity. The winner is the player who makes the last move; the other two players are loners.

Does the first player win this game? No, because she can't win on the first move, and she never gets to make a second move.

Does the second player win? In certain cases, yes; but not if the first player moves to I + I , for in that case the second player has no winning move.

Does the third player win? Not if the second player has already won!

So for the game I + II , none of the players has a winning strategy. Equivalently, any two of them can gang up on the remaining player and prevent him from winning. Let's call such games indeterminate.

Not all games exhibit this behaviour, of course; there are many determinate games. In particular there is an important family of determinate games called the integer games, or integers for short. The integer n is just the Nim-game that starts from a collection of n singleton heaps:

n singleton heaps

In such a game, the players haven't any freedom at all - they simply take turns removing a single bean until no beans remain.

The game 1 (which is the same as the game I) is a win for the first player, the game 2 = 1 + 1 is a win for the second player, the game 3 = 1 + 1 + 1 is a win for the third (or "zeroeth") player, and so on. We have

0,3,6,... are wins for the 0th player,

1,4,7,... are wins for the 1st player,

2,5,8,... are wins for the 2nd player.

Given games G and H we write $G \sim H$ ("G is like H") if G and H are wins for the same player or if G and H are both indeterminate. For integer games m and n , we have $m \sim n$ iff m and n are congruent mod 3 .

The indeterminate game II + II is denoted ∞ , for reasons to be discussed shortly; thus, every game G is like exactly one of the games $0,1,2,\infty$.

Even though $I \sim II$, it would be a mistake to treat the two games as interchangeable, since (for example) $I + I$ is a win for the second player whilst $II + I$ is indeterminate. Still, it is a good idea to put games into classes. Say

$$G = H \text{ iff } G + T \sim H + T \text{ for all games } T .$$

(Our former notion of sameness, namely that two games are the same, iff their game trees are isomorphic, will be called "equivalence" and denoted "$\equiv$".) The power of this notion of equality makes itself evident in the following fact: Every Nim game is equal to

one of the integer games n, or to
one of the games $II + n$, or to
the game III, or to
the game ∞.

The key fact in the theory of three-person impartial games is that $G + T \sim \infty$ for all games T, so that as a corollary $\infty + G = \infty$ for all G. (That's why we call it ∞.) Nearly all reasonably complicated three-person games are equal to ∞. In the case of Nim-games, every game in which there are two or more heaps containing two or more beans is equal to ∞.

There is no reason to limit ourselves to Nim games. We can correspond a three-player game to every game tree in the obvious fashion. We can in principle determine whether a given game G is like $0,1,2,$ or ∞ by using the following rules:

$G \sim 0$ iff all of its options (i.e., all the positions accessible from G, regarded as games in their own right) are like 2;

$G \sim 1$ iff G has an option like 0;

$G \sim 2$ iff all of its options are like 1 and it has at least one option; and

$G \sim \infty$ iff none of the above conditions hold.

Note that these rules give $0 \sim 0$ as required, because the condition in the first rule is vacuously satisfied for $G \equiv 0$. Note also that the proviso that G have at least one option (part of the condition in the third rule) is necessary to prevent us from thinking that $0 \sim 2$.

This leads us into the theory of general (three-person impartial) games, which can shed some light on the Nim-games. For instance, does $II = III$? There is no Nim-game T that distinguishes between them (i.e., $II + T \sim III + T$ for all Nim-games T), but if we set $T = \{0,2\}$ (the game whose options are an empty heap and a 2-bean heap), then

$$II + T \sim 0 \quad \text{(why?)}$$

$$\text{whilst} \quad III + T \sim \infty .$$

So II and III are not equal. On the other hand, III and IV <u>are</u> equal, and in fact every heap of three or more beans is equal to a heap of just three beans. That's why, in the list of the possible "canonical forms" of Nim-games, there was no reference to heaps bigger than III.

You may now be wondering whether $0 = 3 = 6 = \ldots$ The answer is no, and to understand why not we'll need to construct some special games to distinguish between the integers. Let 2^∞ denote the game $\{II\}$, $3^\infty \equiv \{2^\infty\}$, $4^\infty \equiv \{3^\infty\}$, and so on. We also define $1^\infty \equiv \{\infty, 3^\infty\}$ and $n^\infty \equiv \infty$ for $n \leq 0$. It can be shown that $\{1^\infty\} = 2^\infty$ and $\{\infty\} = \infty$ itself, and it is not much harder to prove that $m^\infty + n^\infty = \infty$ for all m,n. Also, we have the curious fact that $n^\infty + 1 = (n-2)^\infty$ for all n. But the fact that we'll make use of here is that the following addition table holds for sums of the form $m + n^\infty$:

	1^∞	2^∞	3^∞	4^∞	5^∞	6^∞	7^∞	8^∞	9^∞	
0	1	2	0	1	2	0	1	2	0	
1	∞	∞	1	2	0	1	2	0	1	
2	∞	∞	∞	∞	1	2	0	1	2	
3	∞	∞	∞	∞	∞	∞	1	2	0	...
4	∞	∞	∞	∞	∞	∞	∞	∞	1	
5	∞	∞	∞	∞	∞	∞	∞	∞	∞	
				.						
				.						
				.						

(Note: This table only tells what $m + n\infty$ is *like*, not what it *equals*.) Since the $n\infty$'s distinguish among the integers, we see that all the integers are really distinct.

Another useful fact about the $n\infty$'s (noticed by Conway) is that $n\infty + G = \infty$ unless the game G can be completed within $\frac{n-1}{2}$ moves. The reason is that in the game $n\infty + G + T$, any two players can keep the other player from winning by always moving in the $n\infty$-component; if they stick to this strategy, they will be able to drive $n\infty$ to ∞ (via $(n-1)\infty, (n-2)\infty, \ldots, 1\infty$) faster than the other player can drive $G + T$ to 0, and the resulting game $\infty + H$ is indeterminate. (To be honest, the preceding argument isn't quite correct, but the essential idea is right). For example, we have

$$1\infty + T \sim \begin{cases} 1 & \text{if } T \equiv 0, \\ \infty & \text{otherwise.} \end{cases}$$

This result implies that *no* game is equal to 0, other than the game 0 itself (that is, $G = 0$ implies $G \equiv 0$). In particular, a sum of games can never equal 0 unless all of the components equal 0. This is in striking contrast with the two-player theory, in which every game has a unique (up to equality) additive inverse, namely itself.

What about 1 ? We know that no Nim-heap except 1 itself is equal to 1, but might there exist some game $G \not\equiv 1$ which nevertheless equals 1 ? The answer is no, because $4\infty + T \sim 2$ iff $T \equiv 1$. What about 2 ? It too is one-of-a-kind, because $7\infty + T \sim 0$ iff $T \equiv 2$.

I put before you the following problems, two of which are still unsolved (guess which).

(1) Find a finite procedure for determining whether two games are equal.

(2) Prove or disprove: if $G \sim 1$ then $G + G \not\sim 1$.

(3) Prove or disprove: if $G \sim 2$ and $H \sim 2$ then $G + H \not\sim 2$.

(4) Suppose every option of G_1 is an option of G_2 and every option of H_1 is an option of H_2. Prove or disprove: if $G_1 = H_2$ and $G_2 = H_1$, then all four games are equal.

(5) Prove or disprove: the game II is "one-of-a-kind" (just as 0,1, and 2 have been shown to be). Or solve this problem with II replaced by one of the integer games 3,4,5,... .

(6) Prove or disprove: If $G + H = III$, then either $G = III$ and $H = 0$ or vice versa.

(7) (the easiest) Prove or disprove: if $G \sim \infty$ and $H \sim \infty$ then $G + H \not\sim 2$.

All students who are able to solve one or more of the first six problems (on their own, of course) will be invited out for drinks one evening this Easter Term at the author's expense. (If you can only solve the seventh, come along anyway - I'll pay for the first round.)

1. "Some Simple Games We Still Can't Solve", by Richard K. Guy. Eureka 1983, pp

P.S. Question 8

There is a lie in this article - find it.

The Boat Race-a Statistical Survey

by

G.A.Bancroft, D.J.Colwell & J.R.Gillett

The boat race between Cambridge University and Oxford University first took place in 1829 at Henley. Initially the race was not held annually and indeed it was also rowed over various courses. However, by 1864 the race had not only become an annual event, but it also took place over a course similar to that used to this day. The only interruptions to this pattern have been for the years of the First and Second World Wars.

The casual observer of this annual contest would usually expect each university to have an equal chance of victory. However, in this article we shall show that this is not the case. At the start of each race one university seems to have a much greater possibility of winning than the other! This probability value will be investigated.

Now in any regular contest between two teams we would expect one team to have runs of victories, interspersed with runs of victories by the other team. For example, the sequence O,O,C,C,C,O,O, of Oxford and Cambridge wins has three victory runs. Such runs can sometimes be quite long, without violating the equal chance of victory hypothesis (1). However, the length of such runs in The Boat Race contest is suspicious. For example, Cambridge had a run of six victories between 1968 and 1973, while Oxford have had an unbroken run of seven victories since 1976. This phenomenon is not new. It has been occurring regularly since the contest began. Indeed one run, with Cambridge as victors, stretched from 1924 to 1936.

Hence, having established the probability of victory for each university, we shall proceed to deduce the expected number of races needed for a given number of victory runs and an associated confidence interval. This expected number and the limits of the confidence interval will then be compared with the actual number of races which have been necessary for that number of runs.

Finally, to add weight to our assertion that the chances of victory are unequal, we shall carry out a similar comparison exercise under the assumption that each university has an equal chance of victory.

Given a list of the victorious universities in every boat race since 1864, the following frequency table may be constructed.

Victory by \ Followed by victory by	Cambridge	Oxford
Cambridge	30½	18
Oxford	18	40½

Table 1.

In this table the (1,1) position, for example, gives the number of times a Cambridge victory has been followed by another Cambridge victory. One debatable point in the construction of the table is the method to be used for recording the tied race of 1877. We have resolved this point by allocating halves for the sequence of outcomes

Cambridge (1876), Tie (1877), Oxford (1878),

in such a way that positions (1,1), (1,2) and (2,2) are allocated ½, 1 and ½, respectively.

It may be deduced from Table 1 that the probability of a university winning, when it has won the previous year, is

$$\frac{40\frac{1}{2} + 30\frac{1}{2}}{107} = 0.6636,$$

a result which may be conveniently taken to be $\frac{2}{3}$.

This probability invites an explanation. Can it be due to the fact that several members of a victorious crew often return to form a strong nucleus for the following year?

Returning to the original data, it is helpful to consider it as a sequence listing the victors. Let X_i denote the i^{th} run of victories in the sequence and let p be the probability that a term in the sequence is the same as the previous one. Also let

$$T = \sum_{i=1}^{n} X_i \quad \text{and} \quad q = 1 - p \ .$$

Then it is easily show that

$$P(X_i = r) = p^{r-1}q \quad (r = 1,2,\ldots) \ ,$$

allowing us to conclude that the random variable X_i follows the geometric distribution. Hence, (2), it may be deduced that

$$E(X_i) = \frac{1}{q} \ , \qquad Var(X_i) = \frac{p}{q^2} \ ,$$

$$E(T) = \frac{n}{q} \ , \qquad Var(T) = \frac{np}{q^2} \ ,$$

and, using $p = \frac{2}{3}$ and $q = \frac{1}{3}$ that

$$E(T) = 3n, \qquad Var(T) = 6n \ .$$

We may interpret $E(T)$ as the expected number of races needed to produce n different victory runs.

Since the random variable T is normal for large n, we may easily find various confidence intervals for T. For instance the following table for the observed and expected number of races required for n victory runs, together with the 68.26% confidence interval (that is $E(T) \pm 1$ standard error, rounded up or down as appropriate) may be constructed.

Number of Runs (n)	Observed Number of Races Needed for n Runs	Expected Number of Races Needed for n Runs (3n)	68.26% Confidence Interval for Expected Number of Races $(3n-\sqrt{6n}) \longleftrightarrow (3n+\sqrt{6n})$
1	6	3	1 <——> 5
2	11	6	3 <——> 9
3	12	9	5 <——> 13
4	13½	12	8 <——> 16
5	15	15	10 <——> 20
6	16	18	13 <——> 24
7	20	21	15 <——> 27
8	21	24	18 <——> 30
9	22	27	20 <——> 34
10	26	30	23 <——> 37
11	35	33	25 <——> 41
12	37	36	28 <——> 44
13	38	39	31 <——> 47
14	41	42	33 <——> 51
15	42	45	36 <——> 54
16	45	48	39 <——> 57
17	50	51	41 <——> 61
18	54	54	44 <——> 64
19	55	57	47 <——> 67
20	68	60	50 <——> 70
21	70	63	52 <——> 74
22	71	66	55 <——> 77
23	72	69	58 <——> 80
24	77	72	61 <——> 84
25	78	75	63 <——> 87
26	79	78	66 <——> 90
27	80	81	69 <——> 93
28	84	84	72 <——> 96
29	86	87	74 <——> 100
30	88	90	77 <——> 103
31	89	93	80 <——> 106
32	90	96	83 <——> 109
33	93	99	85 <——> 113
34	99	102	88 <——> 116
35	100	105	91 <——> 119
36	101	108	94 <——> 122
37	108	111	97 <——> 125

Table 2.

Despite the stringent nature of the confidence interval used in this table, it can be seen that the observed number of races lies well within the confidence limits. Further the observed and expected values compare

...ably. Hence our claim that $p = \frac{2}{3}$ is strongly supported.

Finally, to remove any lingering suspicions that p ought to be $\frac{1}{2}$, we will draw up a table, similar to Table 2, using $p = \frac{1}{2}$. However, to give supporters of this value of p a chance we will relax the confidence limits by constructing a 99% confidence interval.

Number of Runs (n)	Observed Number of Races Needed for n Runs	Expected Number of Races Needed for n Runs (2n)	99% Confidence Interval for Expected Number of Races $(2n-2.58\sqrt{2n}) \longleftrightarrow (2n+2.58\sqrt{2n})$
1	6	2	0 <——> 5
2	11	4	0 <——> 9
3	12	6	0 <——> 12
4	13.5	8	1 <——> 15
5	15	10	2 <——> 18
6	16	12	4 <——> 20
7	20	14	5 <——> 23
8	21	16	6 <——> 26
9	22	18	8 <——> 28
10	26	20	9 <——> 31
11	35	22	10 <——> 34
12	37	24	12 <——> 36
13	38	26	13 <——> 39
14	41	28	15 <——> 41
15	42	30	16 <——> 44
16	45	32	18 <——> 46
17	50	34	19 <——> 49
18	54	36	21 <——> 51
19	55	38	23 <——> 53
20	68	40	24 <——> 56
21	70	42	26 <——> 58
22	71	44	27 <——> 61
23	72	46	29 <——> 63
24	77	48	31 <——> 65
25	78	50	32 <——> 68
26	79	52	34 <——> 70
27	80	54	36 <——> 72
28	84	56	37 <——> 75
29	86	58	39 <——> 77
30	88	60	41 <——> 79
31	89	62	42 <——> 82
32	90	64	44 <——> 84
33	93	66	46 <——> 86
34	99	68	47 <——> 89
35	100	70	49 <——> 91
36	101	72	51 <——> 93
37	109	74	52 <——> 96

Table 3.

This table clearly demolishes the case for $p = \frac{1}{2}$.

References

(1) D.J. Colwell and J.R. Gillett, Coin Tossing, Math. Spectrum, to be published in 1983.

(2) C.M. Clarke and D. Cooke, A Basic Course in Statistics, Edward Arnold (1978).

Codes and Curves

By J F Voloch *

Some three years ago the mathematical community was shocked by the discovery of V.D. Goppa that there exists a connection between codes and curves over finite fields. It was a surprise that a branch of the so-called applied mathematics (coding theory) should have connections with a branch of mathematics lying in the intersection of Number Theory and Algebraic Geometry, considered to be two of the purest parts of mathematics. The aim of this paper is to give a brief description of what this connection is and how it works.

1. Codes

Coding theory consists of the study of how one can transmit a message with ease and accuracy and how one can decipher this message. Its main application is in satellite communication, where one is faced with the problem that interference in communication may cause problems in decoding a message.

More formally, suppose we have a finite set A, called the alphabet, and the elements of this set will be called the letters. A code is a subset of A^n and its elements the words. Since we are not interested in the military uses of codes, we will ignore the problem of coding and decoding the messages from ordinary language to the code. Our problem will be the following: suppose that on transmitting a message some letters of a word have been changed. How can one recover the word?

For this purpose one defines the distance between two words v and v' as the number of coordinates where v and v' differ, and denote this number by $d(v,v')$. It is a metric on A^n, as one can easily check. One defines

*The author was supported by CNPq grant no. 200.916-82-MA.

the weight of a code C as $w(C) = \min\{d(v,v') : v \neq v' \in C\}$. The problem now will be to find a code big enough to contain all the words needed to send our message, but with economy on the length of the words, that is, n and such that $w(C)$ is as big as possible.

The study of general codes is very difficult in every aspect, so we shall restrict ourselves to a subclass of codes that are considerably easier to handle, the linear codes.

Suppose now that our alphabet is a finite field k with q elements. Then a linear code C is defined to be a subspace of the vector space k^n. The size of the code can now be measured by its dimension, which will be denoted by $d(C)$ or simply d when discussing a fixed code.

One can define the weight of $v \in k^n$ as being the number of non-zero coordinates of v and denote it by $w(v)$. In this notation $d(v,v') = w(v-v')$, so for a linear code $w(C) = \min\{w(v) : v \in C - \{0\}\}$.

Let us now define two numerical quantities associated with a linear code $C \subseteq k^n$ that will give the measure of how good a code is for our own purposes. As it can easily be shown, one can correct a word in a message in a linear code if we know that it has less than $\left[\frac{w(c)-1}{2}\right]$ errors, so we define the error correcting rate of a code as being $e(C) = w(C)/n$. The other quantity measures the number of words and the economy of length of the words, and is called the information rate of the code defined by $y(C) = d/n$.

Our problem is now to maximize $e(C)$ and $y(C)$ simultaneously for large n. Some upper and lower bounds for this best value are known although the precise value is not. We will not enter into a discussion of those bounds because this would lead us too far into coding theory and deviate from our aim of describing the codes arising from curves over finite fields.

The reader interested in knowing more about coding theory can consult [4].

2. Curves

In its beginning Algebraic Geometry was concerned with the study of curves, or more generally varieties of arbitrary dimension defined by algebraic equations in $\mathbb{R}^n$ or $\mathbb{C}^n$. It turned out that the definitions and most of the results could be carried over to sets defined by algebraic relations in k^n where k is an arbitrary field. In this more general setting some algebraic complications arose and the subject became very technical. To avoid these technicalities we will be a little informal in our discussion, sketching the analogy with $\mathbb{R}$ and $\mathbb{C}$. The reader interested in seeing the formal definitions and proofs of the results quoted and knowing more about the rich and beautiful world of Algebraic Geometry is advised to consult the beautiful book [2].

Let k be a field and consider the equivalence relation that identifies v and $v' \in k^{n+1} - \{0\}$ if there exists $\lambda \in k - \{0\}$ such that $v = \lambda v'$. The quotient space is called n-dimensional projective space over k and is denoted $k\mathbb{P}^n$ or simply $\mathbb{P}^n$ when k is fixed in the discussion. The class of $(x_0,\ldots,x_n) \in k^{n+1} - \{0\}$ is denoted by $(x_0:\ldots:x_n)$. Note that if some $x_i = 0$ in $(x_0:\ldots:x_n)$ then $y_i = 0$ for all $(y_0,\ldots,y_n)$ in the class $(x_0:\ldots:x_n)$. One can therefore talk about the vanishing of a coordinate of a point in $\mathbb{P}^n$ without ambiguity. Also if $f(X_0,\ldots,X_n) \in k[X_0,\ldots,X_n]$ is a homogeneous polynomial, i.e. all the monomials $aX_0^{i_0}X_1^{i_1}\ldots X_n^{i_n}$ occurring in it with $a \neq 0$ have the same degree $i_0+\ldots+i_n$, one can ask if it vanishes or not at $P \in \mathbb{P}^n$, by taking any representative $(x_0,\ldots,x_n)$ of P and seeing if $f(x_0,\ldots,x_n)$ is zero or not, and this will not depend on the choice of representative of P.

Let $I \subseteq k[X_0,\ldots,X_n]$ be an ideal generated by homogeneous polynomials. We can define $V(I) = \{P \in \mathbb{P}^n : f \text{ vanishes at } P \ \forall f \in I\}$. Such a set is called a projective algebraic set. By defining the closed sets as being the algebraic sets, one can define a topology on $\mathbb{P}^n$ called the Zariski topology.

Later when we talk about local properties, we will be referring to this topology.

By dropping the word 'homogeneous' in the above, one can define in a similar way (affine) algebraic sets in k^n and the corresponding Zariski topology. Note that on the set $A_i = \{P \in \mathbb{P}^n : \text{the ith coordinate of } P \text{ is not zero}\}$ one can define $\phi_i : A_i \to k^n$, $\phi_i((x_0:\ldots:x_n)) = (x_0/x_i,\ldots,x_{i-1}/x_i,x_{i+1}/x_i,\ldots,x_n/x_i)$. ϕ_i is a homeomorphism. We will now make some definitions concerning algebraic sets in k^n and afterwards will carry them to $\mathbb{P}^n$ via the ϕ_i's .

Def.1: An irreducible curve is an algebraic set $V(I)$ where I is a prime ideal of $k[X_1,\ldots,X_n]$ such that the field of fractions of $k[X_1,\ldots,X_n]/I$ has transcendence degree 1 over k (this intuitively means that there exists only one independent variable on the curve and irreducibility means at least connectedness.)

Def.2: A curve is non-singular if given a set $f_1,\ldots,f_r$ of generators of an ideal defining it the matrix $(\partial f_i/\partial x_j(x_1,\ldots,x_n))$ has rank n-1 at every point $(x_1,\ldots,x_n)$ on the curve.

In the case $k = \mathbb{R}$ or $\mathbb{C}$, definition 2 means that the curve is smooth* and then one can define a tangent line at every point of the curve, and this is also true in the general case.

Given a projective algebraic set V defined by the ideal $(f_1,\ldots,f_r)$, the set $\phi_i(A_i \cap V)$ is also an algebraic set and it is defined by the polynomials g_j obtained by assigning the value 1 to the ith variable of f_j for all $j = 1,\ldots,r$.

A non-singular irreducible projective algebraic curve is an algebraic set X of $\mathbb{P}^n$ such that $\phi_i(X \cap A_i)$ is a non-singular irreducible curve for all $i = 0,\ldots,n$. We will now consider only non-singular irreducible projective algebraic curves and will refer to them simply as curves. As a

*By the implicit function theorem.

subset of $\mathbb{P}^n$ they inherit a topology from the Zariski topology on $\mathbb{P}^n$ and we will consider these curves with this topology.

Def.3: A rational function r on a curve X is a function defined on an open set A of X such that for every $i = 0,\dots,n$ it can be written as $f\circ\phi_i^{-1}/g\circ\phi_i^{-1}$ where $f,g \in k[X_1,\dots,X_n]$ are homogeneous polynomials of the same degree and g does not vanish at any point of $\phi_i(A_i \cap A)$. The set $X-A$, which can be proved to be finite, is called the set of poles of r if A is maximal. (Of course it can be proved that such an A is unique.)

Given a rational function r on X one can assign to it, similarly to the case $k = \mathbb{R}$ or $\mathbb{C}$, a differential form dr which is, at each point P where r is defined, a linear function from the tangent line of P to k.

Def.4: A differential form ω on X is a function defined on an open subset A of X that assigns to each $P \in A$ a linear function to k from the tangent line of X at P and such that it can be written in a neighbourhood of P as sdr for some rational functions r,s. Again if A is maximal, $X-A$ is called the set of poles of ω.

We remark that in the case $k = \mathbb{C}$ the curves are the same as the compact Riemann surfaces and in the general case the rational functions (resp. differentials) play the same role as the meromorphic functions (resp. differentials) on the Riemann surfaces.

As in the case of $\mathbb{R}$ and $\mathbb{C}$ one can find a local uniformising parameter z establishing an isomorphism (i.e. a map carrying all the properties from the curve to its image) from a neighbourhood of every point of X to an open subset of k (again in the Zariski topology). In this parameter a rational function r can be developed in a power series $\sum_{n_0}^{\infty} a_n z^n$, $n_0 \in Z$, $a_n \in k$, $a_{n_0} \neq 0$. If $n_0 < 0$, then the point corresponding to $z = 0$ is a pole of z, and $-n_0$ (which does not depend on the choice of the parameter as can be proved) is called the order of the pole. If $n_0 = -1$, then the pole is called simple and the function is said to have residuce a_{-1} at this pole. If $n_0 > 0$, then the function has a zero at $z = 0$ and n_0 is called

the order of the zero. Similarly a differential form can be written as $(\sum_{n_o}^{\infty} a_n z^n)dz$ and the same definitions for zeroes and poles can be given.

Consider now the free abelian group generated by the points of X, i.e. the set $G = \{ \sum_{i=1} n_i P_i : n_i \in \mathbb{Z}, P_i \in X\}$ with the obvious operation of addition. An element of G is called a divisor of the curve. Given a rational function r or a differential ω on a curve, it can be proved that it has finitely many zeroes and poles. Denote the zeroes as $P_1,\ldots,P_s$, the poles as $Q_1,\ldots,Q_t$ and the corresponding orders $n_1,\ldots,n_s$ $m_1,\ldots,m_t$ and associate to it the divisor $\Sigma n_i P_i - \Sigma m_j Q_j$ denoted by (r) or (ω) in the corresponding cases. A divisor of the form (r) where r is a rational function is called a principal divisor and a divisor of the form (ω) where ω is a differential is called a canonical divisor.

Let $\deg: G \to \mathbb{Z}$ be the function $\deg(\Sigma n_i P_i) = \Sigma n_i$. It is called the degree.

If a divisor $D = \Sigma n_i P_i$ is such that $n_i \geq 0 \ \forall\, i$, then it is called a positive divisor. If D and D' are divisors, then we say that D is greater than or equal to D' (denoted by $D \geq D'$) if $D-D' \geq 0$ i.e. is positive.

Given a divisor D, let $L(D)$ be the set $\{r,$ rational function: $(r) + D \geq 0\} \cup \{0\}$. It is a vector space over k and one can prove that it is finite dimensional. Its dimension is denoted by $\ell(D)$. Similarly define the space $I(D)$ with differentials in the place of functions and denote its dimension, which is also finite, by $i(D)$. The next theorem connects $\ell(D)$ with $i(-D)$ and is the most important single theorem in the theory of algebraic curves.

Theorem (Riemann-Roch) Given a curve X, there is an integer g attached to X such that for every divisor D we have

$\ell(D) = \deg D - g + 1 + i(-D)$.

In the case $k = \mathbb{C}$, the curve can be viewed as a Riemann surface, so it has a topological genus g', given by the number of handles in its

canonical topological form as a sphere with handles. It can be proved that in this case $g = g'$, so by this analogy we call g the genus of X in the general case.

Still for $k = \mathbb{C}$, by Cauchy's theorem a function has the same number of zeroes and poles counted with multiplicities so $\deg(r) = 0$ for a principal divisor and by Liouville's theorem a function with no poles is constant. It is not surprising that the same holds for the general case and we will use this in what follows.

It can also be proved that the degree of a canonical divisor is $2g - 2$.

3. Codes arising from curves

Let k be a finite field with q elements and X a curve over k. $X = \{P_0, \ldots, P_n\}$. X is finite because $k\mathbb{P}^n$ is finite. Let $D = aP_0 + P_1 + \ldots + P_n$ be a divisor of X where $a \in \mathbb{Z}$ $2g - 2 < a \leq n + g - 1$, hence we suppose $n > g - 1$.

Consider the vector space $I(D)$ over k and the linear map $\text{res}: I(D) \to k^n$, $\text{res}\,\omega = (\text{res}_{P_1}\omega, \ldots, \text{res}_{P_n}\omega)$, where $\text{res}_{P_i}\omega$ is the residue at P_i of ω, defined also when P_i is not a pole of ω as 0. Since $\omega \in I(D)$ has at most simple poles at P_i and no others, res is well-defined. This map is injective since if $\text{res}\,\omega = 0$, then ω has no poles, and also it has at least a zero of order a at P_0. Therefore $\deg(\omega) \geq a$ but since $\deg(\omega) = 2g - 2$ and $a > 2g - 2$ this is a contradiction proving the injectivity of res. Let C be the code given by the image of res.

The weight P of res ω is the number of poles of ω. If N is the number of zeroes of ω counted with multiplicities, then $N - P = \deg(\omega) = 2g - 2$, so $P = N - (2g - 2) \geq a - (2g - 2)$, since ω has at least a zero of order a at P_0, so $w(C) \geq (a - (2g - 2))/n$.

By Riemann-Roch, $d(C) = \ell(-D) - \deg(-D) + g - 1 = n - a + g - 1 + \ell(-D)$. Therefore, $y(C) \geq (n - a + g - 1)/n$, so $w(C) + y(C) \geq (n - g + 1)/n = 1 - \frac{g}{n} + \frac{1}{n}$. These codes will be good when

n is as big as possible compared with g . Let us define then $A_q(g) = \max\{\#X,$ X curve over k with genus g$\}$ and $A_q = \limsup \frac{A_q(g)}{g}$

The celebrated Riemann hypothesis for curves over finite fields proved by A. Weil (see [1] for a simple proof) asserts that if X is a curve with N points then $|N - (q + 1)| \leq 2gq^{\frac{1}{2}}$. Therefore $N \leq 2gq^{\frac{1}{2}} + q + 1$ so $A_q(g) \leq 2gq^{\frac{1}{2}} + q + 1$ so $A_q \leq 2q^{\frac{1}{2}}$. This means that the number $1 - \frac{g}{n} + \frac{1}{n}$ that approaches $1 - \frac{1}{A_q}$ as $q \to \infty$ is not much greater than $1 - \frac{1}{2q^{\frac{1}{2}}}$. If this bound could be obtained, the resulting codes would be the best possible. The known bounds for codes show that this is not possible for $q = 2$ or 3 . On the other hand Drinfeld and Vladut (unpublished, see [5]) proved that $A_q \leq q^{\frac{1}{2}}-1$, improving Weil's bound, and Ihara constructed curves over fields with p^{2m} elements, p prime ≥ 7 with enough points to guarentee that $A_q = \sqrt{q} - 1$ in this case (see [3]). These curves give some of the best known codes but in applications one uses mainly $q = 2$ and 3 . Very little is known in such cases apart from Serre's recent calculation of $A_2(g)$ for $g \leq 50$ and a few more (unpublished).

Added in proof: Some unofficial rumours coming from Hollywood say that the next film in the James Bond series marking the return of Sean Connery as Bond will be entitled "The Terrible Prof. Bourbaki".

References

[1] Bombieri, E. Hilbert's 8th problem: an analogue in mathematical developments arising from Hilbert's problems. F. Browder, ed. Proc. sym. pure math. vol XXVIII AMS 1976.

[2] Hartshorne, R. Algebraic Geometry, GTM, Springer-Verlag 1977.

[3] Ihara, Y. Some remarks on the number of rational points of algebraic

curves over finite fields: J. Fac. Sci., Univ. Tokio, sect IA 28 (1981) pp. 721-724.

MacWilliams and Sloane. The theory of error-correcting codes: North-Holland 1977.

Manin, Yu.I. What is the maximum number of points on a curve over F_2? J. Fac. Sci., Univ. Tokio, Sect IA 28 (1981) pp. 715-720.

Solutions to Problems Drive

1. 9

2. 11

		X		
X	X		X	X
X	X	X		X
	X	X	X	
		X		

3. i) 19924. one = 15,14,5 as 0 is the 15th letter of the alphabet etc.

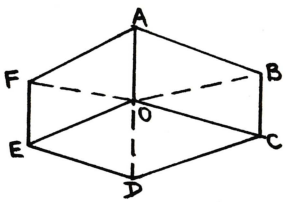
   ii) 98. The first digit of each number comes from the decimal expansion of π and the second from e .

4.

Team	P	W	D	L	F	A	Pts.
England	3	1	2	0	7	3	4
Wales	2	0	2	0	2	2	2
Ireland	3	0	2	1	1	2	2
Scotland	2	1	0	1	1	4	2

England-Wales draw 2-2

5. Planes AOD, BOE, COF .



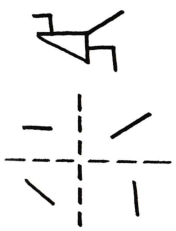
6.

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

7. Yes. If it is homeomorphic to a torus.

8. 5 : 2

9. None.

10. 

(Other plausible answers were also found.)
Take all even permutations of the line segments, joining them together as appropriate.

11.
3 = 1 x 4 - 3 + 2
4 = 2 x (1 + 3) - 4
5 = 1 x 3 + 4 - 2
6 = 4 x 2 - 3 + 1
7 = 3 + 4 x (2 - 1)
8 = 4 x (3 + 1 - 2)
9 = 3 x 4 - (2 + 1)
10 = 2 x 4 + 3 - 1
11 = 4 x 3 - 2 + 1
12 = (3 - 1) x (2 + 4)

12. D